ARAB-GERMAN YOUNG ACADEMY OF SCIENCES AND HUMANITIES

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

by Kalman Graffi & Tobias Amft

Abstract

Online social networks and online real-time communication tools have gained large popularity in the last few years. During the Arab uprisings they emerged as one of the main tools for exchanging ideas and for organizing activities. In this article, we review the technology and infrastructure for online social communication, as well as the weaknesses that were used to spy, censor and block it, and highlight current trends in research on how to overcome these obstacles. Specifically, we present networking technologies that provide tools to the users to make their communication resilient, secured and impossible to track. Thus, we investigate social communication during but also beyond the Arab uprisings from the perspective of computer science, and combine the resulting insights with current developments in this discipline.

September 2016

Academia in Transformation

This Working Paper is part of a series of publications in the project “Academia in Transformation”. A collective volume of all project papers will be edited by Florian Kohstall, Carola Richter, Fatima Kastner and Sarhan Dhouib and published by NOMOS in 2017.

Suggested Citation

Graffi, Kalman & Amft, Tobias (2016): Webs of Change? The Transformation of Online Social Networks and Communication Infrastructures from a Technological Point of View. Arab-German Young Academy – Transformation Group Working Paper No. 3/2016.

Working Paper Series

About the Authors

Kalman Graffi

is Junior-Professor for the ''Technology of Social Networks'' at the Institute of Computer Science at the University of Düsseldorf in Germany. With his nine PhD students, he concentrates his research on network protocols and mechanisms to support the freedom of speech and privacy around the globe. He is an AGYA member since 2014.

Tobias Amft

M.Sc., is doctoral student and researcher in the Lab for Technology of Social Networks, led by Jun.-Prof. Dr.-Ing. Kalman Graffi, at the Institute of Computer Science, Heinrich Heine University of Düsseldorf. His research interests include distributed (peer-to-peer) systems, network protocols, network security and many other topics.

About the AGYA Working Group Transformation

Popular uprisings in the Middle East and North Africa (MENA) have had a deep impact, not only on the societies in the respective countries, but also on academic disciplines and scientific relations between Europe and Arab countries. Many of the developments that have taken place in the region are not exceptional but reflect and accelerate global trends. The importance of new media, new forms of social mobilization and new instruments of governance are not limited to the MENA. Through a transcultural perspective the Working Group Transformation of the Arab-German Young Academy of Sciences and Humanities (AGYA) aims to better understand these trends. The Working Group debates how ideas, norms and concepts are diffused in a context of mutual exchange and how scientific relations between Europe and the MENA can be improved.

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

Free speech is the most valuable achievement of mankind. 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 apparent as the predominating communication channel to exchange information and data. Billions of bits and bytes travel around the earth at the speed of light at any given moment. As technology improves, authorities increasingly feel the urge to monitor, censor, or even prohibit communication via the Internet as it allows information and ideologies to spread rapidly within seconds. People are able to form groups and meet in virtual reality although they are scattered around the globe.

From a computer scientist's point of view, the Egyptian upheavals are technically the most interesting of the Arab uprisings. The Egyptian government managed to shut down the country's Internet access (almost) completely with the intention of hindering the growing revolts from heating up. Paradoxically, it was a decision which might have even intensified the revolt. More than 80 million people had, considering Egypt's communications engineering, a communication blackout. As explained in Eaton (2013), during the demonstrations of January 25, 2011, *Facebook* was mainly used (>85%) to organize and plan activities around the revolts or to inform Egyptians and the remaining world about the ongoing events. Other services accessible through the Internet, such as *Twitter*, *Flickr*, *YouTube*, etc. were being 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 of *Facebook* followed one day later (Dainotti et al. 2011). Moreover, Internet access was entirely shut down during the night of Thursday, January 27 through Friday, January the 28. The Egyptian government instructed the Internet providers to shut down their services (Cowie 2011a). On February 2 Egypt returned to the Internet again (Cowie 2011b). According to Dainotti et al. (2011), Libya experienced the same procedure around two weeks later, on February 18. While previously activists had already suspected that digital communication was being spied on, these steps showed that also the connectivity itself was in danger.

In this article, we review the technology and infrastructure for online social communication and discuss the weaknesses of the technology for spying on, censoring and blocking the dissemination of information. We present the current state of technological developments in computer science which provide tools for secure, anonymous and untraceable communication. With the aid of our insights we offer an evaluation of how far the Arab uprisings affected academic thinking in computer science, with a particular focus on topics concerning privacy, anonymity and security in networking and communications. We provide a brief overview of the changes in academic thinking. Relying on our expertise, we analyze and explain the advancements in technology and predict a future trend concerning privacy, surveillance and censorship.

The Fields in Computer Science Impacted by the Arab Uprisings

In the following section we present how Internet services can be – and have been – blocked, and how the Internet as a communication platform can be closed by governments upon inclination.
Researchers in computer science reflect on current events and sometimes include them in their research activities as case studies. Here, it is worthwhile to discuss which fields in the research sphere of computer science have been affected by the Arab uprisings. According to the classification system of the German Research Association (DFG), the field of computer science is clustered in eight subject areas, the most prominent of them being "theoretical computer science," "software engineering and programming languages", and "computer architecture and embedded systems".
These three subject areas investigate basic bedrocks of computer science, namely theories as well as the engineering aspects of software and hardware. The theoretical aspects of computer science are highly abstract and analytical, often also simplifying practical experience. The hardware-related subject area on computer architectures and embedded systems aims to provide solutions for accelerated, improved hardware thinking in long time scales. Software engineering and programming languages offer tools to harness the potential of the hardware fully, and to support further ongoing trends such as parallelization, distributed computing or device and technology-specific programming. These subject areas are therefore rather less affected by current events or singular cases of usage.

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

Two subject fields which have gained interest in recent years and which are related to the events in the Arab uprisings are "massively parallel and data intensive systems" and "interactive and intelligent systems, image and language processing, computer graphics and visualization". Both subject fields aim at the identification, processing and interpretation of large amounts of data. This trend is known as "Big Data". Processing digital information, either from advertisements, meta-data, social networks or communications allows to cluster customers, increase revenues through improved advertisements and recommendations as well as to predict the future behavior of customers. The same concept of deep data analysis can be used to observe communication patterns on the Internet, to identify discussion and communication topics, and to initiate a reaction to them, such as reporting, blocking or even extending beyond that. Through advancements in the subject 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 have contributed to the surveillance of Internet users in the Arab world during the Arab uprisings and also worldwide in general.

The two remaining subject areas comprise trends that support the flow of information and counteract surveillance and control of communication. These two subject areas 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, results in this field directly affect the options in terms of what data can be obtained from the users against their will. Secure communication over the Internet, i.e. confidential and anonymous, would allow the Internet users to exchange their ideas freely. However, secure communication would still leave traces, which allows the identification and blocking of this secure communication.
Here, the subject area of “operating, communication, database and distributed systems” provides various solutions 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 for digital communication. Combined with security considerations, these novel distributed platforms promise to support digital communication which 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 subject area of secure communications that have been initiated through the observations during the Arab uprisings.

A Brief Description of the Internet

Before we describe the Internet itself, we 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 that 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 into life .
Those rules, or more precisely protocols, define a communication structure which 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 which 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 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 form of data packets, from a given source host to an arbitrary destination host.
Unfortunately, the Internet Protocol itself gives no warranty 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 TCP is to secure a 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, TCP comprises different techniques which control the traversal through a network. The second purpose of TCP is to identify and separate different applications running on a single host. One example for running different applications could be that a user is streaming music from an Internet Radio station while she/he is at the same time retrieving the latest news from an online magazine. Since nowadays the Internet consists of millions of connected devices, the task of finding the computer to a given Internet address is not an easy task. Rules have to be defined and followed to find a way from a source computer to a destination. For a proper explanation we introduce the terms forwarding and routing. With forwarding we mean the process of 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 given a set of potential nodes to which to forward a data packet. Algorithms and rules that specify a forwarding strategy for participating devices are thus termed routing algorithms or routing protocols. A device which decides how to forward a given packet, on the other hand, is usually called a router.

The Internet, which has meanwhile become one of the most complex infrastructures humanity has ever created, consist of many different devices, routers, and routing protocols which in combination yield a great variety of services we can use. Despite its complexity, the Internet comprises multiple parts which are controlled and managed by different organizations, typically an Internet Service Provider, so that a certain hierarchy is formed. The parts of the Internet managed by different organizations are called autonomous system. One indispensable protocol which connects all existing autonomous systems is the Border Gateway Protocol. The task of this protocol, amongst others, is to announce an autonomous system's existence to other autonomous systems on the Internet. Furthermore, the Border Gateway Protocol assures that all autonomous systems on the Internet know how to route messages to a specific autonomous system.

Technical Possibilities for Censoring Communication on the Internet

The Arab uprisings and the resulting blockade of the Internet in Egypt and Libya prove that surveillance and censorship of Internet traffic are desirable goals of certain governments, as are the possible attempts to oppress certain groups of interest – insofar as the current state of the art permits it – such as activists during the Arab uprisings. 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 keyword "passive" suggests, adversaries may only 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 revolutions of the Arab uprisings (passive attacks alone are not sufficient to block Internet access for a whole country), we focus on active attacks on network traffic in the following discussion. These attacks have in common that they are, at least partially, noticeable

to Internet users. With "partially noticeable" we refer to the fact that the content of censored web sites might be blocked. A user will notice the absence of such content only if she/he has a non-blocked site as reference. Next, we present some commonly used techniques of active network attacks.

Search Engine Censorship

The Internet as a constantly growing system contains more than 46 billion sites, according to measurements from de Kunder (2015) in August 2015. Regardless of this fact, the number of websites every person frequently visits 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 which 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 70.23% in July 2015, followed by *Bing* (10.33%), *Yahoo* (9.54%) and *Baidu* (7.06%).
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 part is called web crawling. All websites found by the web crawler are stored by the search engine provider in a database for later use. If it comes to a search query initiated by a user, the search engine compares its index database with the given keyword(s) in order to identify matches between the search term and stored websites. It depends on the service provider if it returns all or no matching results to the user, or if it filters 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 in order to restrict, according to the local laws, illegal websites which deal, for example, with anti-Semitic, Nazi-related, or radical Islamic content. Since the technique of search engine censorship is simple, the bypassing of its 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. Other search engines can be used to examine other parts of the Internet. Sometimes the usage of a proxy can help to circumvent local restrictions. We provide more details on proxies in the section on proxy routing.

Deep Packet Inspection

Actively hindering people from accessing specific sites on the Internet is more costly than just monitoring network traffic.
In order to enable well-aimed filtering and surveillance of information that traverse the Internet, access to the Internet infrastructure has to be available to place an attack. There is no real benefit for an attacker to discard arbitrary packets or to distort the global functionality of any service at random, as this happens on a small scale in the network as well. Large projects for the purpose of packet fil-

tering (or any other projects) are only effective if they pursue a certain goal and are therefore placed at the right location or advertised to the right group of people, thus being on the main routes of a data flow.

Furthermore, it is necessary that potential attackers have access to those parts of the network which are worth intervening in. 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 package inspection have been present long before the Arab uprisings emerged (Wagner 2012).
To be in charge of investigating packets in depth, a government must be capable of intervening in network traffic at some specific locations of the Internet. Therefore, the Tunisian government had to manipulate inherent Border Gateway Routers that run the Border Gateway Protocol directly.
At this point, we have to remember that the Border Gateway Protocol enables routing (forwarding of packages) between different autonomous systems. The Border Gateway Routers are best suited to monitoring the connection of the national network, the Tunisian part of the Internet, to the other networks and other parts of the Internet. Among routers which are 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 Tunisia, the Tunisian Internet Agency (ATI) represents the gateway which serves all Tunisian ISPs (OpenNet Initiative 2009). Since this agency was in close contact with the Ben Ali regime, it was the institution that intercepted network traffic.

Since at all those gateways it is theoretically possible to investigate packets which traverse the Internet, packet filtering can be done very easily. Whenever a packet which is not encrypted traverses a gateway that is under surveillance, firewall-like programs search for specific keywords in bypassing data, which is marked as suspicious by the inquisitive government.

The work of Clayton, Murdoch & Watson (2006) describes in detail how TCP connections that are associated with specific keywords can be terminated by a willing attacker. China as an example forces a suspicious connection to shut down by answering a query with special TCP packets. Similar to a normal firewall, which supports the forwarding of desired packets and drops undesired packets, any government – the Tunisian, the Egyptian, etc. – is capable of controlling the forwarding mechanism of packets in their national network. The government can decide whether or not to forward, observe, or drop messages. Taking Tunisia as an example, to control the national network traffic, in 1996 the Tunisian Internet Agency was created and instructed to start the process of Internet censorship in the country in 1997 (Wagner 2012).

However, what is astonishing is that deep packet inspection techniques operate more subtly and unobtrusively than we might think. A normal user would probably think about technical problems that seem to depend on the browser or on the Internet Service Provider. Even trickier is when TCP connections are properly closed by the adversary, and the user receives nothing more than the notifica-

tion 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, amongst others, was already able to analyze and filter different URLs and emails during the tenure of Zine El Abidine Ben Ali. A telecommunications law from 1998 even allowed the Tunisian authorities at that time to investigate the content of personal email messages (OpenNet Initiative 2009). Commercial filtering software scans different 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 thereupon successfully blocked. Email messages which 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 in the network are directly blocked. From the technical point of view this kind of attack is a simple firewall setting which blocks the traffic to or from a specific IP address or whole address blocks.

Disconnection of Networks

As we have seen above, the Internet has grown to a medium which connects billions of different devices. We have already discussed the Border Gateway Protocol whose goal is to interconnect different autonomous systems and to announce their existence to each other. In other words, the linkage of all the different autonomous systems forms the Internet as we know it. The Border Gateway Protocol, or better yet, the routing entries in a Border Gateway Router are necessary for packets to find their way from a 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 unwanted 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 the neighboring countries. Doing this, packets which were addressed to any target outside Egypt were not able to find a path towards their destinations. Packets that reached a Border Gateway Router responsible for the forwarding of the packet across national borders were deleted, since a Border Gateway Router without routing entries normally does not know how to forward an incoming packet.
A more drastic method would be to disconnect the Border Gateway Routers from the physical network, or even to cut the cables connecting different devices. Drawback of this method is mainly the increased overhead material costs. In any case, the deletion of routing entries at Border Gateway Routers is enough and fulfills its purpose.

Solutions to Fight against Surveillance and Censorship in General

The techniques for surveillance and censorship are as numerous as the possibilities to bypass those mechanisms. 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. We present here an assorted collection of possibilities which can be used to avoid censorship driven by active attacks and surveillance brought by passive network observation. These solutions originate from the subject area of "security and dependability" and "operating, communication, database and distributed systems".

Encryption

The wish to hide confidential information from curious eyes leads to the oldest known approach against surveillance: encryption. One of the first encryption algorithms known from historical records is the Caesar Cipher, invented by Julius Caesar. Letters taken from the alphabet are simply shifted to a known number of positions. Doing this, only people who share the knowledge about 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 been a commonly used method to transfer information in unreadable code up to the present day. Simple methods like the Caesar Cipher suffer from small key sets and smart algorithms which are able to rebuild the unencrypted plain text without knowing the secret which has been used to encrypt information.
Modern encryption algorithms rely on more complex methods to translate plain text into cipher text. In theory, the recalculation of the encrypted text requires to guess the key in a very large pool of combinations. Currently, this technique would require billions of years with current hardware and software. Encryption in general can only be used to secure the content of communication from being seen by unauthorized persons – a property termed confidentiality. Nevertheless, such methods are not enough to provide anonymity, privacy and security. Attackers could still be able to determine the identity of the communication partners and hinder them from exchanging further messages and from initiating further actions.

Proxy Routing

The idea of anonymity, especially on the Internet, is usually pursued and implemented through proxy routing. The main goal of this technique is to hide the sender, receiver, or sender and receiver simultaneously from being tracked 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 to a specified destination. Optionally, messages are often encrypted. The strategy of routing messages via additional participants is necessary in those systems to conceal the 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 IP address and location. Using *Tor*, requests for a website are routed through an encrypted connection over several *Tor* servers before they reach the required web server. The last participant in the chain, called exit node, connects to the web server and requests the desired website. The website itself is passed all the way back to the initial requester. Although *Tor* is designed to provide a certain anonymity level by concealing the address of a user, *Tor* is helpless against the manipulation or censorship of websites or other information the requested server maintains. The method of proxy routing has a minor side effect which allows one to circumvent regional search engine restrictions, for example. Using a proxy to forward messages and queries, a search engine believes the request starts at a location near the proxy. If the proxy is located in a region in which no restriction is 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 uniqueness of the protests during the Arab uprisings is characterized by the enormous usage of social media and familiar Internet platforms like *Facebook*, *Twitter* and *YouTube*, which mainly have been used to organize demonstrations, to share informational content or simply to criticize the government. Furthermore, social media was used to communicate with countries outside the MENA region and to exchange information with people living in other countries that were involved in the Arab uprisings (Howard et al. 2011). According to the Institute of World Economy and International Relations (IMEMO), *Facebook* even outmatched the Arabic TV channel *Al Jazeera* in the speed of information traversal (Stepanova 2011).

As a response to the revolutionary movements in North Africa, the Egyptian government instructed mobile operators and Internet Service Providers to suspend their services. As a result, most parts of the Internet were cut off. Few governments had done this before: Nepal cut off Internet access entirely in 2005, as did Myanmar two years later in 2007 (Richtel 2011). The cases of Nepal, Myanmar or Egypt are rare examples that could be repeated any time. They show clearly that governments of countries with simple Internet infrastructure are capable of stopping national Internet traffic almost entirely. In such cases, most Internet services and therefore social media are not reachable, as the providers' servers are mostly located in the USA, such as it 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, while all users act as (passive) clients which simply use the service. These servers are single points of failures and are easy to intercept and to manipulate information. The NSA affair is current evidence that major Internet services like *Facebook*, *Yahoo* and *Twitter* which are all based on the client-server architecture, are well suited to being spied on. Edward Snowden revealed in 2013 how the NSA uses its PRISM program to investigate

packets traversing the Internet. The main argument has been that almost all information about the users of these services are 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 the communication being manipulated or overheard, 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, propose to alleviate the security and censorship risks of centralized online social networking sites. Two large trends have emerged in distributed social networking: private server approaches and peer-to-peer-based approaches. The private server approaches assume that users set up private web servers, connect them and create a distributed social network in this way. With this approach, central storage points are omitted and the control over the data remains with the users or their friends. Still, the risk of data misuse and censorship remains, as any web server may be compromised or shut down. Diaspora (diasporafoundation.org) is one prominent example of the private server approach. The project was initiated in 2010 by four students of New York University (NYU) who wanted to create a *Facebook*-like network that would be based on a decentralized structure and therefore control over user content would remain with its owners.

In contrast to the centralized server architecture, peer-to-peer-based online social networks like LibreSocial (libresocial.com), formerly known as LifeSocial (Graffi et al. 2010), came into focus a few years ago. Participants in a peer-to-peer network have basically equal rights and duties. User-related information is distributed and hosted among all participants in a network in a decentralized manner, without the need for dedicated servers. The peer-to-peer architecture is therefore suitable for data sharing or information dissemination without being stored on a central server. Users are expected to be only temporarily active in the network and permanently online servers are not assumed. 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, similarly to peer-to-peer networks. Thus, content is introduced by the participants and is spread directly between the users that are in contact with each other. In darknets, the set of potential contact partners of a node is highly restricted to trusted friends of that node. Strangers are not contacted, as they might misuse the information on the observed communication patterns, such as the question of what files were queried or served. Another characteristic of darknets is that single hosts are unable to be traced on the Internet since they are connected to friends in an arbitrary fashion without being registered on a search engine or any other central server. The motivation for private p2p networks, which is another term for darknets introduced by Rogers and Bhatti (2007), lies in their anonymity and privacy. While for regular social communication applications the actions of users can be traced, in a private peer-to-peer network users only com-

municate with their friends that are assumed not to be tracing them. The security of communication between the users can be further enhanced through encrypted communication between the nodes.

During the last few years the need for anonymous communication strongly evolved and led to the forming of three major kinds of anonymous peer-to-peer networks. In the first category communication paths inside the network are hidden from any interested eye. One common approach to provide anonymity in these networks is to apply multi-hop relaying. Nodes only forward chunks of data without knowing the identity of the originator and the destination node. When a query is sent out, it leaves a trail that is used to send the requested data item reversely hop by hop along the path of the request message. In addition, communication is encrypted to provide confidentiality.

Group-based networks in the second category assume that the set of users in the network is trusted. Anonymity is provided to the users only from entities outside the network. These networks are as trustable as the members invited to them. Here, the complete group is considered trustworthy, and the communication is encrypted with a group key. Using a shared group key and encrypted communication is a common approach to avoid the entities outside the network from gaining insight into the interactions in the network.

In friend-to-friend networks, connections are only established with selected trusted friends, and they act as trusted proxy routers of traffic for their friends. While in group-based approaches the whole group of participants is considered trustable and anonymity from outside attackers is sought, in friend-to-friend peer-to-peer networks in the third category, only a few friends are trusted, while the other members in the network are not trusted. A simple approach to form a friend-to-friend network is to connect only to friends, and thereby to establish an unstructured peer-to-peer network.

Encryption for hiding message contents, proxies for hiding communication traces, and decentralization to create self-operated, self-organizing communication networks, are the main viable ways for secure and private communication. These approaches typically are less user-friendly than the common centralized communication tools on the Internet. Encryption keys have to be managed, proxies operated, and complex protocols and their emerging effects have to be controlled. Since the security challenges of these solutions have for the most part been solved, the focus of the corresponding research community is shifting towards more user-friendly adaptations.

Influence of the Arab Uprisings on Computer Science

A sharp change in academic thinking within the field of computer science cannot be ascertained directly. Only selected subject areas within the academic section of computer science are affected by, or have themselves affected, the happenings during the Arab uprisings at all. Research on big data analysis has enabled the identification of communication patterns and topics in large networks, thus allowing the surveillance authorities to track down activists and limit the free flow of information. At the same time, research in the subject area of security and communication systems also reacted to

the happenings by providing a set of solutions for secure communications in the future. Although the immense communicational collapse during the revolutionary protests in the Middle East and North Africa cannot be seen as a trigger for a new era of technological thinking, the Arab uprisings are a modern example of small changes in the way the Internet is being used today.

The Snowden Affair, also known as the NSA Scandal or the PRISM Affair in 2013, probably has had more impact on the people in Europe and the USA than the Arab uprisings. People suddenly realized that they have been systematically monitored by a foreign agency and government. The threat moved closer. The way people were concerned about their privacy changed drastically. The technology used for communication purposes, however, still follows the well-known architectures.
One explanation for the fact that main trends in computer science have not changed due to single incidents such as the Arab uprisings is that the political revolutions did not lead to a technical revolution. After the uprisings in North Africa, no surprising new technologies or systems have emerged. All software and systems used or shut down during the Arab uprisings had been developed long before the civil riots began. Once again, a technical evolution seemed to precede a political revolution.

Social media and communication tools played a peculiar role during the Arab demonstrations. Many articles analyze the usage of social media platforms like *Facebook*, *Twitter*, etc. at that time, but only few analyze the technology behind those systems. Without going too deeply into detail, social media platforms are mostly based on technologies that had already been known for many years before the uprisings in the Middle East and North Africa took place. The most powerful change in those systems is the very simple way people can access social media nowadays. In contrast to the early days of the Internet, smartphones, tablets and computers, in combination with cheap and easy to use communication platforms, rule the Internet today. Modern-day usage of the Internet does not require special knowledge anymore. Anyone who is able to read and write is able to post his or her thoughts online in few milliseconds.

As we see, protests and demonstrations during the Arab uprisings were not driven by social media platforms themselves but by their users. It seems obvious now that cheap and easy-to-use platforms like *Facebook*, *Twitter*, *Google*, *YouTube,* etc. are gaining more and more popularity among most users of the Internet. Those systems are open to all users and the more they are used, the more they become interesting for other users that want to express themselves.

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

One of our anonymous interview partners described the problems with those tools, such as *Textsecure* or *Redphone* for 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).

It can be seen that although technical solutions exist to avoid security risks and massive censorship, most people do not possess the knowledge of how to use these techniques properly. Researchers are aware of this problem, and a user-friendly adaption of scientific solutions is more and more desirable.

The Arab uprisings are one good example to learn that social media often needs the right time and place to be used widely and to gain broader popularity. Nevertheless, those people using social platforms to express their feelings, to show pictures and share emotions define the platforms – not the other way round. It might be that the Arab uprisings constitute an important catalyst which pushes the development of free Internet, free communication, and all the necessary tools in the Middle East and North Africa. From a scientific point of view, however, it has had a rather small influence on academic research in computer science. In fact, it can be observed that the use of technology and social media in the Middle East and North Africa is a small part of a bigger process which might affect computer science and natural sciences as a whole. More and more people are affected by technology and even find pleasure in its use. Most users prefer those inventions that are easy to use, even if they are more unsecure. This change in costs, usability and design of technical devices might shift science to a new field that would combine the study of complex technology and human beings.

Besides scientific projects, there exist many community-driven projects that focus on the challenge of providing surveillance-robust systems for communication. The main characteristic of those projects is that source code and ideas are often shared in an open fashion. The development of such projects is transparent to any user and developer in order to avoid mistakes and security issues. The more people inspect a specific source code, the more possible security leaks or privacy-compromising vulnerabilities can be detected and avoided. Another side effect from open source projects is that the chance to distribute malicious code is reduced since users can inspect the code before its execution.

Computer science as an academic discipline might in the future become more and more interested in better understanding the change in social media platforms and their underlying technologies. In general, all natural sciences might diverge into different new areas of expertise that might also overlap with the existing fields. The reason is that different fields are growing faster and technology becomes increasingly complex.

Although the uprisings in North Africa have had only a small impact on computer science itself, they constitute a good impetus for stimulating and extending existing research questions, which is mainly happening in the subject areas of security and communications. However, the challenges of enabling secure and private communication are part of an old research area which is now being expanded with another real-life case of application. Best example is an article written by Kelev Leeraru (2011), in which he describes how computational analysis could have been used to forecast the revolutions in the Middle East and North Africa. Big Data and computational analysis is an up-and-coming research field in which the Arab uprisings could play an important role as a case study that can be used to teach new self-learning analysis methods and machine learning algorithms to produce better predictions about political unrest in the future.

Instead of changing technology itself, political unrest such as the Arab uprisings changes the usage of technology both for civilian populations as well as for political agencies and governments. The Arab uprisings have been a great example for demonstrating the lack of knowledge about the Internet and correlating technology that most regimes had and still have. Governments still have to learn about the relatively new media and how to use the Internet for their strategic purposes. Shutting down 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 a heavy use of modern communication platforms by its citizens. Quite the contrary, it seems that the governments in the region shut down all communication paths on the Internet as an act of panic due to the immense loss of control they had experienced.

Another immense problem that will likely remain is the commercialization of the Internet. As long as large parts of the Internet are maintained by organizations or companies that are bound to a given regime's despotism, it will likely occur that Internet Service Providers will be forced to block content or access to the Internet. Current research trends like peer-to-peer networks or darknets are still rarely used in practice. Decentralized services, for example, benefit from their distributed data structure if we consider terms of privacy, efficiency etc., but suffer on the other hand from insufficient technical controllability which defines challenges for the inclusion of new participants and the technical maintenance of certain quality levels. The decentralized nature further seems to frighten many companies or Internet Service Providers from putting effort into the development of further peer-to-peer networks. In other words, most companies are not interested in maintaining systems that cannot be controlled since their business models require a larger emphasis on usability and practicability of the secure solutions. This circumstance brings an open-source community together which is usually willing to provide own solutions to overcome the aforementioned drawbacks without the need to emphasize a monetary utilization. Challenge of these communities, as in many other cases, is how to finance their work. Which brings us back to the topic of commerce again.

Conclusion

The techniques and systems described in this article, which aim to battle surveillance and censorship, have not been developed out of an urgent necessity. All techniques and systems, like encryption, the *Tor* project, *LibreSocial*, as well as all attacks we have described, had been developed before the Arab uprisings and their revolutions came up. Neither the methods to block the Internet access, nor the solutions against the blocking, evolved during the process of the Arab uprisings. Rather, these events have been used by academia to highlight the relevance of their previous results in the context of new political events.

The process of shutting down the Internet completely had happened before in Myanmar in 2007 and Nepal in 2005. Years after the events of the Arab uprisings, other countries are still blocking and monitoring specific services on the Internet. Turkish Internet Service Providers, for example, still frequently block the access to *Twitter*, *Facebook* and other social networks. On July 22, 2015, after a suicide attack in Suruc, Turkish ISPs blocked the online social networking service *Twitter*.

Technology mostly affects people using it. The truth is that each region in the world is connected through the Internet, and the flow of ideas finds a way. Ideas might carry the spark of revolution, as they display other, potentially better, realities. Eric Schmidt, former CEO of *Google* 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 for a certain time the flow of information can be blocked, the speakers punished and the information falsified, technology worldwide progresses nevertheless, and new ways of secure communication will come up. 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, UK: Springer, 20-35.

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

Cowie, Jim (2011b): 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: 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: http://www.independent.co.uk/life-style/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/.