GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

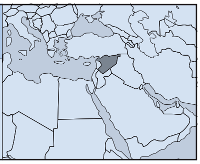
This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

SYRIA



Circumventing surveillance of internet communications

Karim Bitar

Introduction

Hardly a day passes without news about the conflict in Syria making headlines. After more than three years of clashes, the death toll is estimated to have exceeded 150,000.[1] Since the early days of the uprising, the government has imposed strong restrictions on foreign media coverage of the events, granting access only to reporters who share its side of the story.

Under such restrictions, it would be expected that the opposition would turn to citizen journalism to provide coverage of the events from its perspective. Many initiatives were started for this purpose, using mobile phone cameras to record and document events, and broadcast this footage to the world through the internet.

With the internet becoming the only viable medium for communication, the issue of the government's ability to intercept, block and exploit the communications of the opposition becomes a major challenge. Citizen journalists and activists had to find creative measures to circumvent government surveillance and protect their communications.

In the following sections of this report, I investigate a major project implemented by the Syrian government to intercept and trace all the digital activities and communications of its citizens. I also explore the tools and techniques developed by Syrian citizens to bypass the government's intrusive eye, and regain their privacy.

Policy and political background

Surveillance of citizens' communications is not new in Syria. While it has certainly intensified in scale and scope over the past four years, government surveillance has been a dominant theme in the country for decades, pre-dating the internet and digital communications. While the Syrian Constitution protects freedom of expression, and guarantees the privacy of all communications of the country's citizens, the government does not seem to be too concerned about that.

Syria was ruled by a state of emergency law from 1963 to 2011.[2] This law severely restricted personal liberty and freedom of expression. The massive secret services organisation established shortly after ensured that the red lines were clearly drawn, and those who crossed them were duly punished. As a result, Syria became the 177th country (out of 179) on the Reporters Without Borders' 2014 Press Freedom Index,[3] and was given the "worst of the worst" title by Freedom House in 2014 for achieving the lowest possible ratings on all criteria in political rights and civil liberties.[4]

This explains the internet's delayed entry into the country, since an open, international and difficult-to-control communication medium could undermine the establishment and lead to situations the government may not tolerate. Over time, the government realised that it could use the exact same technology to expand the scale and scope of its traditional surveillance activities, and it soon acted to make mass surveillance of digital communications the new reality.

Pervasive surveillance in the digital age

In late 2011, an Italian telecommunications company, Idea SpA, was caught in the midst of an unsettling controversy: the company was installing surveillance equipment in Syria that would enable the government to intercept every single email and internet communication that flows through the country.[5]

The leaked details of the deal, which are highly credible given the details they cite, indicate that the installed system would use deep packet inspec-

[1] Evans, D. (2014, April 1). Death toll in Syria's civil war above 150,000: monitor. *Reuters*. www.reuters.com/article/2014/04/01/us-syria-crisis-toll-idUSBREA300YX20140401

[2] Marsh, K., & Black, I. (2011, April 19). Syria to lift emergency rule after 48 years – but violence continues. The Guardian. www.theguardian.com/world/2011/apr/19/syria-lift-emergency-rule-violence

[3] Reporters Without Borders. (2014). World Press Freedom Index 2014. rsf.org/index2014/data/index2014_en.pdf

[4] Freedom House. (2014). Freedom in the World 2014. freedomhouse.org/report/freedom-world/freedom-world-2014

[5] Elgin, B., & Silver, V. (2001, November 3). Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. Bloomberg. www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html

tion to analyse the content of all traffic that travels through the country's national public data network (PDN). The national PDN constitutes the digital communications backbone for the whole country, and all traffic – for internet service providers (ISPs), banks, voice over IP (VoIP), etc. – passes through its infrastructure. This would give the installed surveillance system comprehensive access to all digital communications in the country, and the leaks of the deal confirm that Idea SpA was training local personnel on operating the system's monitoring and tracing capabilities.

While Idea SpA used some of its own technology to integrate the system, it also implemented several components from other hardware and software vendors, including US company NetApp Inc., French company Qosmos SA, and German company Utimaco Safeware AG. These companies were quick to announce that they were unaware that their products were shipped to Syria, and that they were acquired locally in Italy. This raises serious questions about the effectiveness of export control regulations for surveillance gear, and how easily such regulations can be circumvented.

A primary concern for surveillance projects like this is the argument that the government can use them to hide its intrusive surveillance activities under the "lawful interception" of citizens' communications for law enforcement purposes. In fact, that is precisely the claim stated by Idea SpA's CEO in responding to the criticisms of his firm's involvement in the project.

What those who adopt this argument fail to mention, however, is that "lawful interception" is tightly governed by checks and balances to ensure all activities are performed in accordance with the country's constitution and applicable laws. This includes, for example, the need for a court warrant that is only issued after due legal process. The secrecy surrounding this project, and many similar others, makes it impossible to verify its compliance with these requirements.

Another argument used to justify mass surveillance is that "everybody else does it". With the recent revelations on mass surveillance programmes in the United States, the United Kingdom and other countries, even established democracies were caught in the act of invading the privacy of their citizens and those of other countries, despite long traditions of freedom of expression and privacy protection. If it is so easy to bypass the constitutional guarantees and secretly intercept citizens' communications in these countries, how can much less democratically developed countries be expected to set a better example?

The problem is actually compounded for citizens of the latter, since they are subjected to several layers of spying and surveillance. At one level, their governments are engaging in intrusive, large-scale interception and surveillance of their communications. On another, they are subjected to foreign surveillance from countries other than their own. It is not unrealistic to imagine this turning into a global overlapping "spaghetti" of surveillance programmes where everyone is spying on everyone else.

In such a distrustful environment, it can be very difficult to even track who is doing what. For example, the recent story of the US National Security Agency (NSA) bugging telecommunications equipment while in transit to its users without the knowledge of the equipment's vendors themselves is a startling example. That story sparked global outrage among customers of US technology companies, and prompted John Chambers, CEO of Cisco Systems Inc., to send a carefully worded letter to President Barack Obama complaining against these acts.[6]

So how are people in Syria dealing with this ubiquitous surveillance of their everyday digital activities? History has taught us that humans have an amazing ability to adapt to their environment and develop creative solutions to overcome the challenges that come their way. Syrians are no exception.

In addition to many awareness raising campaigns and educational activities, such as the Amenny (Secure Me) Digital Awareness Week[7] (which includes training courses on securing digital communications, erasing trails, awareness videos, and tips on how to use online security tools), a team of Syrian technology professionals developed a specifically designed distribution of the Linux operating system called Virtus Linux to enable users to easily hide their tracks and communicate without fear of the eyes of the person-in-the-middle (or, probably more accurately, people-in-the-middle).[8]

Another approach usually used by Syrian citizens to avoid surveillance is to develop "code language", using agreed upon substitutes for suspicious words and sentences in daily communication. Actually this practice was so widespread that some substitute phrases became famously known for their concealed synonyms. For example, most Syr-

[6] Bort, J. (2014, May 19). Cisco CEO Writes Letter To Obama Asking Him To Stop The NSA Hacking Into His Equipment. Business Insider. www.businessinsider.com/cisco-ceo-letter-to-obama-about-nsa-2014-5

[7] https://www.facebook.com/events/305539792943989/?ref_newsfeed_story_type=regular

[8] internetfreedomfh.strutta.com/entry/426472

ians understand that "he is visiting his aunt" refers to someone who has been arrested or put in prison.[9]

While this code language started offline, aiming mainly to disguise information from "the guy next door", it quickly integrated in the digital communications fabric, now hiding information from "the guy on the wire".

On top of the code language, and several layers of encryption and secure communications, Syrian activists became masters in the art of concealment. They skilfully separated their online identities from their actual selves, using techniques such as pseudonyms and fake friend lists on social networking sites like Facebook and Twitter. These techniques were constantly updated as activists learned about the government's methods for tracking them.

By using such techniques, many activists have successfully overcome the government's elaborate surveillance efforts, limiting their effectiveness to tracking the "naïve" who have not yet acquired the skills to hide their communications. Interestingly, as awareness increases and privacy and security knowledge and tools become widely available and easily accessible, the "naïve" group has started to shrink, as everyone wants to feel in control of their privacy.

But increasing awareness of the privacy violation of mass surveillance activities does not only lead to higher adoption of security tools and techniques; it can also bring about dramatic policy change. For example, following the sustained media focus and reporting on leaks exposing details of some of the US government surveillance programmes, the US Congress moved to limit the NSA's mass surveillance programme.[10] The fact that many US-based companies took swift action to tighten privacy and security controls in their systems, fearing for their market share both locally and internationally, was undoubtedly a factor that was taken into consideration.

While such policy change is possible in established democracies, it would be much more difficult in totalitarian countries. So how could awareness and grassroots movements affect change in countries like Syria? For one, they can lead to tighter export regulations for surveillance solutions so that they are only imported to countries where rule of law is respected. Export regulations can also require assurances that such systems will be solely used under the responsibility of appropriate judicial process.

Conclusions

Information and communications technologies (ICTs) have been a transforming power for the economy, education, development and politics. While many benefits can be cited for ICTs, they have had a major unfortunate consequence: they made it much easier for governments and other agencies to spy on people's communications and activities, both inside and outside their state borders.

While some governments tried hard to resist the adoption of ICTs in their countries, fearing their powerful transforming powers, they eventually realised that these technologies can be used to counter their very own effects in facilitating the free flow of information.

Syria was very late in adopting most new ICTs, mostly because of the fears cited above. However, the government later realised that instead of pushing back, it can actually utilise these technologies to both deepen and widen its surveillance programmes. The project mentioned in this report is but one example that was leaked to the public, and it would be difficult to assert that it is the only existing project. In fact, some reports suggest that other Western companies may have been providing similar equipment to the Syrian government.[11]

There is a difference, though, between offline and online surveillance: while avoiding offline surveillance usually forced people to stay silent or talk in very small circles, online surveillance can be circumvented with some awareness, techniques and accessible tools. That is precisely what happened in Syria, where the citizens' response to the massive surveillance programmes was to intensify awareness campaigns and develop technical tools to ensure that people can still communicate and express their opinions without being caught by the government's expensive surveillance and tracking systems.

But technical approaches are only part of the solution. Policy making is also an important factor. Unfortunately, advocacy efforts for policy change on such sensitive topics in Syria are doomed to yield limited results. Despite the protections afforded by the constitution, several laws were enacted

[9] Friedman, J. J. (2013, October 6). In Syria, code language defies surveillance. The Boston Globe. www.bostonglobe.com/ideas/2013/10/06/syria-code-language-defies-surveillance/1c18bNgxlIkqoCElLi1eYM/story.html

[10] Roberts, D., & McVeigh, K. (2014, May 22). NSA surveillance reform bill passes House by 303 votes to 121. The Guardian. www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house

[11] Spiegel Online. (2012, April 11). Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria. Spiegel Online. www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html

to restrict privacy and grant several government agencies the right to intercept, track and monitor citizens' communications. Still, activists and human rights organisations can advocate for higher accountability for companies providing mass surveillance systems, and for better enforcement of export regulations for these systems. However, under what appears to be a global government attack on personal privacy, seeing the fruits of these efforts seems to be a rather long shot. In fact, the failure of the Global Online Freedom Bill, proposed to the US Congress in 2011 to ban sales of US surveillance gear to undemocratic countries, is a recent testament.[12]

Action steps

Despite the increasing efforts to invade privacy and deprive people of personal liberties, several mitigation approaches exist to counter these efforts and reduce their effectiveness. The first step is increasing awareness of the extent of such mass surveillance efforts and their subsequent risks. Sufficient awareness among global citizens will lead to higher adoption of readily available technical tools that circumvent most of these surveillance efforts and restore confidence in the privacy of digital communications.

Advocacy for policy changes will certainly be needed to create a lasting effect and reduce the need to take sometimes cumbersome technical measures. Policy change is mostly possible in countries with established democracies with a history of relative response to public opinion. Unfortunately, such change is unlikely to happen in countries with less democratic governments. However, the moral responsibility towards citizens in these countries mandates that other options be pursued on the international stage, such as imposing and enforcing appropriate trade sanctions to ensure that capable mass surveillance systems will not be unlawfully abused by governments with a known track record in human rights abuse.

[12] beta.congress.gov/bill/113th-congress/house-bill/491