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

From digital threat to digital emergency

Fieke Jansen
Hivos, the Digital Defenders Partnership
www.digitaldefenders.org

Introduction

In recent years there has been a crackdown on internet freedom and increased targeting of the communication of journalists, bloggers, activists and citizens. During times of social or political crisis, communication lines have been shut down and critical forms of expression are met with censorship, harassment and arrests. Our communication is under surveillance, intercepted and collected without our knowledge or active consent, and is used for the profiling of people and spying on networks by governments and commercial companies. These acts of censorship and targeted surveillance are undermining our freedom of speech and our basic human rights, and lead to digital emergencies for those who are targeted. In this fast-changing political and technological environment there is an urgent need to understand the risks, protect those critical internet users who are being targeted, and expose surveillance practices.

Challenges, threats and digital emergency

The first time people started uttering the term "digital emergency" was when former Egyptian president Hosni Mubarak pulled the internet kill switch during the protests in 2011, leaving Egypt without internet communication.[1] However, digital emergencies are not only related to an internet kill switch: for the Digital Defenders Partnership[2] a digital emergency is an urgent need for assistance arising from digital threats to the security of an individual or organisation. A digital threat can include cyber attacks, vulnerabilities to communication infrastructure, unsafe data use, compromising of devices, stealing of equipment, legal proceedings or weak digital security practices. There are three levels at which to distinguish digital attacks and communication surveillance that can lead to a digital emergency: infrastructure, censoring of content and profiling of people.

Infrastructure

Communication is often referred to as the interaction that happens between people, a stream of words whether they take place on- or offline. Yet very few of us realise that all digital communication runs on a physical communications infrastructure that consists of several "layers" made, owned or operated by different commercial and state entities. The Open systems interconnection model distinguishes seven different layers in the internet architecture that range from the physical layer (e.g. copper and fibre optical cables) up to the application layer (e.g. https and email protocol).[3] Depending on a state's technical capabilities, access to the infrastructure, as well as to service providers, surveillance and censorship methods may differ. In some cases a government can engage in sea-cable tapping, which requires direct access to the physical infrastructure layer, or use an application layer exploit, where internet or mobile traffic is monitored through exploiting a vulnerability in the transport layer encryption (https), as in the case of Heartbleed.[4] Partial network interference, called throttling, is also possible.

The fact that infrastructure is made, owned or operated by different entities makes our communication vulnerable to censorship and surveillance. Since Mubarak pulled the internet kill switch in 2011, other mobile and internet blackouts in Pakistan, Syria and other places have become more visible. These usually take place in times of military, political or social unrest.[5, 6]

[1] AlJazeera. (2011, January 28). When Egypt turned off the internet. *AlJazeera*. www.aljazeera.com/news/middleeast/2011/01/2011128796164380.html

[2] Digital Defenders Partnership, a programme that aims to mitigate digital threats to human rights defenders, bloggers, journalists and activists in internet repressive and transitional environments. https://digitaldefenders.org

[3] https://en.wikipedia.org/wiki/OSI_model

[4] The Heartbleed bug. heartbleed.com

[5] Article 19 (2012). Pakistan: Government must stop 'kill switch' tactics. Statement by Article 19. www.article19.org/resources.php/resource/3422/en/pakistan:-government-must-stop-%27kill-switch%27-tactics

[6] Franceschi-Bicchierai, L. (2013, August 29). Does Syria Have an Internet Kill Switch? *Mashable*. www.mashable.com/2013/08/29/syria-internet-kill-switch

In April 2014 the Heartbleed vulnerability, a critical flaw in OpenSSL, was discovered. As one analyst put it: "[OpenSSL] is a software which is used to secure hundreds of thousands of websites, including major sites like Instagram, Yahoo, and Google. This security exploit can give attackers access to sensitive information like logins and passwords, as well as session cookies and possibly SSL keys that encrypt all traffic to a site."[7] Other than the security hole there were two major problems with Heartbleed. The first was that the National Security Agency (NSA) in the United States knew about this vulnerability for at least two years and used it to intercept communication traffic instead of fixing this global security problem.[8] Secondly, after the vulnerability was discovered, the bigger internet companies fixed the problem quickly while internet companies with less security expertise lagged behind, leaving their clients vulnerable for a longer period of time.

It is important to realise that Heartbleed is only one example of a vulnerability used for monitoring of communication. At the end of 2013 the German newspaper *Der Spiegel* reported on the NSA's Tailored Access Operations unit (TAO). *Der Spiegel* uncovered that TAO has multiple methods to intercept communications between people, which required them to install backdoors on, among others, internet exchange points (IXPs), internet service providers (ISPs), modems, computers and mobile phones. To increase the ability to intercept communication traffic the NSA chose to compromise the security of the entire internet and mobile infrastructure for intelligence purposes.[9, 10] Both Heartbleed and Tailored Access Operations are examples of the government using infrastructural vulnerabilities for surveillance instead of fixing the problem, leaving us all more exposed to exploitation.

Censoring of content

States have different ways to censor content; technical blocking, search result removal, take-down of content and induced self-censorship.[11] Technical blocking can target specific websites, domains or IP addresses, or use keyword blocking which automatically looks for specific words and blocks access to websites where these keywords are found. Government can also request the blocking of specific search results. Google's transparency report states: "Governments ask companies to remove or review content for many different reasons. For example, some content removals are requested due to allegations of defamation, while others are due to allegations that the content violates local laws prohibiting hate speech or adult content."[12] Take-down of content is used when states, companies and others can demand the removal of websites or content through the court.

However, in the last two years we have seen other ways in which non-state groups use the terms and conditions of social media platforms to take down content. Syria activists believe that the Syrian Cyber Army, a collection of computer hackers who support the government of Syrian President Bashar al-Assad,[13] is using Facebook's terms and conditions to take down content published by the Syrian opposition. Facebook's community standards are guidelines to protect the community and do not allow content that can be described as graphic content, nudity, bullying and more.[14] If a user believes that a post on Facebook violates these terms they can report it as abuse, which is called flagging. The Syrian Cyber Army is allegedly using this complaint procedure to flag content which shows human rights violations by the Syrian regime as inappropriate and graphic content, after which it can be taken down.[15] This is particularly problematic since the Syrian opposition moved to social media after a crackdown on the traditional media – and the country's citizens.

There are also cases where a state does not need to have legal jurisdiction over social media sites to request the take-down of content. In May 2014 Twitter censored tweets in Russia and Pakistan. In the case of Pakistan, Twitter caved in to pressure from the government to censor specific tweets that were deemed blasphemous or unethical. In Russia, Twitter took down the content of a Ukrainian

[7] Zhu, Y. (2014, April 8). Why the web needs perfect forward secrecy more than ever. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy

[8] Riley, M. (2014). NSA said to have used Heartbleed bug for intelligence for years. *Bloomberg.* www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

[9] Appelbaum, J., Horchert, J., & Stocker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel.* www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[10] Appelbaum, J. (2013). To Protect and Infect: The militarization of the internet. Presentation given at the 30C3, Hamburg, Germany, 29 December. https://www.youtube.com/watch?v=vILAlhwUgIU

[11] https://opennet.net/about-filtering

[12] Google. (2014). *Transparency report: Requests to remove content.* https://www.google.com/transparencyreport/removals/government/

[13] https://en.wikipedia.org/wiki/Syrian_Electronic_Army

[14] https://www.facebook.com/communitystandards

[15] Pizzi, M. (2014, February 4). The Syrian Opposition is Disappearing From Facebook. *The Atlantic.* www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562

Twitter account which, according to Eva Galperin of the Electronic Frontier Foundation (EFF), is "plainly political... These actions are highly problematic as independent media in Ukraine is increasingly under attack."[16] In both countries, Twitter does not have formal representation and there is no legal jurisdiction over the service, yet still the service providers complied with government requests.

Profiling of people

Much of our behaviour is already leaving digital traces – even actions that seem as harmless as walking down the street. Traffic and surveillance cameras are monitoring us, our mobile phones are registering our whereabouts every moment of the day and we voluntarily post our private lives on public proprietary platforms. This might seem innocent at first, but there have been numerous instances where a mobile phone has been used to locate someone, and online behaviour and information are used for profiling.

During the protests in Ukraine in the beginning of 2014 a collective message was sent to mobile phone users near the scene of violent clashes in Kiev: "Dear subscriber, you are registered as a participant in a mass riot," it said.[17] In the end the protestors toppled the regime of ex-president Viktor Yanukovych, yet the records of who was near the square still remain. Mobile phone companies have the capabilities to track and collect the following information on you through your phone: phone calls, text messages, data services you use, and your approximate location, and may share that information with the government. A mobile is a goldmine of information: your phone book with all your contacts in it, call history, text messages, locations and previous locations, data from any application you are using, and photos and videos. In addition, governments and phone companies can see which phones are close to yours, which other "people" or phones are in the room.

Regimes have also used malignant viruses to profile political actors and their networks. The most well known cases are of the commercial malware Hacking Team[18] and FinFisher[19] that were – and might still be – deployed in countries like Ethiopia, Bahrain, Mexico and Turkmenistan. Privacy International published one of FinFisher's brochures, which states: "The product is known as FinFisher and is delivered onto computers, it then harvests information from the computer, from passwords and web browsing sessions, to Skype conversations. It can even switch on a computer's webcam and microphone remotely."[20]

Challenges

In mitigating these different threats there are a number of challenges we have encountered, specifically when you approach censorship and communications surveillance from a human rights defenders or journalist perspective.

The majority of digital threats are invisible and abstract. While a virus on your computer or phone can grant someone access to your physical surroundings by turning on the camera or microphone, we do not see it and therefore the threat remains abstract. The second challenge is that secure communication is always a trade-off between security and convenience. Security measures are seen as cumbersome and a distraction from the priorities of the day. When in the trenches, short-term wins and threats are more pressing then the intangible nature of communications surveillance and long-term exposure – especially when installing and using certain tools can be more inconvenient and time consuming than using unsecure communication methods.

When a digital emergency happens, it is difficult to know where to turn, who to ask for help and how to solve the problem. Very few organisations have done work on the prevention of digital emergencies. If we live in an earthquake-affected area, we have flashlights, water and emergency plans ready; but even with all the knowledge of different digital threats and communication surveillance, similar contingency plans to mitigate digital threats are few and far between. If NGOs, human rights defenders or media organisations recognise

[16] Galperin, E. (2014, May 21). Twitter steps down from the free speech party. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/05/twitter-steps-down-free-speech-party

[17] Walker, S., & Grytsenko, O. (2014, January 21). Text messages warn Ukraine protesters they are 'participants in mass riot'; Mobile phone-users near scene of violent clashes in Kiev receive texts in apparent attempt by authorities to quell protests. *The Guardian.* www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

[18] Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014). *Hacking Team and the Targeting of Ethiopian Journalists.* Toronto: The Citizen Lab. https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists

[19] Marquis-Boire, M., Marczak, B., Guarnieri, C. & Scott-Railton, J. (2013). *For Their Eyes Only: The Commercialization of Digital Spying*. Toronto: The Citizen Lab. https://citizenlab.org/2013/04/for-their-eyes-only-2

[20] https://www.privacyinternational.org/sii/gamma_group

the problem and want to increase their security, they have few funds to spend on prevention or do not know where to start. There is a lack of technical knowledge and skills in the human rights and media community.

How can you mitigate the threats and where do you find support?

There are a number of ways to be more prepared for a digital emergency as an individual or organisation. Prevention is key: try to increase the overall digital security awareness and practices of your organisations,[21] establish a relationship with a technical person you trust and can turn to for immediate advice, make a thorough threat analysis, and establish some protocols and procedures in case you are targeted. If you think you are suffering a digital attack, turn to a trusted technical expert or international organisation or make a self-assessment.[22]

Conclusion

The field of digital emergency support for human rights defenders, journalists and bloggers around the world is still emergent. The intangible nature and rapidly changing technical environment makes it difficult to mitigate digital threats. It is crucial to understand what the different threats are and work on prevention. If you are in the midst of a digital attack, turn to a trusted technical expert or international organisation for support.

[21] Tactical Tech Collective and Front Line Defenders, Security in a Box https://securityinabox.org/ and Electronic Frontier Foundation, Surveillance Self-Defense https://ssd.eff.org/risk

[22] Digital First Aid Kit digitaldefenders.org/wordpress/launch-of-the-digital-first-aid-kit or on GitHub https://github.com/RaReNet/DFAK