POLICY AND PRACTICE NOTE

Rethinking Risk and Security of Human Rights Defenders in the Digital Age

STEPHANIE HANKEY AND DANIEL Ó CLUNAIGH*

Abstract

Human rights defenders (HRDs) are increasingly empowered by, and dependent upon, digital technologies. These technologies have opened up new potentials, enabling HRDs to extend their capacity to document and analyse human rights abuses, to amplify them, and to more effectively organize locally and internationally. Digital technologies, however, have simultaneously created new points of weakness: exposing HRDs' whereabouts, activities and networks, and creating evidence against them through data leakages, digital traces, and direct surveillance and interception. Attacks on HRDs have escalated over the past two years, with a significant increase in the number of entrapments and networks being compromised through the use of computers, cameras, mobile phones and the internet. This rapidly changing landscape poses a number of challenges to practitioners working in the field of security and protection for HRDs and has led to a growing concern about how best to enable HRDs to assess and mitigate the related risks. After contextualizing and introducing the dimensions of digital insecurity for HRDs, this paper will note some of the responses to HRDs' digital security needs which have been developed, and their limitations. It will then go on to identify three key principles that should inform the work of practitioners in future and to raise a series of critical questions for further research and work in this area.

Keywords: capacity building; digital security; encryption; privacy; protection; surveillance

1. Introduction

Human rights defenders (HRDs) are increasingly empowered by, and dependent upon, digital technologies. These technologies have opened up new potentials, enabling HRDs to extend their capacity to document and analyse human rights abuses, to amplify them, and to more effectively organize locally and

* Stephanie Hankey co-founded the Tactical Technology Collective (Tactical Tech, https://tacticaltech.org; ttc@tacticaltech.org) in 2003; since 1998 she has worked to strengthen information activism and reduce limits to freedom of expression online. Daniel Ó Clunaigh has carried out research and advocacy on the security and protection of human rights defenders at an international level, as well as grassroots human rights observation, protective accompaniment and training, and at Tactical Tech contributes to digital security materials and trainings for human rights defenders.

Journal of Human Rights Practice Vol. 5 | Number 3 | November 2013 | pp. 535–547 DOI:10.1093/jhuman/hut023

internationally. Digital technologies, however, have simultaneously created new points of weakness: exposing HRDs' whereabouts, activities and networks, and creating evidence against them through data leakages, digital traces, and direct surveillance and interception.

Attacks on HRDs have escalated over the past two years, with a significant increase in the number of entrapments and networks being compromised through the use of computers, cameras, mobile phones and the internet. This rapidly changing landscape poses a number of challenges to practitioners working in the field of security and protection for HRDs and has led to a growing concern about how best to enable HRDs to assess and mitigate the related risks.

After contextualizing and introducing the dimensions of digital insecurity for HRDs, this paper will note some of the responses to HRDs' digital security needs which have been developed, and their limitations. It will then go on to identify three key principles that should inform the work of practitioners in future and to raise a series of critical questions for further research and work in this area.

2. The dimensions of digital insecurity for human rights defenders

2.1 The importance of information and communications in attacks against human rights defenders

In spite of the legal recognition of the legitimacy of the work of HRDs at international and, in many cases, regional and national level, their physical and psychological integrity, liberty, and in some cases even their lives are put at risk as a result of their work. In carrying out their activities, HRDs incur the ire of different social actors in various ways; their actions often pose a direct threat to powerful interests who are willing and—all too often—able to constrain or terminate their work. It is not only those directly involved in the promotion and defence of human rights who face risks as a result of such work; family members, friends, associates and supporters of HRDs are often also the targets of such attacks (see UN Human Rights Council, 2009, 2010, 2011).

The central role that information and communications play in HRDs' work is often the object of control and harassment by adversaries. This includes direct surveillance and intelligence gathering for the purposes of monitoring HRDs' actions, contacts and networks; using information gathered as evidence against HRDs and their organizations; more manipulative forms of information misuse such as entrapment or the circulation of misinformation; and direct interventions in access to and circulation of information by HRDs such as blocking and censoring web-based content.

Whilst the scale and dimensions of threats to HRDs' information and communications in the digital age are unique, the manipulation of information and communications surrounding HRDs is not new.

Information and communications have always been weak spots vulnerable to exposure, litigation or retaliation and key assets in intelligence gathering and in maintaining control or asserting power. For these reasons, they remain central targets for adversaries. Over the past century, we have seen this approach played out within significant civil society movements and opposition movements, from the African-American civil rights movement in the United States to pro-democracy dissidents in Eastern and Central Europe, and from the 'Dirty War' in Argentina to anti-apartheid activists in South Africa. In each of these cases, exposure, entrapment and intimidation through HRDs' use of information and communications has been a key technique of control.

We will not seek to fully draw out historical parallels in this paper, but it is useful to briefly put the issue of information and communications vulnerabilities of HRDs into perspective in order to recognize that information flows have always been—and probably always will be—a key target for those interested in undermining the work of HRDs. In turn, there has often been a creative response to subvert these controls, often thanks to the creativity, innovation and perseverance of those targeted (see Meier, 2008). There has also always been a close link between the role of information in physical threats to HRDs and techniques for psychological intimidation and control. In this sense, many of the threats emerging in the digital age that seem new are simply extensions and expansions of well-established practices for the control and curtailment of freedom of expression, association and assembly. This fact can help us to reflect on current risks and trends and better understand the status quo so as to map its potential trajectory and seek possible solutions. Understanding this history can also ensure that those of us working as practitioners in the field to enhance the digital security and protection of HRDs not only concentrate on the unique and complex technological challenges of the present but learn from the responses of the past.

2.2 The specifics of digital security and privacy threats to human rights defenders

Simultaneously, putting current threats to HRDs into historical relief can also play an important role in helping us recognize which threats are established practices which have been extended into the digital sphere and which ones are new.

Along with the increased ease of use of digital technologies, we have witnessed an increase in the quantity of information exchanged and the frequency of communication and coordination among HRDs, their networks and their constituencies—particularly in repressive societies. This has, in-step, led to new methods for tracking and controlling HRDs' information and communications through mechanisms that have been claimed by some to be 'doing the work of the intelligence services for them' (Morozov, 2011), leading to what is often referred to as a 'cat and mouse game'[1] or an 'arms race'. The speed and scale at which this is happening, as well as the relatively limited resources required to stay on top of this intelligence, is unprecedented. This is, in part, evidenced by the mushrooming surveillance technology industry, now commonly thought of as the new arms trade.[2] This is not all about passive monitoring, however; there are a growing number of reports of adversaries using digital technologies to undermine HRDs. This can be seen in the increased number of Distributed Denial of Service (DDoS) attacks against independent news sources, HRDs and activists (Berkman Center, 2010) and in efforts to lure activists or would-be activists into actions that will then be used against them. In Ethiopia, for example, phishing attacks have entrapped activists downloading fake opposition videos, as was reported in the *New York Times*, summarizing the findings of the Citizen Lab report (2013) on spyware:

> In Ethiopia, FinSpy was disguised in e-mails that were specifically aimed at political dissidents. The e-mails lured targets to click on pictures of members of Ginbot 7, an Ethiopian opposition group. When they clicked on the pictures, FinSpy downloaded to their machines and their computers began communicating with a local server in Ethiopia. (Perlroth, 2013)

HRDs are at a serious disadvantage in this game not only because of the unequal access to resources but also because of the asymmetry in the access to backdoors within the systems, devices and platforms they use.[3] Governments and law enforcement agencies—with greater or lesser effort depending on the country—can not only request that information be taken down from platforms and services such as Google or Twitter, but can also gain access to information about users through their control of in-country Internet service providers (ISPs) or mobile phone network providers, and the significance of mobile phone monitoring in exposing HRDs and controlling their actions should not be underestimated.

As digital technologies become ubiquitous they also become part of the regular working practices of most HRDs. Notable examples include social networking and media sites such as Facebook, YouTube, Skype or Twitter. The paradox is that as technologies become easier to use, they become increasingly difficult to control, thus reducing the number of end-users with the expertise to

[1] This is an expression used repeatedly in the media but also by researchers and commentators in the field. For example, see Jillian York from the Electronic Frontier Foundation (York, 2010).

[2] See Privacy International's project 'Big Brother', including news and a database of surveillance companies as well as details of who is selling to whom: https://www.privacyinternational.org/projects/big-brother-inc.

[3] See projects such as the Chilling Effect (http://www.chillingeffects.org) and the Google Transparency Report (http://www.google.com/transparencyreport), which other companies such as Twitter and Microsoft are now following as best practice.

understand how they work, where information is stored, what data is collected, and who has access to it. This is extremely problematic. As HRDs increasingly rely on mainstream tools due to their ease of use and broad reach, they also create 'honey-pots' (Doctorow, 2011) for those who wish to monitor and control them. What is often a frustrating level of opacity and lack of data control for an 'average' user becomes extremely dangerous in the context of a 'high risk' user such as a HRD working in a relatively closed society. Most of the risks to HRDs using these tools, though, tend to sit with the choices that HRDs make as users: the detailed information they submit to these services and therefore the potential for exposure they afford. In Syria, for example, a large number of activists were reportedly captured after some who had been arrested were forced to provide passwords for their accounts on Facebook and Skype, leading to the exposure of their networks (Freedom House, 2012).

The combination of these factors creates a complex topology of risk, a terrain which HRDs find increasingly difficult to navigate in an 'artful' manner. HRDs have always taken unavoidable risks; the problem comes when they lose their ability to assess and control them.

3. Digital security for human rights defenders and its challenges

3.1 The movement towards digital security for human rights defenders

The new threats and vulnerabilities faced by HRDs and others have not gone unnoticed by those who work to support civil society. Human rights support organizations, technologists, researchers and policy makers have developed different ways of approaching the problem, and working to develop solutions that are distinct but directly complementary. These are:

- *tool development*: specific digital security software tools, particularly Free, Libre and Open Source Software (FLOSS) communities;[4]
- *policy and research work*: research into exact vulnerabilities faced by HRDs and related policy, lobbying work with governments, regulators, service and platform providers;[5]
- *capacity building*: the development of awareness raising and skill building toolkits and guides for human rights defenders and digital security training,

[4] There are too many initiatives in this area to mention all, but to highlight a few: software tools which facilitate file storage and drive encryption using standards such as Advanced Encryption Standard (AES) (a popular example being TrueCrypt); communication encryption protocols including Pretty Good Privacy (PGP), released by Phil Zimmerman in 1991; GNU Privacy Guard (GnuPG), developed by Werner Koch in 1999; Off-the-Record (OTR); and anonymity and censorship circumvention tools such as Virtual Private Networks (VPN), or proxy networks such as The Onion Router (TOR) project.

[5] Key organizations include the Electronic Frontier Foundation, the Berkman Center at Harvard, the Citizen Lab within the Munk School of Global Affairs at the University of Toronto, the Oxford Internet Institute at Oxford University, and the Center for Internet and Society at Stanford University.

> particularly by non-governmental organizations (NGOs) which work to directly support HRDs and civil and political rights more broadly.[6]

In this regard, significant progress has been made over the past decade in the field of digital security for HRDs. This has included work that has transformed the sector's understanding of the problem, pushed back restrictions to freedoms online and provided solutions that have helped keep HRDs and their communities safe. However, there is much work that remains to be done. It is extremely hard for those working in different ways to keep up with the diverse range of fast-changing threats. The demand for such support often outstrips the level of response available, and shortcomings in the responses to what has become an extremely complex terrain are increasingly being identified. In particular, each of these approaches could greatly benefit from more information sharing and coordination.

3.2 Key challenges facing capacity building

Capacity building is an important aspect of efforts to push back threats to HRDs. This is partly because we cannot solely rely on technology to protect us from technology. Policy advocacy in relation to the rights to privacy, access to information, free expression and assembly—among many others—remains a vital element of the battle to protect HRDs and their work, particularly in light of recent revelations regarding widespread surveillance and data collection by the United States and United Kingdom intelligence services. However, whilst the efforts of researchers and policy makers are essential, they cannot move fast enough or reach far enough to protect individuals struggling with these issues on a daily basis.

For these reasons, we believe a significant amount of work in the area of capacity building is essential. This must develop through more grounded approaches informed by three important principles. First, we should not solely rely on fighting problems created by technology with more technology; second, we need to understand the role of behaviour when building capacity; and third, we need to move beyond a techno-centric approach to capacity building, embedding these issues within broader approaches to security.

3.2.1 The limitations of relying on technology to fight technology

In identifying the specific technical challenges facing HRDs above (section 2.1), we have already outlined why entering an 'arms race' is not an option for HRDs. Furthermore, in discussing some of the user choices that have served to entrap and expose HRDs—as in Syria—we have also highlighted why some of these challenges are not ones that can be solved with tools. Changing the ways

[6] A number of handbooks, manuals, websites, and visual materials attempt to demystify some of these complex issues. Examples include the 'Digital Security and Privacy for Human Rights Defenders' handbook (Vitaliev, 2007) and the 'Security in a Box' toolkit (https://securityinabox.org) developed by Front Line Defenders and Tactical Technology Collective under creative commons licences. A number of derivatives have subsequently been created.

technologies are used and the amount of information given are difficult but necessary.

This is not to deny that there are certain technologies that have been critical to fighting back and mitigating risks. These technologies are not only useful but often critical in enabling some HRDs to continue working in extremely difficult circumstances. However it is important to be realistic about the shield these technologies provide, given the context they are working in.

An inherent problem is that when security oriented technologies are effective, they often become the cause of significant concern to authorities. As a result, such technologies become the targets of crackdowns by authorities determined to keep HRDs firmly under the panoptical lens. Encryption algorithms remain subject to significant legal constraints in a number of countries: in some countries any use of Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG) is illegal, while in others authorities may demand that users hand over their private keys to facilitate a warranted search of their devices. HRDs are often on the back foot legally and the same governments restricting the use of these tools are investing significantly in the procurement of instruments designed to broaden the net of surveillance of civil society. This was further evidenced in 2011, when WikiLeaks released a series of 287 documents which partly exposed the extent to which governments—democratic or otherwise—have been investing in an array of technologies for surveillance, from simple packet sniffing tools to location and voiceprint tracking (WikiLeaks, 2011).

The resource gap is such that HRDs using these tools are likely to be always outgunned or stunted by legislative restrictions often facilitated by counter-terrorism laws. HRDs run the risk of drawing unwanted attention to themselves through the use of such technologies. When monitoring of email, chat or text message communications reveals the use of encryption technologies, digital threat can become a physical threat.

These observations certainly do not mean that these tools are not important. However, we may need to look outside of this frame to find strategies that can better inform the way we use these tools. In short, we need to make more effective choices about the services we use or don't use and the information we choose to give away.

3.2.2 Understanding the response and behaviour of human rights defenders in the context of capacity building

As essential as a less techno-centric response is in order for capacity building efforts to have traction, they also need to be designed with a deeper understanding of how HRDs are processing and responding to digital security risks. In February and March of 2013, Tactical Tech carried out interviews with 11 experienced security trainers who, over the past several years, have offered training worldwide in an attempt to begin to map these trends. These interviews identified some initial common patterns among HRD recipients of digital security advice and training, which, while deserving further investigation, are explored only cursorily below.

When asked to elaborate upon the challenges that trainers face in transferring knowledge, the following common issues were noted:

- *Lack of time*: Trainers identified the time demands of learning and integrating digital security practices as being too great for some HRDs, who are already overworked and unable or unwilling to take the necessary time for this.
- *Defeatism and 'martyrdom'*: Trainers identified an attitude of defeatism among a number of HRDs who, exasperated by the resource differential between their adversaries and themselves, are often resigned to the fact that 'they're going to get me anyway' and therefore eschew 'cumbersome' security practices in favour of direct confrontation with their antagonists.
- *Information overload*: Trainers noted that some recipients of digital security trainings find themselves overwhelmed by an overload of technical information in a short period. While a number of steps taken in isolation can be understood, HRDs can find the combination of tools and tactics covered in training to be overwhelming, and consequently they 'physically and psychologically tense up', inhibiting their ability to learn effectively.
- *Dependence upon the trainer*: Some HRDs, perhaps due to cultural factors, approach a digital security training as a one-way knowledge transfer and depend absolutely upon the trainer for all the answers to their digital security problems, rather than interpreting their own needs and making demands based on them. This can be aggravated by internal organizational dynamics inhibiting open communication between participants and trainers.
- *Misinformation*: Many HRDs often operate under mistaken impressions about digital security that risk putting them in great danger. Common mistaken impressions tend to lead to further exposure: for example, that using the Apple OS X operating system, rather than Microsoft Windows, precludes the possibility of malware infection, and that online storage or 'cloud' storage such as Dropbox is 'secure'.
- *Dropping out*: A small number of high-risk HRDs are simply opting not to use technology once they know they are directly under threat. In some cases the risks of being caught are so great and the learning curve so steep that it is easier to stop using technology altogether, even if this means the risk of greater isolation.

In the same interviews, we also asked trainers to highlight some of the proactive responses they have found HRDs adopting. In particular, we asked for examples of those integrating digital tools into their security strategies in innovative and effective ways, going against the techno-centric approach that has been dominating the digital security discourse. Examples include:

- *Going public*: Rather than 'locking down' their use of computers, email and social networking in light of the probability that they are under surveillance, some HRDs have fully embraced publicity as a path to security, thus detailing their names, pictures and activities in public forums to create awareness of their work and, as a result, of their security situation among the general public so as to 'shame' those attempting to stifle their legitimate efforts.
- *Filming everything*: The proliferation of video creation and editing software—particularly on mobile devices—has facilitated HRDs turning lenses on authorities. As one trainer stated: 'It surprised me how [activists in China] use mobile phones. They film everything . . . even when they run out of battery on their phones, they still act as though they are filming. It acts as a preventative strategy [against] being taken.'
- *Returning to low-tech or pre-digital tricks*: Some HRDs are employing 'old school' tricks to transport information safely. For example, rather than employing relatively complex encryption techniques to secure sensitive files on a USB key, they delete them in the 'traditional' way from their computer and empty the 'recycle bin' but do not overwrite the files, allowing them to be recovered once they have arrived at their destination.

These represent only sketches. The challenges to capacity building and the emerging responses from the field need to be explored further in order to better understand what is happening in practice as efforts to build awareness and transform capacity are deployed. More importantly, a better understanding of the types of behaviour and responses to digital security threats could help create more nuanced materials and training methodologies that are based on a more 'bottom-up' approach.

3.2.3 Towards an integrated approach to security

Hence, practitioners of digital security should stop reifying the false distinction between digital security and physical or psychological security, but should rather develop a holistic and integrated approach to security.

Personal and organizational security capacity building as expressed through manuals like the 'Protection Manual for Human Rights Defenders' (Eguren and Caraj, 2009), as well as security training regularly carried out by experts in the field of personal and organizational security, have at their core a context-dependent approach to the development of risk analysis and security practices for HRDs: readers and participants are encouraged to make iterative use of tools such as activity mapping, actor mapping, analysis of security incidents and use of the 'risk formula' in order to produce an analysis of their environment upon which to base security and emergency plans. The logic of such an approach is quite clear: there is no 'one-size-fits-all' approach to security, and no trainer should prescribe arbitrarily 'secure' measures, since the development of appropriate security measures requires a profound understanding of the set of forces contributing to the risk level of the particular HRD or organization concerned. Furthermore, in recent years practitioners from this field have made significant progress in developing materials and curricula that focus on the importance of psychosocial security and the gender dimension of security, although only nominal attention is paid to digital security in this context.[7]

Thus far, neither of the above elements have been fully integrated into the mainstream discourse on digital security for HRDs. Digital security tends to be presented in something of a vacuum and, at least formally, it takes no stock of the psychological effect of the environment in which HRDs are often operating.

In February 2013, Tactical Tech initiated a conversation with practitioners from these fields at a four-day event[8] with a view to exploring the challenges posed by their separation and identifying ways in which they could be overcome. These key issues emerged from the initial dialogue:

- The concept of 'safe spaces' cuts across all three disciplines in different ways and can be utilized not only in creating a space for effective and sensitive sharing and learning during trainings, but also as a means to conceptualize security.
- Approaches to security capacity building should not assume 'rationality' on the part of HRDs, particularly in situations where they are or have been subjected to high stress levels and/or trauma. Fear, as a naturally occurring by-product of risk and threat, should be accepted as an element of HRDs' experience in dealing with risk and should be considered when talking about security. HRDs should be given tools to help them evaluate risk in acceptance of this and fear should not be reinforced as a teaching method or to 'get a point across'.
- Practitioners' knowledge of the 'do no harm' approach to development interventions should be deepened in order to minimize the negative messages and resources transferred during training interventions and strengthen their positive impact.
- A defensive or militaristic conceptualization of security reinforces the idea of security practices as being a constraint on the efficiency of HRDs' work, which is inherently dangerous and widely accepted as such by HRDs themselves. Rather—while its definition should be personal to each HRD—a

[7] This has been particularly well-developed in tandem with a gendered perspective on the security and protection of HRDs, by organizations including Front Line Defenders, Kvinna till Kvinna (KVK), the Urgent Action Fund for Human Rights Defenders (UAF) and the Women Human Rights Defenders International Coalition. See e.g. Barry and Nainar (2008).

[8] The 'Holistic Security Retreat' took place over four days from 26 February to 1 March 2013 and aimed at initiating a dialogue between practitioners from various fields of security and protection for HRDs in order to overcome common challenges and identify opportunities for collaboration. The event was attended by trainers and practitioners from Tactical Technology Collective, the Center for Victims of Torture, Free Press Unlimited, Front Line Defenders, Hivos, Internews Europe, Internews US, Information Innovation Lab, independent human rights and security experts, Open ITP, Protection International, and Witness, among others.

practical working definition should account for it as the *maintenance of agency* in the face of hostile forces and acts aimed at obstructing the realization of HRDs' goals.

4. Conclusions

The aforementioned principles suggest that an evolution of the existing approach to digital security capacity building is imperative, and reveal a number of key questions that ought to be explored in order to develop our understanding of security threats.

Firstly, it seems there is a need to move away from a techno-centric conceptualization of digital (in)security. Rather than focusing solely on software-based mitigations of digital security threats, which tend to age fast in a rapidly changing climate, HRDs need to be empowered to react quickly and flexibly. They need to be made aware of their antagonists' abilities but also need to be able to look at these challenges through the broader question of how they handle information. This implies a capacity building process, which would foster the development of critical thinking, agility and creative responses to digital security threats. Furthermore, all this entails a need on the part of some digital security practitioners who take a 'zero-sum' approach to digital security ('you are either completely secure or completely insecure') to recognize the inherent complexities of the context, work and personal lives of HRDs.

Key questions that should be answered in order to facilitate this would include:

- To what extent is the development of basic computer skills and knowledge necessary in order to facilitate better long-term digital security decision making among HRDs?
- How can trainees be kept abreast of new developments in digital security software and practices and how can they be best 'plugged in' to this community without reinforcing knowledge gaps?
- To what extent can broader principles related to information practices and processes be separated from choices in the use of tools?

Secondly, and in order to facilitate the above, practitioners need a deeper understanding of barriers to behaviour change in terms of security among HRDs and of the ways in which they respond and adapt, independently of the training and advice of established trainers and so-called experts. For instance, since a number of experienced trainers have made reference to defeatism, 'martyrdom', lack of time, and so on, these initial prototypical responses need to be expanded, the understanding of these characteristics refined, and some examination made of their possible causes in order to help to foster more of a 'bottom-up' approach to security practices.

Thirdly, the discourse of digital security for HRDs needs to be embedded within a more coherent or holistic approach. This needs to take into account the elements of personal, organizational and psychosocial security rather than reinforcing a false compartmentalization of 'distinct' fields of security. Indeed, practitioners of other 'fields' of security and protection of HRDs should recognize that given the proliferation of digital technologies and their ever deeper integration into the personal and professional activities of HRDs, digital security is no longer merely an issue for 'computer people' but rather an inescapable dimension of HRDs' physical and psychological integrity and well-being.

The digital aspect of security for human rights defenders has become extremely complex and continues to develop at a pace it is difficult for practitioners to keep up with. The integration of digital tools, information and communications technologies into the work and everyday lives of HRDs is ever deeper and cannot be ignored in any intervention aimed at treating their situation. At the same time, given the resource differential between HRDs and many of their adversaries and the rapidly developing technological climate, the community of practitioners trying to build HRDs' capacities in digital security can no longer afford to adopt an approach that fosters dependence upon their direct advice in order to stay safe. Although it represents something of a mammoth task, a coherent and holistic approach to HRDs' security must go beyond any one approach. It must foster critical thinking, be fully informed by shifting needs and practices emerging from the field, and must be addressed within the overall question of how to protect and enable the work of HRDs.

Acknowledgements

The authors are grateful for the kind support of Tactical Tech's funders and their colleagues at Tactical Tech, as well as the broader community of digital security trainers and developers, human rights organizations, defenders, journalists, technologists and activists for their support, advice and inspiration.

References

Barry, J., and V. Nainar. 2008. *Insiste, Resiste, Persiste, Existe*. http://www.frontlinedefenders.org/files/en/Insiste%20Resiste%20Persiste%20Existe.pdf.

Berkman Center for Internet and Society. 2010. Distributed Denial of Service Attacks against Independent Media and Human Rights. http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.

Citizen Lab. 2013. You Only Click Twice. https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2.

Doctorow, C. 2011. The Most Powerful Mechanism we have for Securing the Privacy of Individuals is for them to Care about that Privacy. Video. *The Guardian*, Comment is Free Interview. 18 April. http://www.guardian.co.uk/commentisfree/video/2011/apr/18/cory-doctorow-networking-technologies-video.

Eguren, E., and M. Caraj. 2009. New Protection Manual for Human Rights Defenders (3rd ed.). Protection International. http://protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf.

Freedom House. 2012. Freedom on the Net: Syria. http://www.freedomhouse.org/report/freedom-net/2012/syria (referenced 24 May 2013)

Meier, P. 2008. Operation Vula: ICT vs Apartheid. http://fl3tch3r.wordpress.com/2008/04/02/operation-vula-ict-vs-apartheid.

Morozov, E. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. London: Penguin.

Perlroth, N. 2013. Researchers Find 25 Countries Using Surveillance Software. *New York Times*, Bits blog. 13 March. http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software.

UN Human Rights Council. 2009. Report of the UN Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya. 30 December. A/HRC/13/22.

———. 2010. Report of the UN Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya. 20 December. A/HRC/16/44.

———. 2011. Report of the UN Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya. Summary of cases transmitted to Governments and replies received. 28 February. A/HRC/16/44/Add.1.

Vitaliev, D. 2007. Digital Security and Privacy for Human Rights Defenders. Front Line Defenders.

WikiLeaks. 2011. The Spyfiles. https://wikileaks.org/the-spyfiles (referenced 29 March 2013).

York, J. 2010. The ‘Cat and Mouse’ Game between Bloggers and Government. Blog post from Google’s ‘Internet and Liberty’ conference, Budapest 22 September 2010.