UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

BUILDING DIGITAL SAFETY FOR JOURNALISM

A survey of selected issues

Jennifer R. Henrichsen • Michelle Betz • Joanne M. Lisosky

UNESCO SERIES ON INTERNET FREEDOM

BUILDING DIGITAL SAFETY FOR JOURNALISM

a survey of selected issues

Jennifer R. Henrichsen • Michelle Betz • Joanne M. Lisosky

A report prepared for UNESCO's Division for Freedom of Expression and Media Development. The opinions expressed in this report are those of the authors and do not necessarily reflect the views of UNESCO of its Division for Freedom of Expression and Media Development.

Published in 2015 by the United Nations Educational, Scientific and Cultural Organization, 7, place de Fontenoy, 75352 Paris 07 SP, France

ISBN 978-92-3-100087-4 (print/pdf)

ISBN 978-92-3-100096-6 (ePub)

This publication was made possible under a contribution by the Kingdom of Denmark.

Graphic design: UNESCO

Cover design: UNESCO

Typeset: UNESCO

Printed in France

BUILDING DIGITAL SAFETY FOR JOURNALISM: A SURVEY OF SELECTED ISSUES

Authors:

Jennifer R. Henrichsen, Program and Research Coordinator, Journalism After Snowden, Tow Center for Digital Journalism at Columbia Journalism School

Michelle Betz, Consultant, International Media Development

Dr. Joanne M. Lisosky, Professor of Communication, Pacific Lutheran University

With special thanks to individuals from the following organizations who kindly agreed to be interviewed for this publication:

Access, Al Jazeera America, Article 19, Bytes for All, Citizen Lab, Columbia University, Committee to Protect Journalists, Digital Rights Foundation, Electronic Frontier Foundation, eQualit.ie, Federation of Nepali Journalists, Freedom House, Free Press, Global Journalist Security, Global Voices Advocacy, Global Voices, Index on Censorship, International Center for Journalists, International Federation of Journalists, International Media Support, International News Safety Institute, International Women's Media Foundation, Internews, International Research and Exchanges Board, Iraqi Journalists Rights Defense Association, *Management Magazine*, Media Legal Defence Initiative, National Democratic Institute, Open Internet Tools Project, Open Technology Fund, PEN American Center, Reporters Without Borders, Robinson + Yu, Rory Peck Trust, SKeyes Center for Media and Cultural Freedom, Southeast Asian Press Alliance, Tactical Technology Collective, The Guardian Project, The Mozilla Corporation, The Mozilla Foundation, The New America Foundation, *Today's Zaman*, Tow Center for Digital Journalism at Columbia Journalism School, Trustwave, and several freelance journalists, bloggers and human rights activists.

Surveys included in this report were translated by:

Abeer Al Kazimi, Frederic Castellan, George Donald, Maren Anderson Johnson, Mahlon Meyer, Bassel Sommakia, Tamara R. Williams, Katie Youtz, and Ellen Wenjia Zhou.

Thank you to those who read drafts of the report or provided guidance at various stages of the research process:

Binod Bhattarai, Eva Galperin, Sabina Izzatli, Geoffrey King, Tom Lowenthal, Silvia Chocarro Marcesse, Karen Reilly, Seamus Tuohy and Eric Zimmermann.

Launch Event

The research for this study was launched at the Internet Governance Forum in Istanbul, 3 September 2014, at a workshop co-hosted with Article 19, Committee to Protect Journalists, and the Centre for Studies on Freedom of Expression (CELE) at the University of Palermo in Argentina. We express appreciation for the comments of the audience and the panelists. Those speaking on the panel were:

Mr Geoffrey King, Internet Advocacy Coordinator and Digital Security Specialist, Committee to Protect Journalists, United States of America

Mr Eduardo Bertoni, Researcher, Center for Studies on Freedom of Expression and Access to Information (CELE) of the University of Palermo, Argentina

Ms Laura Tresca, Brazil Freedom of Expression Officer, Article 19

Ms Silvia Grundmann, Head of Media Division, Council of Europe

Mr Scott Busby, Deputy Assistant Secretary in the Bureau of Democracy, Human Rights and Labor at the U.S. Department of State, Washington, DC.

Table of Contents

Foreword

As the United Nations agency with a mandate to promote freedom of expression and its corollary press freedom, UNESCO has a long-standing commitment to foster the safety of journalists. The safety of digitally interfaced journalistic actors has significant implications for freedom of expression, press freedom and privacy protection, and is of particular concern to UNESCO.

In order to improve global understanding of emerging safety threats linked to digital developments, UNESCO commissioned this research within the Organization's on-going efforts to implement the UN Inter-Agency Plan on the Safety of Journalists and the Issue of Impunity, spearheaded by UNESCO. The UN Plan was born in UNESCO's International Programme for the Development of Communication (IPDC), which concentrates much of its work on promoting safety for journalists.

Safety for journalists, including digital safety, is a matter of public concern that is wide-ranging. It is vital for those who practice journalism, for their families and for their sources. It is essential for the wellbeing of media institutions, civil society, academia and the private sector more broadly. If we value the free flow of information for citizens, their governments and their international organisations, then the safety of journalists is central.

In short, when it is safe to practice journalism, society benefits. However, with the rise of digital platforms, ensuring this safety for journalists has become even more complex. There are new vulnerabilities opened up across the full value chain of the digital interface – and the new digital dimensions are not separate from existing threats to journalists in the physical world.

The current study, based on research by Jennifer R. Henrichsen, Michelle Betz and Joanne M. Lisosky, helps us to comprehend and address the new challenges as a growing issue in securing the safety of journalists. The research was enabled by Denmark, to whom we express appreciation. The ideas and opinions expressed in this publication are those of the authors; they are not necessarily those of UNESCO and do not commit the Organization.

In examining cases worldwide, this publication serves as a resource for a range of actors. In a nutshell, it surveys the evolving threats, and assesses preventive, protective and pre-emptive measures. It shows that digital security for journalism encompasses, but also goes beyond, the technical dimension. Recommendations are made for governments, journalism contributors and sources, news organizations, trainers, corporations and international organisations.

While not all the people who contribute to journalism are fulltime journalists, the research takes an inclusive approach that is relevant to any actor who is in danger of being targeted for doing journalism. Indeed, many points made are also of direct relevance to human rights defenders in general, to people who are sources for journalists, and even to actors who simply make use of digital communications for personal use.

The research also shows that digital safety is not a gender-blind issue, and that this should be acknowledged in digital safety training. It proposes that training should include not just digital know-how and resources, but also cover normative, psycho-social and physical aspects.

Amongst the useful advice given in this study is the suggestion that practitioners develop a risk assessment or 'threat model'. This can serve as a foundation for a personal security plan that covers both digital and physical safety. In turn, that can help individuals make an informed trade-off of time, resources and judgment-calls about security.

Given rapid technological development, this publication is a snapshot document of significant challenges and recommendations as of 2014-2015 and its insights will need to be reviewed and updated over time. Nevertheless, the principles endure – that journalism deserves to be treasured and protected, no matter its technological interface.

UNESCO's approach, informed by the UN Plan of Action on the Safety of Journalists and Issue of Impunity, is that the protection of journalism needs the support of many other actors. Top of the list is the public. In particular, and as this publication proposes, journalism needs a public that is media and information literate, including in the changing digital dimensions. It is these kinds of competencies that can ensure that citizens are empowered on an ongoing basis to cherish and help defend journalism against its adversaries.

Getachew Engida
Deputy Director-General of UNESCO

Executive summary

Parallel to the growing digitisation of journalism which brings unprecedented benefits to both producers and consumers of journalism, there are worrying trends that have emerged.

Electronic communications of news media, critical bloggers, and other individuals or organizations disseminating information have become targets. The danger emanates from various sources ranging from State-based actors to third parties. There is digital surveillance that goes beyond international standards on privacy and freedom of expression. There is hacking of data and disruptive attacks on websites and computer systems. More extremely, some media actors are being killed for their online journalism. From 2011-2013, 37 of the 276 killings of journalists condemned by the UNESCO Director General were killings of journalists whose primary platforms were Internet-based.[2] Many, if not most, of the other journalists who were killed also used digital tools in their daily work, which may have exposed them in various ways.

Some safety risks have simply been transferred from the offline world to the online world. Death threats are now emailed, and may be in response to web-based content rather than in newspapers or in broadcasting. A media office or printing press may still be bombed, but now a Denial-of-Service attack may also be launched to bring down a media website. However, other threats take on a new dimension in their digital shape. As more data is being generated, stored, transmitted and searched, old threats such as gender-based harassment can intensify. There are also new privacy and freedom of expression issues which arise. Examples are journalists' movements being exposed through cellphone-linked geolocation data, their personal lives being visible on social media, and their communications meta-data being mined.

The threats identified in this publication cover at least 12 digital threats, including illegal or arbitrary digital surveillance, location tracking, and software and hardware exploits without the knowledge of the target. Further examples that are considered are: phishing, fake domain attacks, Man-in-the-Middle (MitM) attacks, and Denial of Service (DoS).

Also covered are instances that show how journalists need protection from threats such as website defacement, compromised user accounts, confiscation or theft of their digital resources, and online intimidation, disinformation, and smear campaigns. At the same time, it is recognised that digital security is undergoing constant change, and that it is also becoming ever cheaper for those who wish to mount digital attacks.

These insights are valuable for policymakers, civil society organisations, media companies, and a range of journalistic actors, offering them enhanced understanding about new challenges to journalism safety. This publication also gives an overview of actors and initiatives working to address digital safety, as well as identifying gaps in knowledge that call for awareness-raising.

The digital safety risks are analysed in technological, institutional, economic, political, legal and psychological dimensions. Recommendations in each of these categories are proposed for concerned stakeholder groups. These cover issues such as the digital behaviour of practitioners, capacity-building for digital security, digital expertise services, and measures that are needed by media companies. The recommendations also point to ongoing needs for data and research. Also highlighted is the need to promote national mechanisms to protect journalists from all threats, and to raise awareness about the evolving norms in the UN system and their relevance to the safe practice of journalism.

The case is made for a multi-stakeholder approach to protect journalists more broadly, including the digital dimensions. With co-operation by relevant actors, the rights to free expression and press freedom can be secured – including in their interfaces with the Internet. In this way, the unfettered flow of journalistic information can continue to make its contribution to society and ensure more broadly that the Internet's advantages are not overshadowed by its risks.

1. INTRODUCTION

This chapter introduces journalism and its evolution, and seeks to identify the approximate range of online media actors doing journalism. As journalism moves into the digital space, it will continue to benefit from expanding access to information, audiences, and publishing tools that new technologies offer. At the same time, there are new threats.

Journalism informs and educates its audience. It serves a societal interest in transparency. Those who practice it frequently act as watchdogs, scrutinizing the formulation of public policy and highlighting blocks to development such as corruption, human rights abuses or inefficient governance. This plays an essential role in realizing democratic and developmental rights. Many scholars agree that journalism provides citizens with the information they need to be free and self-governing.[3] Studies by Pippa Norris have shown a statistical correlation between free media and the realisation of democracy and development.[4] In a book published by the World Bank Institute, Joseph Stiglitz and other authors further demonstrate that accurate, timely information results in better, more efficient resource allocation, concluding that free and critical media play a crucial role for development.[5] These points have become increasingly topical as the UN develops its sustainable development goals.[6]

Journalism is developed through human interaction, yet is often generated, processed and disseminated through electronic means – particularly digital. In today's global multimedia environment, journalism can be practiced in a multimillion-dollar newsroom or from one's bedroom. Wherever it takes place, journalism often involves enormous risk to those producing it and their sources, particularly where its output challenges power or brings to light information that other actors seek to conceal.

Those who practice journalism may attract attacks because of the important role they play, and it is because of this role that they also particularly merit protection. They need to be safe and free to provide opportunities for the expression of opinions and information, monitor and shed light on government and corporate operations, and encourage accountability.[7] They should not have to work in fear of giving voice to the voiceless, or afflicting the comfortable.

Technological innovations have made it easier than ever to engage in newsgathering and content dissemination. As of December 2013, almost 40 per cent of the world was online (although this connectivity was substantially higher in the developed world) and there were 96 mobile cellular subscriptions per 100 people.[8] Today, anyone producing journalism can face risks. Digital security and operational security concerns will increase in importance as lines increasingly blur between online and offline activity.

1.1 Definitions, scope and objective of research: defining the wide range of actors and evolution of journalism

All media actors on all platforms are entitled to enjoy the fundamental right of freedom of expression, and entitled to the safe exercise of this right. Society has a particular stake in protecting those who produce journalism. The interconnectedness that the Internet and mobile technologies foster has enabled everyday citizens to participate in journalism by documenting local events or even researching and analyzing distant ones, and disseminating news and opinion around the world. In situations where journalists at media houses have limited access to information or sources because of natural disasters, or humanitarian or political crises, citizen reporting is especially valuable because it provides critical information to various members of the indigenous and international communities. Rather than the era of an exclusive press, today news gathering and dissemination is often distributed across diverse actors and media platforms, including social media.

Those established players now publishing online are complemented by new contributors who bring an increasingly significant contribution to public information and opinion. In addition to these changes, much online journalism has become interactive, involving discussions online amongst consumers of journalistic content themselves, and between them and the producers, with the line between the two blurring in many cases. Open-source reporting – or collaboration among reporters, sources and readers – is a developing phenomenon.[9]

This proliferation of voices on newsworthy matters has led to increased opportunities for media to foster global civil society, and has enabled a broader coverage of topics of interest to the public, including subjects of particular interest to often voiceless minorities.[10] It has also strengthened real-time reporting of events. At the same time, when citizens bear witness or comment through digital means such as blogs, tweets or SMS comments on television screen tickers, questions arise about journalistic identity and status.

Who is a journalist?

The debate over who is and who is not a journalist is ongoing. The primary question focuses on whether individuals who gather information and disseminate such content on their own are journalists. Many define journalists not on platform or formal status, but by practice of journalism as the generation and circulation of newsworthy information and opinion in the public interest. According to Oktavía Jónsdóttir, program director of the Securing Access to Free Expression (S.A.F.E.) Initiative at the International Research Exchanges Board (IREX): 'It's not about where you conduct your work, but the fact you engage in newsgathering activities.'[11] This approach is similar to that of the Council of Europe in its Recommendation No. R (2000)7: 'The term 'journalist' means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication.' It also parallels the United Nations (UN) Human Rights Committee, which in 2011 defined journalism in its

general comment No. 34, as 'a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere' (para. 44).

Today, this view embraces many individuals who consider themselves journalists and yet are not employed in the traditional news media institutions. Many are bloggers and videographers who create and publish articles online. Some practice journalism in their spare time in addition to other jobs and are not necessarily compensated monetarily for their efforts. In addition, there are other digital contributors who do not see themselves as journalists, but who also contribute to journalism as witnesses, fact-checkers, commentators or reporters, and mostly by making use of digital technology.

This technology-neutral perspective is implicit in the view of the former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue:

> Journalists are individuals who observe and describe events, document and analyze events, statements, policies, and any propositions that can affect society, with the purpose of systematizing such information and gathering… facts and analyses to inform sectors of society or society as a whole.[12]

For the purposes of this report, it is recognized that, irrespective of technology, not all media actors who produce or contribute in a 'systematized' way to journalism do so to the same extent as those individuals who engage in newsgathering activities as their professional employment. Not all who do journalism or make a contribution to it are journalists. However, digital safety is certainly relevant to all.

This inclusive conception corresponds with the 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity' which states that, 'the protection of journalists should not be limited to those formally recognized as journalists, but should cover others, including community media workers and citizen journalists and others who may be using new media as a means of reaching their audiences.'[13]

Such a perspective aligns with UNESCO's accepted documents which refer to, 'journalists, media workers and social media producers who generate a significant amount of public interest journalism.'[14] It is this perspective that therefore informs this research. And because almost every person connected to journalism today uses Internet and telecommunications to one extent or another, even if their output is published or broadcast offline, digital safety is a matter of generic relevance.

1.2 Examining the digital challenges and dangers faced by journalists and others who contribute to journalism

The Internet is a pathway for information sharing and a virtual meeting square where individuals can provide contrary information and views, debate key issues, and associate with each other, offering the opportunity for people to realize the right to freedom of expression and association like no other time in history. Newsgathering and information dissemination can often overlap with social media, as well as blogs and mobile phone communications. The activities can be done by both professional journalists and untrained citizens who nevertheless produce journalistic content. These latter media actors serve as increasingly vital sources of information as new platforms and tools allow them to produce content in an unprecedented way, and to engage with the output of more traditional journalism on a range of platforms.

As more actors take up the mantle of participating in journalism and contribute to informing public opinion, they also become subjects of interest to actors wishing to control the flow of information. According to a report on the safety of journalists from the UN High Commissioner for Human Rights in July 2013: 'As the number of online journalists has increased, so have attacks against them, such as illegal hacking of their accounts, monitoring of their online activities, arbitrary arrest and detention, and the blocking of websites that contain information critical of authorities.'[15]

According to the Committee to Protect Journalists' East Africa representative Tom Rhodes:

> The level of threats against press increases every year … as government authorities – among other actors – are looking more closely at the impact of online media. Besides receiving threats online, many are tracked down via mobile phone networks and threatened further via their phone lines. We also have cases of online journalists/commentators being killed. It is becoming just as dangerous, if not more dangerous given the impact of online media, for journalists who work for online media outlets as it is for other mediums such as print and radio.[16]

The safety of journalists, conceptualized inclusively, has risen to prominence on the global stage in recent years, spearheaded by international press freedom organizations and UN bodies like UNESCO, the Human Rights Council, the UN High Commissioner for Human Rights, the UN General Assembly and the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. In 2012, the 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity' (UN Plan) was endorsed by the UN Chief Executives Board with the goal of 'creating a free and safe environment for journalists and media workers, both in conflict and non-conflict situations, with a view to strengthening peace, democracy and development worldwide.'[17] The Plan sets out a multi-stakeholder framework for national and international action to secure safety for journalism. In 2013, the UN General Assembly itself welcomed the UN Plan. For this research study, the researchers have drawn upon the UN Plan's conceptualization of safety as designating:

> A broad category that extends from preventive, protective and pre-emptive measures, through to combating impunity and promoting a social culture which cherishes freedom of expression and press freedom. … Safety spans both online and offline worlds, and … solutions require informed action at global, national and local levels whilst at the same time responding to contextual specificities in each case.[18]

Journalists and other actors doing journalism with digital technologies face a range of digital challenges and dangers, which sometimes contribute to the hostile environment they face in the physical world. According to the Committee to Protect Journalists, 44 per cent of the 70 journalists they recorded as killed in 2013 were journalists who worked for online media platforms.[19] Meanwhile, such 'online journalists' accounted for half, 106, of the prisoners CPJ recorded as imprisoned in 2013.[20] However, dangers face not only those who publish online. They apply to all actors whose journalistic activities interface with electronic technology, whether through their use of computers to process information, their utilization of telecoms or the Internet for news gathering and research, or simply their reliance on email for communications. This study is concerned with the threats facing all individuals whose use of digital communications for journalism may expose them to defined dangers. These are elaborated in chapter 2.

It is difficult to research the attacks and threats facing those doing journalism digitally, for a number of reasons.

First, digital attacks are often difficult to identify without a high level of digital expertise. While some news organizations may have resources at their disposal – including system administrators well versed in digital threats – many independent bloggers, freelancers, or citizen journalists often do not have this expertise or even access to such expert assistance.

Second, news organizations and individual journalists do not often know or share that they have been victims of digital attacks. There are a variety of reasons for this. Some might be worried that revealing sensitive information might lead to further victimization. They could also be concerned that sources could be reluctant to make contact because of a perception that they are not able to keep sensitive information confidential.

Third, it is difficult to directly pinpoint which entity or entities are carrying out surveillance or other interference with electronic communications. A digital security specialist might be able to discover the name of the company that created the surveillance software, but it is more difficult to ascertain who ordered or deployed the attack. The same applies to attacks that visibly disrupt communications such as defacement of sites or implanting of malware. Many examples informing this study are believed by various observers to be caused by specific actors; but it is not possible to prove this definitively. As a result, this study concentrates more on the type of reported attacks, and does not endorse any reported assumptions about the identity of perpetrators. The important task is to identify the kinds of threats and appropriate protection for those who find themselves digitally endangered.

Lastly, human rights organizations – which seek to protect and extend the digital rights of users at risk around the world – may not have data on journalists and other online

actors who have had rights to free expression and privacy violated in digital space. Even when they do, they do not always have sufficient resources to analyze and make the data anonymous so it can be shared safely. [21]

In order to better understand and assess emerging threats to journalism in regard to its interface with digital technology, these challenges need to be unpacked.

1.3 Mapping activities regarding digital safety

A variety of stakeholders, including commissions, news organizations, governmental and non-governmental organisations, technologists and journalists are becoming more aware of the digital dimensions of journalistic safety, and are taking steps to mitigate these. Through a variety of commitments, initiatives, training courses, meetings and materials, areas of practice can be mapped according to the following categories:

- Normative work and awareness raising,
- Digital security training guides and training courses,
- Hotlines and safety assistance, and
- Reports and research.

The following section will present an overview of these topics, including the challenges. A review of some of the actors and their particular actions aimed at dealing with the challenges is presented in depth in chapter 2 of this report. The third chapter offers recommendations for addressing the problems in the identified four areas of practice.

Normative work and awareness raising

Awareness raising is a way to sensitise all actors about comprehensive safety for journalism, and to promote the social norm that this special kind of public communication should enjoy security and protection, and not least in regard to its interface with digital technologies.

Promoting broad awareness is a common activity among the key stakeholders involved in promoting the protection and safety of journalism. Press freedom organisations send letters to high-level officials, calling on them to investigate crimes – including digital crimes – against journalists. Intergovernmental bodies work with their partners to ensure the safety of journalists remains a priority on the international agenda.

Meetings to coordinate efforts to improve the safety of journalists are often spearheaded by UNESCO in both global and local contexts. These meetings typically include UN agencies, government representatives, non-governmental organizations (NGOs), media houses, journalist associations, journalists and academia, and they incorporate specific action lines on digital safety and online rights. The topic of protection of journalists is also addressed in international human rights fora, such as the UN Human Rights Council. Today, more technologists are also joining forces with human rights and press

protection organizations to help journalists and others learn about digital security best practices, circumvent censorship, limit their vulnerability to surveillance and better protect their sources.

However, there is limited awareness of these developments amongst many practitioners. In addition, popular elaboration of how these actors can use such normative standards for advocacy and policy change – including in the digital arena is lacking or limited. The gender dimension is not always sufficiently appreciated.

Digital security guides

The field is awash in digital security guides, and in formats ranging from mobile apps, video, and animation through to plain text. While it is helpful to have new guides in the field, the proliferation and the sometimes contradictory advice can generate confusion. As a whole, the guides are also limited in terms of the number of languages covered, and they can quickly become outdated.

Digital security training

Digital security training programs for human rights defenders and journalists are increasing. However, approximately 54 per cent of 167 respondents to the survey for this report said they had not received digital security training.

Other organizations have also registered this lack of digital security training in their research. A report sponsored by the Internews Center for Innovation and Learning and conducted by the Pakistani NGO Bytes for All interviewed 37 journalists and 15 bloggers from across the country and found that three-quarters of them had little awareness of the security risks they could face, including the interception of email or the theft of their data. Many interviewees were also unaware of strategies and tools they could use to protect themselves online.[22]

According to Andrew Ford Lyons, Digital Producer at the Rory Peck Trust, a London-based NGO that provides resources and support to freelancers, freelance journalists have a particularly low level of awareness on how to safely use satellite and mobile phones, file stories from the field, and successfully implement encryption.

Where it happens, digital security training faces several challenges, including a lack of:

- Understanding among donors and clients of what a digital security trainer can achieve with his or her audience in the time allotted,
- Self-care guidelines for digital security trainers, as they may be susceptible to burnout and compassion fatigue, and
- Permanence, as practices and technologies that may be recommended as safe at one time can become redundant or ill advised at a later point.

Another problem which some digital security trainers and program officers have noted is that even though the journalist or human rights defender trusted them individually, that relationship did not extend to the trainer/program officers' organization or to a technologist.[23] This lack of trust has sometimes led to the journalist not implementing the digital security assistance.

Hotlines and safety assistance

Many NGOs provide safety assistance to journalists and have done so for many years. Much of this safety assistance has focused on physical protection measures, such as safety gear for journalists covering conflict areas, insurance, financial assistance for relocation and other provisions. In more recent years, some organizations have worked with journalists and news organizations, as well as bloggers and others, within country contexts in order to provide digital security expertise and training. Others have acted as liaisons between journalistic actors and trusted technologists, connecting them when there is a digital security need. Challenges are limited resources and knowledge of such facilities by journalists under stress.

Reports and research

Reports and research by press protection organizations, academic institutions, and international human rights organizations help to shed light on the types of attacks that journalists and activists face. In recent times, this research has included digital threats and attacks such as surveillance and targeted malware. Interdisciplinary research organizations like the Toronto, Canada-based Citizen Lab investigate online attacks against civil society and journalists. The challenge is to maintain and extend this kind of in-depth research into digital threats and attacks which are likely to increase with higher levels of Internet connectivity, the increase in data storage capabilities, and the inexpensive cost of disruptive and surveillance technologies.

1.4 Specific challenges

Actors doing journalism in a digital context face numerous and complex challenges including technological, institutional, economic, political, legal and psychosocial. These are identified below:

Technological, institutional and economic challenges Affecting journalists and news organizations

- Surveillance, data storage capabilities and digital attack technologies are becoming less expensive and more pervasive.

- Digital security tools are not always user friendly, leading to too few journalists implementing the tools correctly or at all.
- Commercially available digital security tools may be too expensive for freelancers or bloggers to purchase, and many tools (free or otherwise) are not user friendly for non-technologists.
- Open source digital security tools often lack a sustainable business model, which means they may become obsolete after a short period of time or may not be updated against vulnerabilities.
- Denial-of-Service attacks may result in financial loss for news organizations or individual journalists.
- Many journalists and their sources are unaware of technologists willing and able to assist them if they experience a threat or attack that is digital or digitally-relayed.
- Many journalist and their sources are not adept at understanding data anonymisation or the use of secure technologies such as encryption.
- There is a lack of publicly available data documenting the types of digital attacks and threats those doing journalism face.
- State and non-state actors can use location tracking technology to identify media actors – and their sources – who often need confidentiality for the production of journalism.
- The digital security of both those who do journalism and their associates (sources, families, colleagues) can often easily be compromised via phishing campaigns. Compromised user accounts and devices can be used to identify the sources and networks of those doing journalism, leading to increased insecurity.
- Digital security is often taught ad-hoc, if taught at all, instead of being systematic and holistic.

Political and/or legal challenges
Affecting national governments, UN bodies and intergovernmental organizations, NGOs, and corporations

- Controls on journalism are sometimes obscured in data protection laws, while other laws are interpreted in ways that can lead to the arrest or detention of journalists for receiving, obtaining or disseminating information, by digital means.
- Lack of political will to address crimes against journalism, including digital crimes, which results in a climate of impunity for the perpetrators.
- Sanctions can result in reduced availability of technology or software updates needed for those doing digital journalism to stay safe, while the lack of sanctions can result in exposure to more powerful threats as a consequence of unregulated trade in software exploits and advanced surveillance and cyber-attack technologies.

Psychosocial challenges
Affecting journalists, news organizations, journalism schools and other educational and training institutions, and journalist associations

- A low level of appreciation and understanding of digital security principles and tools.
- Decision-fatigue among journalists and other media actors may result in weak application of digital security tools or complete avoidance.
- Digital security training is often not systematized or holistic (e.g. it may exclude operational security and psychosocial care).
- Previous traumatic experiences may result in journalists making bad decisions that lead to greater insecurity.
- Family and friends may unintentionally compromise the digital security of those doing journalism such as by inadvertent disclosures on social media.

The crosscutting and diverse nature of the challenges facing journalism in a digital context, has specific relevance to a wide range of stakeholders, and specific recommendations for these are presented in Chapter 3.

2. GLOBAL OVERVIEW: CHALLENGES, STAKEHOLDERS AND PRACTICES

2.1 Introduction

Across the world, the digital threat landscape is expanding and becoming more complex. Online security threats like phishing, malware and cyber espionage have grown and evolved in recent years, serious software vulnerabilities like Heartbleed and Shellshock have been discovered, and traditional threats have found new ways to cause harm, including via social media and mobile devices.[24] Meanwhile, the capacity to collect, analyze and store digital communications is becoming more sophisticated and inexpensive and the market for offensive computer network intrusion capabilities continues to grow at a rapid pace.[25]

For years, global civil society groups have viewed the Internet and other new media as a powerful tool for their causes, but recently they have discovered how new media can be controlled to limit access to information and freedom of speech.[26] According to Citizen Lab's Ronald Deibert, cyberspace is becoming a dangerously weaponized and insecure environment where independent media can be trapped, harassed and exploited as much as they can be empowered.[27]

Organizations like Access, Citizen Lab, Committee to Protect Journalists, IFEX and Article 19 are increasingly documenting attacks against journalists suffered in the online realm, often by actors seeking to further sociopolitical goals. These attacks are carried out by large and well-resourced adversaries.[28] According to Google security engineers Shane Huntley and Morgan Marquis-Boire, 21 of the world's top 25 news organizations have been the target of likely state-sponsored hacking attacks.[29] 'If you're a journalist or a journalistic organization we will see state-sponsored targeting and we see it happening regardless of region, we see it from all over the world both from where the targets are and where the targets are from,' Huntley told Reuters.[30] According to Marquis-Boire, the number of attacks on media organizations and journalists that went unreported was significantly higher than those made public.[31]

These attacks, as well as others, occur at great cost to journalists and their networks as well as to freedom of expression and association more generally.[32] This chapter illustrates some of the varied (and often overlapping) threats facing media actors in today's technological environment:

- Surveillance and mass surveillance,
- Software and hardware exploits without the knowledge of the target,

- Phishing attacks,
- Fake domain attacks,
- Man-in-the-Middle (MitM) attacks,
- Denial of Service (DoS) attacks (and DDoS – distributed denial of service),
- Website defacement,
- Compromised user accounts,
- Intimidation, harassment and forced exposure of online networks,
- Disinformation and smear campaigns,
- Confiscation of journalistic work product, and
- Data storage and mining.

Limitations of research

This chapter focuses on the safety of journalists and others who contribute to journalism and not on digital issues that affect freedom of expression in the broader sense, such as communication blackouts, online copyright issues, denial of e-payment facilities, content filtering or blocking, takedown notices, etc. Although the researchers aim to present a comprehensive picture of digital threats and attacks facing journalistic actors, not every type or case is documented. It is likely that revelations of new digital security threats and surveillance will come to light after this report is published. Nonetheless, this chapter provides a starting point for discussion among key stakeholders seeking to safeguard journalists and others who generate a significant amount of public interest journalism.

2.2 Mapping of digital challenges and dangers facing journalists and others who contribute to journalism

State or non-state actors can attempt to influence the flow or content of information by denying, disrupting, manipulating, or monitoring access to a range of electronic data. Methods vary, because exploits and attacks are influenced by a variety of factors including the economic, social, and political context where the information controls are applied.[33] The control of information is also influenced by the types of communications infrastructure that countries have, such as the number of Internet Service Providers (ISPs), telecommunication companies, degree of market competition and the overall level of Internet penetration and growth. [34]

Surveillance and mass surveillance

Surveillance, as the monitoring, interception, collection, preservation and retention of information that has been generated, stored and relayed over communications networks, is one way actors seek to monitor information.[35] Surveillance technologies are diverse and can include location tracking, deep packet inspection, facial recognition and mass monitoring.[36] Bulk interception methods for voice, SMS, MMS, email, fax and satellite phone communications also exist.[37] Surveillance can occur en masse or target individuals. Although surveillance has many legitimate uses, when it is collected en masse, without credible oversight by an independent monitoring body, it can chill internationally recognized human rights – including freedom of expression, freedom of association and the right to privacy – and threaten democracy. This is recognised in a resolution of the Human Rights Council adopted in March 2014 where deep concern was registered 'at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights'.[38]

According to the Report of the Office of the United Nations High Commissioner for Human Rights published in June 2014, 'Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programs may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime.'[39] Mass surveillance reduces the ability of a free press to function because it facilitates the indiscriminate collection of information on the communications of all possible sources.

In addition, mass surveillance is often governed by many secret and ambiguous laws, which can sow confusion among journalists and their sources about how closely they might be monitored.[40] This lack of information makes it more difficult for journalists and their sources to try to shield themselves from mass surveillance and protect their sources. Journalism depends on sources' willingness to talk on and off the record; if communications between journalists and sources cannot be kept confidential, then it is possible sources will stop talking.[41]

Mass surveillance also can result in a chilling effect on writers' willingness to research and publish stories. For example, in 2013, the PEN American Center (PEN) and the Farkas Duffett Research Group conducted a study to determine what impact, if any, government surveillance has had on PEN's members.[42] The study revealed that:

- PEN writers now assume that their communications are monitored.
- The assumption that they are under surveillance is harming freedom of expression by prompting writers to self-censor their work in multiple ways, including reluctance to:
    - Write or speak about certain subjects,

- Pursue research about certain subjects, and
- Communicate with sources, or with friends abroad, for fear that they will endanger their counterparts by doing so.

In the context of mass surveillance, there are not always special provisions that protect journalistic communications from being collected or assessed. Further, if journalistic communications are collected, there are rarely protections against them being used for legal purposes unless wholly necessary and after due process.[43]

And, as more content and metadata (or information generated as one uses technology) is collected and stored, the picture of a journalist and his or her sources becomes clearer. According to a recent statement by several international NGOs to the Office of the High Commissioner for Human Rights:

> The historical distinction between data about an individual's communications and the content of his or her communications has become insignificant. As data becomes more and more revelatory, either in isolation or when paired with other data, it is no longer appropriate to subject communication data to lower thresholds or consider its collection and processing a less invasive practice than interception of content. Communications data can now reveal equally sensitive information as communications content, and must enjoy equal protections under human rights law.[44]

Put simply, without even considering the content of email or telephonic interactions between a journalist and a source, by merely analyzing the metadata of time, place and frequency of communications, it is possible to identify the actors involved in a particular journalistic exposé.

Software and hardware exploits without the knowledge of the target

Surveillance technology can also be used to infect computers worldwide with malware 'implants' allowing external entities to break into specific computer networks.[45] Tools that allow access for monitoring and surveillance include intrusion software and trojans, which operate as attack vectors. 'Attack vectors are like the lock-picks or copied keys to get into a building,' says Seamus Tuohy, associate technologist at the New America Foundation's Open Technology Institute.[46]

Surveillance technologies developed by commercial entities have been found on networks in many countries and reportedly have been used to target individual journalists and activists.[47] Citizen Lab has also recorded commercially available surveillance technologies that have been sold to a number of countries.[48] The market for mass surveillance technologies and network intrusion capabilities is booming. Surveillance technologies that detect encrypted and obfuscated Internet usage are hot ticket items, as are technologies that enable users to analyse web and mobile interceptions in real-time.[49]

Entities can also target journalists for surveillance by installing a physical 'bug' (or hardware tweak in an Internet router) or a hidden microphone on a journalist's communications devices or person. This might occur in the journalist's home, or from long distances through windows using high-powered microphones. A journalist could be the subject of wiretapping, where the content of his or her phone calls and Internet communications could be secretly monitored by those wishing to exert control. 'Pen registers,' which record the phone numbers made as outgoing calls, and 'trap and trace devices' that record numbers on incoming calls could also be used to capture the metadata of journalists' communications.[50]

Journalists might also be targeted with a 'zero day attack' – when an adversary exploits a vulnerability in software or hardware when there is no prior knowledge of the flaw in the general information security community, and therefore no fix or software patch available yet.[51] This is done to gain access to a target's device in order to deliver malware. Once an adversary has access to someone's computer, he or she can then install software to monitor the communications on that computer, such as keystroke logging, remote webcam/microphone access, email monitoring, file extraction, etc. It also allows the attacker to bypass encryption. This is especially important given the increase in encrypted traffic over recent years.

Other times, journalists may be targeted via their location data.

According to Oktavía Jónsdóttir, program director of the SAFE Initiative at IREX, geo-tagging is accurate within 2 to 5 meters if a phone is on (even in cases where privacy settings are on and location settings are off) and within 50 meters if a phone is turned off.[52] A 2013 study by researchers at the Massachusetts Institute of Technology (MIT) in the USA and the Catholic University of Louvain in Belgium, shows that location data reveals a significant amount of information about a person, resulting in little anonymity.[53]

To help protect the content of communications, journalists and their sources need to consider using encryption technologies. However, even encryption of content is not fool proof for protecting sources. Much can be gleaned from the metadata of exchanges. The use of encryption and other technologies may also actually flag the journalist or source as a person of interest who has something to hide. Indeed, merely interest in online privacy, anonymity and encryption projects has been reported to trigger enhanced tracking and monitoring in some cases.[54] In some countries, encrypted channels such as Virtual Private Networks (VPNs) are considered illegal, even if not always strictly enforced. Such communication can be stored and possibly decrypted when and if there is significant enough interest to access the information that the encrypted message is believed to contain. Still, encrypted communication can 'buy time', says the Electronic Frontier Foundation's (EFF) Eva Galperin.[55]

Not knowing if your communications, even if encrypted, are being monitored may have a chilling effect on journalistic work. Some journalists assume they are under surveillance even if they cannot prove it. Yet, this belief does not necessary correlate with an understanding that their insecure digital communication practices might have facilitated the surveillance.[56] In other cases, journalists realize their accounts have been

compromised, but they are not sure how it happened. Journalists and human rights defenders sometimes only have proof that they have been monitored after they are arrested and their chat logs or emails are read back to them by government authorities.

Phishing campaigns

Journalists and news organizations can be targeted for surveillance through phishing or spearphishing campaigns. These targeted 'phishing' or 'spearphishing' campaigns often use links or attachments laden with malware that are sent via email or social media.[57] Although malware differs in its capabilities, one of the most malevolent forms of malware that has been known to affect journalists' work is a Remote Access Trojan (RAT). The more sophisticated a RAT is, the more likely it is to avoid detection by anti-virus software. If clicked on or downloaded, these RATs allow the attacker to gather anything they want on the compromised computer.

'If the computer can do it for you, they can make it do it for them, or work differently for their needs, like re-routing traffic for a Man-in-the-Middle attack,' says Seamus Tuohy.[58] Other times, these attacks take the guise of a fake domain (website). The site silently collects account information that the journalist enters on the site, thinking that it is legitimate. A common phishing attack is when a journalist receives an email that appears to be from someone they know. It might be from a familiar email address and/or written as if it comes from an acquaintance. This fraudulent correspondence then lures the recipient into clicking on a link or an attachment that downloads malware onto his or her computer. According to Bill Marczak, a researcher with Citizen Lab and a doctoral candidate in computer science at University of California, Berkeley in the USA, journalists assisted by Citizen Lab researchers continued to be repeatedly targeted via attachments, despite warnings from researchers at Citizen Lab to open attachments only in the cloud (such as offered via several webmail service providers). Marczak believes that harm could be reduced by 85 per cent if journalists would stop directly opening attachments.[59]

Phishing campaigns and the subsequent installation of surveillance technology on a journalists' device can:

- Compromise a journalist's personal information, data and sources often without the journalist ever finding out,
- Result in blackmail by misuse of personal information, and
- Lead to self-censorship.

Fake Domain Attacks

According to Access, an international NGO that defends and extends the digital rights of users at risk around the world, fake domain attacks usually fall into two categories: 1) they inject malware, or 2) they provide fake content that attacks the credibility of the news organization or journalist.

In a fake domain malware attack, the fake domain copies the existing content from the targeted website and serves injected malware to visitors of the fake website. Attackers looking to expand their reach of victims may also create social media accounts to link to the fake site in order to have a higher Google PageRank of the fake site than the real site when searched.[60]

In a fake domain attack that involves false content, the attackers seek to diminish the credibility of the media actor. The attack might aim to influence public opinion, change the location of protests, or prevent new information from being published.[61]

Visitors often do not know that they have been the victim of a malware 'drive-by' or that they are reading fake content. They may access a site through a shortened URL, a URL from a social media source, or be redirected by a private or state-owned telecommunication company providing Internet access.[62]

According to Access, 4 per cent of its 60 unique cases over 10 months were fake domain attacks.[63] To help civil society and journalists defend against these attacks, Access released a browser plug-in called the Fake Domain Detective.[64]

Alleged cases of Internet service providers using DNS redirection or DNS hijacking to direct users to a fake domain have been reported.[65] DNS redirection is when a web address is deliberately moved from the one that is requested or reasonably anticipated to a fake page. In these cases, domestic visitors to specific independent media websites, such as supported by the political opposition, are redirected to fake versions of those sites.

Man-in-the-middle (MitM) attacks

A MitM occurs when attackers insert themselves, or their technology, in between a user and a target site. During a MitM attack, the man in the middle can silently obtain information from both sides and even change the content without either the user or the target knowing. Their exchange continues while the man in the middle watches.

A common variant of a MitM attack involves an attacker who uses a WiFi router to intercept user communications. One illustration of this is when an attacker configures a wireless device to act as a WiFi hotspot and then gives it a common name in a public place to trick individuals into believing it is a legitimate connection. As individuals connect to it and access sites such as online banking or email, their credentials are captured and stored for later use by the attacker.[66] Journalists should also be concerned about the ownership and independence of their ISP, because they could still be targeted by a MitM attack even if they are not using WiFi.

A slightly new variant of a MitM attack involves attacking a browser. This is when an attacker plants malicious code on a victim's machine that runs inside the browser, and which silently records the data sent between the browser and various target sites the attacker has hardcoded into the malware.[67]

Individuals engage in MitM attacks for a variety of reasons. They may wish to collect enough information to conduct future fraudulent actions, such as falsifying information or transferring money to the attacker's account. Other times, the attacker might feed false information to one or both sides, destroying communications and trust, or they may just desire to spy on communications.[68]

Denial of service attacks (DoS)

A DoS attack is another tactic used to intimidate online media actors and limit freedom of expression. A DoS attack is when one computer and one Internet connection is used to flood a server with packets with the intention to overwhelm the site and make it inaccessible to others. Another type of DoS attack is a distributed denial of service attack (DDoS), which utilizes a number of computers and connections, often distributed around the world to attack a computer. Similar to a DoS attack, a DDoS attack overloads websites, rendering them inaccessible.[69] According to Arbor Networks, a security firm in the USA, and Akamai Technologies, an Internet content delivery network in the USA, DDoS attacks in general are on the rise around the world.[70] Dramatic growth—more than 200 per cent—was seen in high-volume DDoS attacks.[71] It is more difficult for a server to withstand a DDoS attack than a DoS attack.[72] Experts point to the use of DDoS attacks as an accompaniment to intrusions, defacements, filtering and offline tactics.[73] While the use of this tactic may be widespread, some experts point to DDoS attacks as being replaced in favor of the targeted hacking or defacement of websites.[74]

According to Gustaf Björksten, Technology Director at Access, eight per cent of Access Tech's 24x7x365 Digital Security Helpline cases (60 unique cases within 10 months) were DDoS cases. Typically, DDoS attacks are event related, happening to political opposition websites and independent media during elections, independent media and activist websites during protests, or occasionally occurring in retribution for something akin to an advocacy campaign.[75] Like Access, Google also helps mitigate DDoS attacks. Its Project Shield provides support for media organizations through a program called Deflect.

DDoS attacks are effective at increasing censorship, although it is hard to attribute to particular agents those attacks which have this effect.

DoS and DDoS attacks are a significant problem for online media actors doing journalism because they:

- Prevent information from being disseminated and viewed, resulting in direct censorship,
- May result in financial loss to the online media actor because they have been taken offline and his or her audience is unable to access the website,
- May incur extra costs for the actor who must seek technical assistance, and
- May result in the public no longer thinking the publication is in existence.

Website defacement

There are many ways a website might be defaced. A common tactic involves using MitM attacks to compromise legitimate user accounts. Alternatively, an attacker might exploit vulnerabilities in the website's web server software.

Defacement of a web page is a frequently used attack against media organizations.[76]

Compromised user accounts

The goal of most attackers is to steal information they do not already have.[77] User accounts, such as for email, social media or Skype, can be compromised in a variety of ways. A phishing attack may install malware on a journalist's device that uses keylogging software, which can capture passwords and other sensitive information as a journalist types their login information. An attacker can also use a fake website, and after the user puts in his or her login information, the attacker can then use it to access the real website, without alerting the user.[78] Two-factor authentication can help avoid having an account compromised because it requires the user accessing an account to both know the account password and have a device (like a mobile phone), which will receive a one-time code when logging in. Unfortunately, even two-factor authentication can be bypassed by a skilled attacker.[79]

Sometimes user accounts are compromised through sophisticated social engineering tactics,[80] such as when the *Associated Press* Twitter account was hijacked in April 2013. As the account was compromised, it falsely reported that US President Barack Obama had been injured in explosions at the White House, causing the Dow Industrial Average to drop suddenly by 140 points.[81]

Intimidation, harassment and forced exposure of online networks

Intimidation, harassment and arrests of journalists are not new phenomena. However, journalists and others who contribute to journalism are now experiencing threats on multiple platforms. Press protection organizations worldwide have acknowledged the growing threats.[82]

Physical and digital threats are a serious concern because they may be a precursor to physical attacks against journalists.[83] According to CPJ research, 38 per cent of journalists murdered in the last 21 years were threatened before they were killed.

Sometimes journalists are intimidated into giving up their digital account information. For example, authorities might detain or threaten a journalist, forcing him or her to divulge passwords to their social media and/or email accounts.

To try to circumvent some of these restrictions, journalistic actors sometimes share passwords with colleagues. If they are arrested, colleagues can log in and remove

information that might be enough to detain someone under strict freedom of expression laws. Sometimes, NGOs are able to work with companies to shut down the account of a journalist as soon as it is reported that he or she has been abducted or arrested. Distributors of content also create multiple accounts, so if forced to reveal their account details, an especially sensitive account can remain secret. The arrest and detention of journalists is significant for digital safety because it can expose their online networks and sources, and increase the risk of harm to both.

Disinformation and smear campaigns

Disinformation against journalists is not new, but online smear campaigns are particularly troublesome for journalists because they may have a long life online and can spread far and rapidly.

Smear campaigns involve many different intimidation tactics that are often both online and offline. Such tactics include setting up fake websites where disinformation can live online, or intimidating a journalist with compromising photos or videos and then spreading them online. Other times, attackers choose to clone a website to confuse readers and threaten the credibility and legitimacy of a news organization. Other digitally interfaced media actors report instances of cyber impersonation, online propaganda campaigns, smear campaigns, and attacks in online forums.

Disinformation campaigns can also be waged against online news sites. In September 2013, the online investigative news site, *Ukrainska Pravda* (Ukrainian Truth) suddenly noticed the appearance of an imitation site called *Ukrainska Kryvda* (Ukrainian Lies) that mimicked *Ukrainska* in design.[84]

Smear campaigns are significant to the safety of online media actors – especially when amplified online – because they:

- Damage the credibility, integrity and confidence of journalists – elements which are essential to successfully carrying out their jobs, and
- Intimidate sources and journalists, resulting in self-censorship.

Confiscation of journalistic product

Confiscation of journalistic product is not a new tactic when seeking to intimidate or harass journalists. However, in an increasingly digital environment where journalists store vast amounts of information on portable devices such as laptops and mobile phones, journalists' confidential sources and information are at risk. These devices contain rich information and data that can reveal sources' names and contact information and put people in danger.[85]

Data storage and mining

Data storage is becoming cheaper and more efficient, allowing data – including content of emails, texts and other communications – to be collected and stored for longer periods of time. This facilitates the process of data mining, understood as the practice of searching through large amounts of computerized data to find useful patterns or trends.[86] For example, it can be used to pinpoint journalists' probable sources. There is a significant market for analyzing big data, with many of the same companies who service consumer markets like Facebook, also servicing intelligence and law enforcement agencies and without proportionate checks and balances.[87]

There are cases where data, including mobile phone locations and traffic data, stored under a country's data retention laws have allegedly been accessed to compile lists of high-profile journalists' sources.[88]

Data mining has consequences long after the immediate act of interception or seizure, including:

- A chilling effect on sources and journalists who become intimidated,
- The invasion of journalists' and sources' right to privacy, and
- Detention, arrest, prosecution, and imprisonment.

2.3 Mapping of key stakeholders and initiatives

This chapter will showcase a number of key stakeholders and their initiatives. The practices will be shown thematically and each section will have examples that reflect the geographic regions of UNESCO member states. As in Section 1.3 above, the key areas of practice have been categorized as follows:

Normative work and awareness raising,

- Digital security training guides and courses,
- Hotlines and safety assistance,
- Reports and research.

This is not an exhaustive list, but is intended to provide an overview of the types of practices that exist around the world. Descriptions of the organizations mentioned can be found in the glossary section at the end of the report.

Normative work and awareness raising

Awareness raising is a way to sensitize all actors about digital safety for journalism, and to promote the social norm that such communication should especially enjoy security and protection. Elaborating these norms globally entails decisions and positions by intergovernmental bodies that have a legitimate base for this. Promoting awareness of such is then necessary if these positions are to become living norms against which behavior can be measured. There is growing normative engagement with the safety of journalism and its digital dimensions.

Global

The Human Rights Council (HRC) is a UN intergovernmental body of 47 member states elected by the General Assembly, and which has focused on the safety of journalists for several years. Significantly, it affirmed in 2012 that 'the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.'[89]

Also in 2012, the HRC passed a landmark resolution on the safety of journalists that focuses specifically on the high risks faced by journalists and the need to secure better protection for media workers. The resolution recognizes the importance of all forms of media, including the Internet, in the promotion and protection of the right to freedom of opinion and expression, and condemns all attacks and violence against journalists.[90] In 2014, the HRC followed up with another resolution (A/HRC/27/L.7) which elaborated substantially on the earlier resolution, and in the same year the UN Secretary General published an extensive report on the safety of journalists and the issue of impunity (A/69/268).

On 18 December 2013, the UN General Assembly adopted the 'Resolution on the Safety of Journalists and the Issue of Impunity' at its 68th session. The resolution 'condemns unequivocally all attacks and violence against journalists and media workers, such as torture, extrajudicial killings, enforced disappearances and arbitrary detention, as well as intimidation and harassment in both conflict and non-conflict situations.' It also proclaimed 2 November as the International Day to End Impunity for Crimes against journalists.[91]

In May 2013, participants at a UNESCO conference adopted the San Jose Declaration, titled 'Safe to Speak: Securing Freedom of Expression in all Media' on the 20th anniversary of World Press Freedom Day. This declaration urges media outlets and professional associations to develop and sustain safety practices, including digital security training for freelance employees and regular staffers.[92] It also calls on UNESCO member states to undertake actions that ensure the freedom of expression of all those who use digital media, including bloggers and social media producers, and safeguard against intimidation, physical and cyber-attacks, and attempts on their lives. Similar principles were advanced in the Paris Declaration 'Post-2015 Agenda: The right of access to information, independent media, and safety for exercising freedom of expression, are

essential to development', adopted at the 2014 World Press Freedom Day conference held at UNESCO headquarters. In the context of a resolution on Internet issues in November 2013, UNESCO's member states affirmed that 'privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference'.[93]

Digital safety is not specifically singled out in the report on good practices by the Office of the UN High Commissioner for Human Rights in 2013 on the safety of journalists.[94] However, the HRC resolution A/HRC/27/L7 on the safety of journalists adopted in September 2014, highlights two dimensions: the important role of media organizations in providing digital security; and acknowledgment of the 'particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or interception of communications in violation of their rights to privacy and to freedom of expression.'

The UN General Assembly in November 2013 called on all states to review surveillance policies and establish independent oversight. The Office of the High Commissioner was mandated to do a further study on privacy, including digital privacy, which appeared as A/HRC/27/37 in June 2014.[95] Although it did not deal specifically with journalists, it concluded 'International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.' It recommended: 'Steps should be taken to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.'

It is not within the scope of this study to go in-depth into the policies and measures of states to follow up these resolutions in ways that enhance the digital protection of people doing journalism. However, it is clear that, by their own agreed standards, states themselves need to respect, protect and promote rights to free expression and privacy. That requires them to have legitimate purpose, as well as adequate checks and balances, with regard to their involvement in digital issues that impact on press freedom. This is to ensure that their own activities conform to international standards such as necessity and proportionality in regard to any limitations or intrusions on freedom of expression and journalistic work. States also need to have adequate data protection regimes that protect privacy and prevent abuse by either public or private actors.

Besides the UN, other international actors engaging in these issues include the Freedom Online Coalition. This partnership of 23 governments has adopted recommendations for freedom online, including a commitment to support digital literacy to empower Internet users and protect their human rights and fundamental freedoms. The Coalition also calls upon governments to halt, among other things, censorship and hacking.[96]

In civil society, International Freedom of Expression Exchange (IFEX) is a global network that defends and promotes free expression. It regularly monitors violations of freedom of expression and journalist safety worldwide and issues alerts, disseminates newsletters and hosts an archive of searchable alerts online.

As part of its international awareness raising efforts, CPJ regularly sends letters to high-level officials calling on them to investigate attacks against journalists and improve the climate of impunity. CPJ also documents threats and attacks in cyberspace and raises awareness of them in news alerts and blog posts.

RightsCon is an annual human rights conference that brings together technologists, human rights defenders, policymakers and others to discuss important issues and policies that relate to human rights and technology.[97]

Another international effort to strengthen norms and build awareness is the Arab Bloggers Meeting hosted by Heinrich Boell Foundation and Global Voices which has played a role in helping digital activists build a network of solidarity with each other.[98] Although the Bloggers Meeting is not annual, there had been four instances by 2013.

North America and Europe

In May 2014, the Council of Europe (COE) adopted the European Union (EU) Guidelines on Freedom of Expression online and offline.[99] In its declaration, the COE stated that it would build on the content of relevant UN resolutions, including those that focus on the safety of journalists and the right to privacy in the digital age. The COE Commissioner for Human Rights, Nils Muižnieks, affirmed via Twitter on 19 May 2014: 'We need to address the particular situation of bloggers & online journalists. #SafetyOfJournalists'.[100]

The Organization for Security and Cooperation in Europe (OSCE) updated its 'Safety of Journalists' guidebook in May 2014, including its guidelines on digital safety.[101] In addition, the OSCE representative on freedom of the media, Dunja Mijatović, has increasingly included the issue of the digital safety in her statements and speeches.

One body that is focused on the issue of journalist safety is the United Kingdom National Commission for UNESCO. The Commission works with a variety of organizations, including journalist and press freedom organizations to ensure journalist safety remains a priority among governments, UNESCO and the international community. Currently, it is working to raise the profile of the UN resolution on the safety of journalists to help protect media professionals around the globe.[102]

In January 2014, Privacy International launched a three-year initiative known as the Global Surveillance Monitoring and Advocacy (GSMA) project. The initiative focuses on detecting and investigating advanced surveillance technologies targeting journalists, activists and human rights defenders. The GSMA intends to advocate for change by using its forthcoming research findings to analyze how and where these technologies are being deployed.[103]

The Netherlands-based Humanist Institute for Development Cooperation (HIVOS), on the initiative of the Freedom Online Coalition, launched a digital defenders project in 2012, which aims to protect freedom of expression by providing emergency support for bloggers, journalists and others who are attacked while promoting and protecting human rights and democracy.

Latin America and the Caribbean

In Colombia, the Foundation for a Free Press (FLIP) monitors press freedom and journalists' safety through its alert and protection network. It has a network of 30 correspondents spread throughout the country who report on press freedom violations.

The International Center for Journalists (ICFJ) launched the Investigative Reporting Initiative in the Americas in 2013. This four-year program co-funded by the US Agency for International Development (USAID) and the US Department of State's Bureau of Democracy, Human Rights and Labor (DRL) focuses on promoting and strengthening transparency, security and freedom of expression for the media. offer country-specific workshops on digital and mobile security in addition to a variety of other training courses and activities.

Africa

The Special Rapporteur on Freedom of Expression and Access to information in Africa, Faith Pansy Tlakula, has integrated digital safety in her promotion on the safety of journalists. In 2014, she delivered remarks on the challenges that online journalism face, as part of the International Press Institute's News Innovation Platform's one-day symposium on digital media, including sustainability, security and self-regulation.[104]

In 2013, an initiative known as Unwanted Witness (UW) was established by Geoffrey Wokulira Ssebaggala, who recently won the European Union Human Rights Defender Award. Among its many undertakings, UW monitors government surveillance, offers legal support to bloggers, and advocates for digital rights.[105]

In early 2014, the African Freedom of Expression Exchange (AFEX) was launched. The network consists of African freedom of expression organizations, which are members of the International Freedom of Expression Exchange (IFEX). The network intends to embark on joint campaigns to ensure access to information for African citizens, promote the safety of journalists, seek justice for attacks against journalists and challenge laws that curtail freedom of expression. The network includes the following organizations:

- Media Institute for Southern Africa (MISA),
- The African Freedom of Information Centre (AFIC),
- The Center for Media Studies and Peace-Building (CEMESP),
- Human Rights Network for Journalists – Uganda (HRNJ-Uganda),
- Journaliste en Danger (JED),
- The Media Foundation for West Africa (MFWA),

- Media Rights Agenda (MRA), and
- National Union of Somali Journalists (NUSOJ).

Another organization working on digital journalism issues is the African Media Initiative (AMI). AMI is a pan-African organization, comprising more than 800 media companies in Africa that works to strengthen the continent's private and independent media sector and promote democratic governance, social development and economic growth.[106] Media consultant and ICFJ Knight Fellow Justin Arenstein heads AMI's digital innovation programme, where he helps to develop strategies and resources to help African media overcome disruptions and bolsters a digital skills programme, among other opportunities.[107]

Arab States

Independent Media Centre Kurdistan (IMCK) is a nonprofit founded several years ago in the Kurdistan Region of Iraq with support from Free Press Unlimited. It provides training programs to journalists and graduates who want to become journalists. It also conducts approximately 80 courses every year, some focused on Internet security.[108]

In December 2013, the Institute for War & Peace Reporting IWPR launched the Cyber Arabs Academy as an online platform for free courses on digital security in Arabic.

Asia-Pacific

In 2012, and in the face of the systemic insecurity of Pakistani journalists and bloggers, the Internews Center for Innovation and Learning produced an extensive report about Digital Security and Journalists: 'A Snapshot of Awareness and Practice in Pakistan'.[109] The report 'aims to highlight areas where journalists and bloggers in Pakistan are particularly vulnerable in their use of digital mediums, and makes some recommendations', namely the use of secure email services, encryption of data, or IP blocking services.

Digital Security Training Courses

A variety of individuals and organizations have responded to the need for greater digital security knowledge by developing specific training courses about digital security, including some of those mentioned under the section on norms and awareness above.

Global

UNESCO's Intergovernmental Programme for the Development of Communication provides annual grants to journalism safety initiatives, including online courses and capacity-building for digital security, as well as supporting safety indicators that include a digital dimension.[110] In March 2014, UNESCO, in cooperation with the Institute for War and Peace Reporting, organized a series of training courses on digital security for Tunisian journalists. The training courses consisted of two, four-day training workshops, with 29 participants total, including 16 women.[111]

At the 2014 RightsCon, the Access tech team hosted a digital security help desk, where its team spent two days diagnosing participant's computers, offering digital security advice, and helping participants implement digital security tools. The desk was busy during the conference, suggesting a previously unmet need for this help. To meet such needs, the IREX one-year pilot initiative known as SAFE opened three regional security resource centers in El Salvador, Georgia and Kenya in summer of 2013. SAFE tailors its assistance using local trainees to provide training in digital security, physical safety and psychosocial care for journalists.[112]

Article 19 provides a number of digital and physical safety training courses throughout the year at a variety of international locations. Article 19 staff also provide expertise on national legal frameworks and their relationship to freedom of expression and media ethics.[113]

While much training is sponsored and provided free of charge to participants, some organizations sustain their services by charging a fee for training. One example is Global Journalist Security, an organization founded and run by Frank Smyth, a long-term advisor to the CPJ.[114]

The International Press Institute (IPI) also held a digital security training in South Africa in 2014 as part of their News Innovative Platform.[115] The event, titled 'ChallengeSSS of the New Age' focused on sustainability, security and self-regulation.

North America and Europe

Digital security training is also happening increasingly online. Deutsche Welle Akademie hosted a week-long online training seminar on digital security for journalists around the world in December 2013. The seminar featured technologists from Tactical Technology Collective and Citizen Lab, as well as Internet freedom experts from organizations such as Reporters Without Borders.

The National Press Foundation in Washington DC and the Rory Peck Trust in London offered online training courses in 2013, which covered digital security issues for journalists globally. These training courses featured technologists and press freedom advocates from organizations such as the Tactical Technology Collective, the Electronic Frontier Foundation, and the Freedom of the Press Foundation. The Rory Peck Trust intends to further its work in digital security by developing and disseminating a guide to online safety. In addition, the Trust will continue working with partners such as the Frontline Freelance Register and the Guardian Project to provide digital security resources to freelance journalists.[116]

Latin America and the Caribbean

The Digital Journalism Center at the University of Guadalajara annually conducts a four-week 'Cobertura segura' programme for journalists in Mexico. In 2013, 14 journalists took part in the training. The workshop helps journalists to analyze and recognize threats and learn good digital security practices. Taught by a diverse set of experts including

local reporters who have worked on organized crime, the training typically focuses on prevention rather than reaction strategies.[117]

Derechos Digitales launched a campaign called: 'Do not fear the Internet: Privacy depends on us', which leverages videos and graphics to provide interesting and engaging advice on how individuals can take care of their personal data in the digital environment.[118] In Mexico, organizations such as Periodistas de a Pie, Social TIC and Article 19 have organized digital safety training courses.

In 2014, FOPEA (Argentinian Journalism Forum), in collaboration with CELE (Centro de Estudios en Libertad de Expresión y Acceso a la Información) and the 'Asociacion por los Derecho Civiles' (Civil Rights Association), organized a cybersecurity workshop for Argentinian journalists. The workshop was led by Robert Guerra, an expert in cybersecurity and human rights.[119]

The International Centre for Journalists (ICFJ) alongside the local Mexican organizations Investigation and Economic Teaching Centre (CIDE) and National Social Communication Centre (CENCOS), as well as NGO Freedom House, are developing digital security courses for journalists.[120] These courses will inform journalists of the security risks associated with smartphones, geolocalization and viruses. They will teach journalists how to safely navigate the web while protecting their communications and data bases.

The Inter-American Press Society (SIP) offers an online video seminar geared towards reporters and editors who wish to understand the risks associated with the use of social networks (Facebook, Twitter…) as well as gain the tools they need to prevent the 'hacking' of these networks.[121]

Asia and the Pacific

In Pakistan, organizations like the Digital Rights Foundation, Bytes for All and Bolo Bhi, have provided digital security training courses for journalists, bloggers and human rights defenders. Bolo Bhi's training courses are part of a pilot initiative called 'Securing Your Everyday Online and Offline' that gives free basic digital security training courses, conducts risk analysis, and gives tips for physical safety and digital security. Bolo Bhi intends to offer the courses once a month. In January 2014, the Digital Rights Foundation hosted a digital safety training in Pakistan specifically for women.

Digital security training guides and training curricula

Digital security training guides

North America and Europe

Numerous organizations besides some of those mentioned above have created digital security guides for journalists. Tactical Tech and Front Line Defenders have developed an online project known as 'Security-in-a-Box', which uses short scenarios to help journalists

better understand digital security threats. It includes recommendations for free software, provides video tutorials and is available in multiple languages. It is also frequently updated with new tools and tactics, including most recently a toolkit specifically for the LGBT community from Arabic-speaking countries.

Internews has a 'Speak Safe Toolkit' which provides journalists with information on how to be safer online and when using their mobile phones. The guide is available in Spanish, English and Arabic. The Rory Peck Trust has an online digital security resource for freelancers, arranged easily by topic and video screenshots, while Small World News has guides in English and Arabic on how to safely use satellite phones.

Reporters Without Borders has an online survival kit on its WeFightCensorship website. It explains the need to purge files of their identifying metadata, outlines how to use Tor and VPNs to anonymize and encrypt communications, and offers advice on securing communications and data on mobile phones and laptops.[122]

Other training guides include CPJ's 'Information Security Guide', Freedom of the Press Foundation's encryption guide, and the EFF's 'Surveillance Self-Defense Project', which is available in English and Russian. The EFF also writes a blog devoted to a variety of issues, including digital security concerns, known as the Deeplinks Blog.[123]

The Association for Progressive Communications, with support from the Swedish International Development Cooperation Agency, has released a resource titled, 'Digital security first-aid kit for human rights defenders', which provides concrete steps, further resources and references to support groups to whom activists and journalists can turn to for guidance.[124]

Arab States

Some training guides have replaced the text heavy approach in favor of video animation. One example is the 'Journalist Survival Guide' produced and released by the Beirut-based SKeyes Center for Media and Cultural Freedom. The guide is available in both Arabic and English and is geared toward professional and citizen journalists.[125]

Latin America and the Caribbean

Former Knight International Journalism Fellow Jorge Luis Sierra wrote a manual in 2013, entitled 'Manual de Seguridad Digital y Móvil' for Spanish speaking journalists and bloggers. The manual offers advice on creating risk-reduction plans and protocols for digital and mobile security and was published by the ICFJ and Freedom House.

Digital security training courses

Digital security training activities for journalists and others doing journalism are hosted by a variety of organizations, including academic institutions, NGOs working at the international level and local organizations. This section looks at what is being done to strengthen courses and trainers, and to mainstream digital security into wider training courses such as in university-based journalism schools.

One example is that of Internews which in March 2014 launched a digital security training curriculum and manual called 'SaferJourno' which has guidelines on best practices that digital security trainers can draw on when teaching journalists.[126] Internews has also launched a free and open-source, step-by-step training curriculum for digital security trainers. It contains six modules including 'Assessing Digital Risks', 'Avoiding Malware', 'Keeping Data Safe', 'Researching Securely', 'Keeping Email Safe' and 'Mobile Phone Safety'. The toolkit was field tested with trainers from the fields of broadcast, print and online, and peer reviewed by some of the leading experts in the digital security community.[127]

In 2013, UNESCO published a model syllabus on safety for journalists, covering the whole landscape of safety although not going in-depth about digital threats.[128] However, it appears that in a number of journalism schools, the digital security training is not yet systematically integrated into the curricula , even although many journalism educators appear to recognize that this is vital for journalism students.[129] This might be for a variety of factors including a lack of awareness and/or skill, inflexibility and/or time constraints in an already overcrowded journalism curriculum, disagreement over how digital security training should be taught and whether all journalism students need training on digital security.

One of the academic institutions spearheading digital security training for journalism is the USA-based Tow Center for Digital Journalism at Columbia School of Journalism in New York City.[130] In November 2013, the Center hosted a three-day workshop on digital security for journalists, bringing together security experts, journalists and lawyers. The workshop provided participants with an overview of how digital and physical security practices support and enhance journalism.[131] During 2014, the Center planned to identify best practices when teaching digital security for journalists, with the intent to eventually develop a methodology that can be used to teach journalism students about digital security. The Center has also launched Journalism After Snowden, an initiative that investigates journalism in an age of state surveillance.

Columbia Journalism School and Columbia University's Department of Computer Science have created a new post-baccalaureate certification programme that will seek to improve digital literacy for journalists. Entitled the Lede Program, it will offer hands-on training in data and data technologies taught in the context of journalism.[132]

Some professors have taken it upon themselves to ensure their students understand risk analysis and digital security basics by incorporating theoretical discussions of digital security training into their existing classroom curriculum. At the University of Minnesota, Jane E. Kirtley, Silha Professor of Media Ethics and Law, teaches an upper-level class on the contemporary problems in freedom of speech and press and discusses digital security of journalists as it relates to online privacy and data security.[133] At the City University of New York (CUNY) Graduate School of Journalism professor Sandeep Junnarkar has added digital security training to his curriculum by creating a 4-hour workshop that focuses primarily on tactics and tools.[134] Investigative journalist and professor at Arizona State University's Walter Cronkite School of Journalism and Mass Communication, Steve Doig, has presented a lecture on surveillance and spycraft every semester for several years, but only recently has he seen a significant uptick in interest.[135] According to an

article in Columbia Journalism Review, Doig's lecture is often the first time that students hear about security vulnerabilities and the steps journalists need to take should they encounter top secret sources.[136] The Knight Center for Journalism in the Americas in Austin, Texas has also organized online webinars on online safety issues.

In Turkey, one professor who has integrated digital security training into his curriculum is Ismail Hakki Polat, a professor of New Media at Kadir Has University. He teaches information security to students in two different courses and has been doing so since 2010.[137] The coursework includes an introduction to basic concepts of information security, cryptography, real time communication security, and laws and regulations on information and security, among other topics.[138]

In Mexico, former ICFJ Knight Fellow, Jorge Luis Sierra, created an online and in-person training curriculum on digital and mobile security for the Center for Education on Digital Journalism at the University of Guadalajara.[139]

Other journalism teaching institutions are beginning to consider integrating digital security into their journalism program's curriculum. At the Danish School of Media and Journalism, professors discuss the issue of digital security with students, although this was not formally integrated into their program at the time of writing.[140] While not affiliated with a university, BBC Academy College is a journalism institution that trains journalists for the BBC. It is planning to offer digital security training for journalists, but this had not been fully deployed at the time of writing.[141] The Medill School of Journalism at Northwestern University in the USA recently published a digital security guide by Executive Director of Global Journalist Security, Frank Smyth, although they too had not yet integrated digital security training in their curriculum at the time of writing.[142]

Hotlines and Safety Assistance

Many organizations provide security assistance, although they prefer not to publicize these resources outside of their trusted networks, for fear of compromising the safety of their staff and their operations. As a result, they have not been included in this report. Other, more public options have been outlined below.

Global

Safety assistance programs for the physical protection of journalists have existed for several years from organizations including CPJ, Reporters Without Borders, and the International News Safety Institute. These safety assistance programs are valuable and often provide legal, medical, and relocation assistance to journalists and their families. Many of these organizations, including the International Committee of the Red Cross, provide hotlines for journalists to call when they experience trouble and need resources.[143]

Interviews with experts suggest it is fairly common for press safety and advocacy organizations to connect journalists with technologists. However, with the seeming

increase in digital attacks against journalists, there is a need for more organizations to provide rapid response assistance to journalists who experience digital attacks.

One organization addressing this need is the international non-governmental organization Access, which in 2013 launched a rapid-response system to mitigate digital threats facing activists and journalists. As part of the rapid-response system, Access operates a hotline that journalists can call for immediate digital security help, should they suspect or be victim of a digital attack.

IREX's SAFE programme also provides a hotline for journalists seeking digital security help, including troubleshooting with tools and techniques, as well as referrals to other organizations, which may be able to assist in case of danger.[144]

Many technologists are increasingly joining forces with human rights and press protection organizations to help journalists improve their digital security, circumvent censorship and avoid surveillance. Sometimes these meetings are known as 'hackathons', an intensive collaboration of programmers and experts on a software project or issue over a short period of time, often in the same physical location.[145]

Numerous organizations host hackathons. One such organization is the Open Internet Tools Project (Open ITP). Open ITP is a USA-based organization that supports software creators and communities who develop open source anti-surveillance and anti-censorship tools.[146]

Open ITP and CommunityRED recently hosted a 'DC Internet Freedom Hackathon' in Washington DC, where participants learned about tools to bypass censorship and received user-generated feedback on these tools. More hackathons are planned in the near future.

Open ITP also created Techno-Activism 3rd Mondays (TA3M), which are informal meetups designed to connect software creators and activists who are interested in censorship, surveillance and open technology. Currently, TA3M are held in 16 cities around the world, with more expected in the near future.[147]

Another organization fostering hackathons around the world is the rapidly expanding international grassroots journalism organization known as Hacks/Hackers. The self-described goal of the organization is to create a network of journalists ('hacks') and technologists ('hackers') who rethink the future of news and information.[148] Numerous local chapters exist in countries around the world and members host talks, demo days, and hackathons.[149]

Two journalists created an app called Hancel to improve safety of journalists in Latin America. Hancel is a cell phone application for Android that allows journalists to program automatic alerts in case of an incident and to also report issues as they happen. The journalists work closely with the Foundation for Press Freedom (FLIP) in Colombia and are currently developing a pilot project for Colombia and Mexico. The project received funding from the Knight Foundation.[150]

Reports and Research

International

Reports by Freedom House and Reporters Without Borders provide valuable data and context about the types of attacks and threats facing journalists and other actors producing journalism with digital technologies, including human rights defenders around the world.

Freedom House released a report summarizing findings from its conference in November 2013 about the safety of journalists and other actors producing journalism with digital technologies.[151] The report outlined a series of recommendations for organizations and funders to implement, which would provide better protection for journalists and human rights defenders online.

Global Voices' 'Threatened Voices' crowd sourced map records threatened bloggers around the world, while the ICFJ also produces maps to document attacks..

PEN America recently conducted a survey of its international members to document digital attacks that writers face, creating an infographic report for easy understanding of the results.[152]

CPJ's annual 'Risk List' and 'Attacks Against the Press' report has begun to include issues of cybersecurity, drawing attention to the issues journalists face in this arena.[153]

North America and Europe

The Tow Center hosted a three-day workshop on digital security for journalists in November 2013 in New York, bringing together a diverse group of digital technologists and journalists. The workshop trainers taught participants about networks and the Internet, and provided hands-on training on ways to bypass censorship and avoid surveillance. The lectures and discussion were off the record, but the Tow Center filmed and took notes for research purposes and planned to create and disseminate a report on best practices in 2014.

Latin America and the Caribbean

Article 19 and the Electronic Frontier Foundation have developed memoranda outlining bloggers rights, while other organizations are publishing information about the rights that journalists and other actors producing journalism with digital technology have, including the right to privacy, and the issues of data protection and access to data.

2.4 Gender perspective on safety issues

Introduction

According to Irina Bokova, the Director-General of UNESCO, female journalists are sometimes victims of a 'double attack', because they are targeted for both being a woman and a journalist.[154] Indeed, nearly two-thirds of female journalists surveyed in a recent study said they had experienced acts of 'intimidation, threats and abuse' in relation to their work,[155] and nearly half of respondents said they had experienced sexual harassment[156] at their jobs.[157] Journalists experience sexual assault and rape which can occur in reprisal for their work, during public events by mobs, or when journalists are in detention or captivity.[158]

The online world often reflects, and may amplify, the realities and hierarchies that exist offline.[159] Online abuse against women is a growing international phenomenon, in forms ranging from sexual harassment to rape threats and gender-based hate speech.[160] Between 2000 and 2012, 72.5 per cent of harassing incidents collected by the USA-based organization Working to Halt Online Abuse were directed toward women.[161]

Researchers from the University of Maryland's Electrical Engineering and Computer Department conducted an experiment that found that online accounts that have feminine names received an average of 100 sexually explicit or threatening private messages a day, versus an average of 25 for ambiguous names and 3.7 with masculine names.[162] This study was not geared toward journalists, but it shows how women online in general can be harassed even without any communication from their side.[163]

There is evidence of a number of female journalists and others who contribute to journalism experiencing online sexual harassment, violent threats, gender-based hate speech, and cyberstalking. According to a study by the International News Safety Institute and the International Women's Media Foundation, more than 25 per cent of a number of respondents to an online questionnaire stated that they received online verbal, written and/or physical intimidation including threats to family or friends.[164]

The next section presents more detailed discussion of this subject, including some campaigns and initiatives that are seeking to mitigate these acts.

Digital threats and abuse

Online sexual harassment, including sexist comments and violent threats

Online sexual harassment has not been well defined, making it difficult to recognize and respond to cases. 'The refusal to recognize harms uniquely influencing women has an important social meaning – it conveys the message that abusive behavior toward women is acceptable and should be tolerated', says Danielle Keats Citron, a professor

at the University of Maryland School of Law. Perpetrators are often viewed as 'juvenile pranksters' and victims are seen as 'overly sensitive complainers'.[165] To respond to the lack of a clear definition and encourage opportunities for redress, Citron clarifies key characteristics of what she calls 'cyber gender harassment': 1) its victims are female, 2) the harassment is aimed at particular women, and 3) the abuse invokes the targeted individual's gender in sexually threatening and degrading ways.[166] Citron believes it is essential to recognize cyber harassment as gender discrimination and raise public awareness to ensure that the victim's stories are heard, to persuade perpetrators to stop their online vitriol and successfully change online subcultures of misogyny to equality.[167]

According to Anja Kovacs, who heads the Internet Democracy Project, women who write online about politics, religion, feminism or sexuality experience more online abuse than those who write about less controversial topics.[168] Kavita Krishnan, a political commentator and activist in India, knows this first hand. She says that online abuse grows more vicious when she voices her political opinions. Threats have ranged from sexual assault to the mutilation of genitals.[169]

Krishnan told *The Observer*: 'Women are subjected to enormous hate speech. Of course there's always vitriol in politics, but this is designed to intimidate women.'[170]

According to female columnist Laurie Penny, who writes for *The Independent* newspaper in London:

> You come to expect it, as a woman writer, particularly if you're political. You come to expect the vitriol, the insults, the death threats. After a while, the emails and tweets and comments containing graphic fantasies of how and where and with what kitchen implements certain pseudonymous people would like to rape you cease to be shocking, and become merely a daily or weekly annoyance, something to phone your girlfriends about, seeking safety in hollow laughter.
>
> … Most mornings, when I go to check my email, Twitter and Facebook accounts, I have to sift through threats of violence, public speculations about my sexual preference … and attempts to write off challenging ideas with the declaration that, since I and my friends are so very unattractive, anything we have to say must be irrelevant.[171]

Female journalists who enter the online fray to write about or discuss politics or other contentious issues are often disrupting the image that some men have of women more generally, which results in their being attacked. These perpetrators likely expect women to be submissive, and that it is their right to use coercive measures such as misogyny to discipline women who are not acting servile.[172]

Sexist comments toward female journalists

Female journalists often receive online comments that focus on physical appearance rather than professional accomplishment.[173] This is 'a kind of visual shorthand that cannot really be used in the same way to dismiss or demean a male reporter', said one female

journalist who was targeted.[174] One journalist noted that her husband, also a well-known journalist, receives vicious attacks on Twitter for his views, but that the comments are not sexually violent in nature against him, like they are against her.[175] According to Suzanne Franks, a professor of journalism at City University in London and recent author of Women and Journalism, 'When someone disagrees with a man's article they go for the ideas which are in that article – with women they go for her looks, fashion and it turns very personal.'[176]

A *New York Times* article in January 2014 reported that many of the anti-genetically modified food arguments at public hearings taking place in Hawaii ignored science. An advocacy group was displeased by the article and responded by digitally pasting the face of the author atop an image of a woman in a leopard-skin bathing suit. The image, posted on Food Democracy Now's (FDN) Facebook page, showed the author smiling while on the beach, holding hands with the chief executive of the biotech and seed company.[177] The caption read, '*New York Times* writer … travels to Hawaii ... falls in love with GMOs'. Shortly afterward, several people posted comments below the photo taunting the author with sexist insults. After some commentators complained that the image of the author was incompatible with the values of a group espousing progressive activism, the advocacy group defended it as 'satire, not sexism'.[178]

Threats of rape and other violence toward female journalists and their families

Threats of violence against journalists' families, especially threats to rape female children or murder them, seem to be more prevalent toward female media professionals and are reportedly extremely effective in silencing them.[179]

A prominent television news anchor in Latin America who has worked for nearly 20 years investigating human trafficking, arms trafficking and extrajudicial killings has faced repeated threats and harassment over several years. It was not until she received intimidating phone calls that threatened her young son, however, that she felt forced to take leave of absence from anchoring her investigative morning news programme.[180]

One female journalist received a bomb threat on Twitter the day after she wrote an article that highlighted online misogyny and abuse.[181] Other journalists received the same type of threat (including from *The Independent*, *The Daily Telegraph*, and *TIME*). These attacks are believed to have been linked to a campaign of violent threats made against other another high profile female journalist and a member of parliament who successfully lobbied for British novelist Jane Austen to be pictured on UK bank notes.

One of the journalists who was targeted said,

> That crystallized for me something I had already suspected, which was that the reason I had received the bomb threat was because I was female. In a way, that made sense of a nonsensical situation. … I think the only provocative thing I did was to be female and to be on Twitter, and to have some modicum of a public profile, and have opinions.[182]

In another case, a Twitter account handle with the name Tehreek e Taliban threatened renowned female Pakistani journalists, as well as others, in a series of tweets, in response to their writing: such as 'These Tweeps Must Stop Puking Against Talibanor We ll Kill Them', or 'No Matter How Much Safe You Feel Inside Your Houses, Remember You Are Always in Our Access – Stop Propaganda Or Get Ready to Be Killed', etc.

In response to the tweets, some of the female journalists reached out to a digital security technologist and trainer for help in better securing their digital communications.[183]

Cyberstalking

Cyberstalking is when someone uses electronic communications to track and repeatedly harass an individual or group, whether online or through digital means.[184,185] Debate still exists over whether cyberstalking is another tool for individuals who engage in traditional stalking, or whether it should exist as a separate concept with separate motives.[186] However defined, cyberstalking, like other forms of abuse, affects mainly women.[187] For example, a survey in India found that victims ages 18 to 32 were predominantly female.[188] In the USA, it is believed that more than one million women and 370,000 men are annually stalked. One in 12 women will be stalked in their lifetimes, compared to one in 45 men.[189] According to the US National Criminal Crime Victimization Survey, women comprised 58 per cent of the victims in cyberstalking cases,[190] and WiredSafety, an online safety group, found that women are the most likely targets of cyberstalkers.[191]

Cases of cyberstalking are expected to rise.[192] This may be a function of several factors. First, it is relatively easy to collect often intimate details about a person online, especially if the victim produces and disseminates revealing content. Second, an attacker is able to track his or her victim fairly easily if the victim does not implement digital security practices that better protect her or his privacy. Third, an attacker can disseminate information about the victim through various online means, reaching a wide and potentially captive audience quickly. Fourth, the distance provided by online communication strengthens the 'disinhibition effect' which means that the perceived consequences of an individual's actions, such as verbally abusing a target or revealing intimate details, are dramatically lessened when the perpetrator does not have the normal boundaries of saying something to their victim's face and seeing their reaction.[193] The disinhibition effect and the ability to remain at least partially anonymous and potentially unaccountable also may influence the degree to which an attacker stalks their victim, or their persistence in doing so.

An award-winning television journalist was sent abusive emails by a stalker whom she suspects hacked her private and work email accounts. In the emails, the stalker describes items in her home and family member names. Despite help from law enforcement and technology experts, she still felt compelled to change her locks, install new security systems in her home, and eventually move cities. After five years of sustained harassment, she quit her job, hoping that would stop the harassment, but the cyberstalking continued.[194]

Consequences and Significance

Online harassment and cyberstalking have numerous consequences for their victims including psychological, convenience and financial costs. After experiencing online threats and abuse, journalists may be increasingly concerned for their personal security and start using pseudonyms when they publish, or stop writing about a story or topic entirely. Others may stop reporting from specific localities, or be forced to relocate. Some journalists are forced to give up journalism or leave their jobs entirely.[195]

Online harassment can also cause significant emotional distress, leading to psychological ailments such as depression.[196] Journalists may have to spend money on legal fees to fight online perpetrators in court, or purchase online protection services that systematically remove personal information from websites. They may also experience a loss of income because they are too psychologically traumatized to continue their profession.[197]

Sexist encounters may also impact on wellbeing.[198] In one study of undergraduate college students in the USA, many of the participants reported increased anger and depression, and diminished self-esteem, on par with their exposure to sexist behavior.[199] The same may apply to online experience and to women engaging with the Internet to do journalism.

Meanwhile, mob mentality can occur when dealing with groups of individuals in online forums. Individuals may see other people attacking someone and join in to be part of the group.[200]

Campaigns and Initiatives

At least one study, which involved undergraduate students as participants in the USA, has shown that standing up to sexism reduces prejudice and discrimination in the long term.[201] Another study has shown that confronting sexism in the offline world makes those who speak up feel better than those who choose to remain silent.[202]

Recent media coverage has documented campaigns that women have launched on Twitter in response to online harassment and threats. In 2011, a feminist writer started a Twitter hashtag, #MenCallMeThings, to document harassment and threats. She dedicated a website to documenting women's experiences and found that 'men are using the same insults and sentiments to shut down women and 'feminine' people, across the board… it's about gender.'[203] The campaign raised awareness of the different types of threats that women face online. Another journalist created the hashtag #silentnomore, which she started to encourage women to speak out about their experiences and confront pervasive and malicious comments.[204] Bloggers from Egypt, Sudan, Syria and Lebanon have encouraged people to speak out against harassment and gender violence by using the hashtag #EndSH on Twitter. Additionally, campaigns have been created to confront sexism and misogyny, such as Everyday Sexism's #ShoutingBack and #MisogynyAlert, which allow anyone to call attention to verbal abuse and respond to the perpetrators.[205]

An online research project on Tumblr called 'Said to Lady Journos' is a repository for anonymous comments toward female journalists. These campaigns are valuable because they seek to change the existing norm of what is perceived as acceptable as they strive to shift the onus from the abused to the abusers.

Another campaign that works to reduce gender-based violence against women is the collaborative campaign 'Take Back the Tech' which began in January 2009 and aims to reclaim information and communications technologies to end violence against women.[206] The campaign brings significant resources to 12 developing countries for documenting violations of women's rights online, provides capacity building for activists and survivors in the creative and safe use of technology, and advocates for policies to strengthen protection of rights online. The project is part of a global effort to achieve gender equality, as outlined in the United Nations' Millennium Development Goals.[207] The campaign occurs during the event 16 Days of Activism Against Gender-based Violence (25 November to 10 December every year).

The campaign calls on all users of information and communication technologies, but especially women and girls, to take control of technology by strategically using ICT platforms (i.e. mobile phones, blogs, etc.) for activism against gender-based violence. It sets out to:

- Create safe digital spaces that protect everyone's right to participate freely, without harassment or threat to safety;
- Realize women's rights to shape, define, participate, use and share knowledge, information and ICT;
- Address the intersection between communication rights and women's human rights, especially against violence against women; and
- Recognize women's historical and critical participation and contribution to the development of ICT.

Take Back the Tech's article, 'CyberStalking and How to Prevent It'[208] is a good resource on ways to prevent cyberstalking. Tack Back the Tech also has a mapping project that documents harassment, stalking, threats and abuse.[209] Another initiative focused on raising awareness of sexual harassment is Harassmap, which collects SMS's and online reports of sexual harassment and assault and maps them on Harassmap. It uses the information and analysis from this research to create communications campaigns that address sexual harassment and assault. In so doing, Harassmap seeks to dispel myths and stereotypes about sexual harassment and assault, change perceptions that put blame on the harassed/assaulted and mobilize people to stand up to harassment.[210]

Corporate responsibility

Social media websites and blogs are constructed in such a way to encourage freedom of expression. As such, they carry an inherent risk for misuse by actors seeking to harass and/or cyberstalk. Rather than arbitrarily restricting freedom of expression, social media

and blogging websites should ensure they offer their customers clear terms of use and opportunities for redress if users are victimized. Two organizations which have taken steps in this direction include Tumblr and Twitter, although there may be many more. Tumblr's more explicit terms-of-service agreement,[211] which give an overview of what is and is not acceptable, may result as a deterrent in some cases.[212] Twitter's 'report abuse' and block buttons enables users to take more control over the content directed at them.

Although corporations have a role to play in mitigating abuse on their user platforms, it is important that journalists and others increase their digital literacy to understand how much data and personal information they are sharing on social networks and blogging websites to begin with. A study has shown that individuals in general still perceive that the benefits of online social networking outweigh the risks of disclosing personal information. The study also found a discrepancy between users' reported understanding and caution in regards to privacy and actually implementing specific steps to maintain privacy. People may say they are familiar with privacy settings, but they still engage in behavior, such as accepting people as friends whom they do not know, that puts their privacy at risk.

Overall, more research needs to be conducted on the forms of online abuse that female journalists face. Anecdotal information and small-scale study findings point to female journalists being particularly targeted and reflective of the offline hierarchy of power. However, a quantitative study focused on this topic would provide deeper insights into the phenomena afflicting female journalists and point to some possibilities for mitigation of these threats.

3. CHALLENGES AND RECOMMENDATIONS

3.1 Introduction

This section of the report identifies specific challenges facing journalistic actors interfacing with digital technology and offers concrete recommendations to the diverse set of actors involved. The protection of journalism entails actions at three levels – (a) state power, (b) media institutions' policies, (c) and the behavior of individuals and their associates. The recommendations that follow highlight the potential of the following organizations and individuals:

- UN bodies,
- International organizations (governmental and non-governmental),
- Regional organizations,
- Governments,
- Corporations,
- News organizations,
- Journalism schools and other educational and training institutions,
- Journalist associations, and
- Journalists and others who contribute to journalism.

The ultimate goal of addressing these challenges is to improve the safety and protection of all those who contribute to journalism. The issue of digital security is complex because it extends across the entire value chain of digital communications. From devices to infrastructure used to transmit and store data, it also includes the acts of electronic interviews and research and communication of data, as well as publishing and interaction. It is not a purely digital realm – for example, devices can be physically stolen or destroyed – not merely subject to electronic theft or disruption. Location and social media data can be used for targeting and timing of physical attacks.

The dimensions of safety are many, and cover aspects as diverse as the technological, institutional and economic, as well as political, legal, and psychosocial.

3.2 Challenges and recommendations[213]

1. Technological, institutional and economic challenges

Journalists and others who contribute to journalism face a variety of technological challenges when carrying out their work. These can range from the practical – such as the limited usability of digital security tools or the lack of a sustainable funding model to support regular buying or updating of digital security tools – to the more complex, such as weathering actual digital attacks and threats.

Challenge 1.1: Some digital security tools are not user friendly, which may lead to few journalists adopting or implementing the tools correctly or at all. Thus, the researchers suggest the following recommendations to specific parties:

- ***Recommendation*** (corporations and others): Encourage corporations and open-source technologists to build tools with consumer-level usability and security built-in.
- ***Recommendation*** (international organizations): Continue to raise awareness of the evolving threats that digitally interfaced journalists face, in order to encourage market demand for digital security tools.

Challenge 1.2: Surveillance, data storage capabilities and digital attack technologies are becoming less expensive and more pervasive. In response, there has been increased debate among key stakeholders about developing protocols that encrypt Internet traffic more generally.

- ***Recommendation*** (corporations): Strongly consider developing end-to-end encryption for services.
- ***Recommendations*** (corporations):
    - Ensure websites and other services enable encryption by default (SSL/TLS) in order to always provide users a secure version of their website.
    - Encrypt the transfer of customer data between data centers, not just between a data center and the user's computer.
    - Use 'perfect forward secrecy', which uses randomly generated, ephemeral keys. This prevents an outside body from being able to decrypt communication, even if it manages to obtain the secret key for encrypted traffic, because they do not have the specific session key. Perfect forward secrecy is perhaps even more important following the disclosure of the Heartbleed bug, which threatened the security of HTTPS on the web.
    - Authenticate and encrypt download channels when providing software update services to prevent these updates from being hijacked and used to download malware.

- Increase transparency and provide clear terms of use for services that collect data from users. Although data collection is a business model for many corporations, seek to minimize and anonymize data collection from services.
- Consider developing more open-source technologies to facilitate transparency and help to ensure the product code has not been weakened by governments or other entities.

- ***Recommendation*** (all stakeholders): Use and promote the use of open-source encryption technologies such as HTTPS Everywhere, so as to facilitate more secure channels.

Challenge 1.3: Journalistic actors often cannot afford commercial software that provides digital security; therefore they need to rely on open-source technologies that are free. However, open-source digital security technologies are often conceptualized and developed without the likelihood of sustainable funding, making them problematic to use if they lack funding to remain updated against vulnerabilities.

- ***Recommendation*** (all stakeholders): Encourage donors to provide funding or other resources to help facilitate the maintenance and update of open-source digital security tools for journalists and human rights defenders, which will help to ensure open-source technologies remain available and updated. Although developers who work on open-source technologies generally do so for the intrinsic love of developing, resources aimed at helping the project become sustainable would help to ensure that journalists and human rights defenders are able to use up-to-date, verifiable open-sourced tools.

Challenge 1.4: DoS attacks may result in financial loss for news organizations or individual journalists.

- ***Recommendation*** (international organizations, governments): Help to fund those organizations which provide free support to journalists and news organizations facing DoS attacks.
- ***Recommendation*** (news organizations and journalism institutions): Employ system administrators who have knowledge about mitigation strategies in order to limit and/or prevent damage inflicted by DoS attacks.

Challenge 1.5: Many producers of digital journalism are unaware of technologists willing and able to assist them if they experience a digital threat or attack, and many technologists who are willing or able to help journalists do not know where to link with those in need.

- ***Recommendation*** (international organizations, news organizations, journalism schools, educational and training organizations): Employ staff technologists who can provide rapid-response help to media actors experiencing digital attacks or network with local facilities or actors who may be able to assist.

- ***Recommendation*** (international organizations): Consider providing a digital security hotline that connects media actors with technologists in different areas around the world and provides 24-hour, year-round assistance.
- ***Recommendation*** (press freedom NGOs, international organizations): Support the creation of an international community of media security experts who can be leveraged by news organizations and journalists for their expertise.

Challenge 1.6: A lack of publicly available data documenting the types of digital attacks and threats facing journalists and others doing journalism.

- ***Recommendations*** (international organizations): Develop a comprehensive, anonymized database that catalogues the number and type of digital attacks against journalists.
- ***Recommendations*** (UN and international organizations): Develop indicators to measure how journalistic actors interfacing with digital technology are being threatened and attacked, including digital threats and digitally relayed threats to better create strategies to inform and protect them.

Challenge 1.7: Location tracking technology can identify media actors and their sources, with the aim or effect of breaking the confidentiality between them, or for mounting physical attacks.

- ***Recommendation*** (international organizations, journalism training institutions, news organizations): Educate digitally interfaced journalistic actors on how to disable location tracking on their electronic devices (although devices with batteries that cannot be removed may prevent this possibility). Practitioners should have awareness raised of how applications and websites may silently geo-track online movements.

Challenge 1.8: The digital security of both those who do journalism and their associates (sources, families and colleagues) can often be easily compromised via phishing campaigns.

- ***Recommendation*** (news organizations and journalism institutions): Provide regular training for journalists and others on best practices in digital security and create a learning culture of strong information security to reduce risk.

Challenge 1.9: Compromised user accounts and devices can be used to identify the sources and networks of those doing journalism, leading to increased insecurity for journalists and their sources.

- ***Recommendation*** (news organizations, international organizations, journalism institutions): Train journalists on how to secure their laptop and other electronic devices in case they are confiscated or stolen. Teach journalists how to set up and consistently use technologies that can obfuscate sensitive information on their electronic devices in accordance with their threat model.

- ***Recommendation*** (corporations): Consider offering two-factor authentication to prevent unauthorized hacking into user data – for example, password and text message – bearing in mind that a smart phone may invalidate such systems by combining services on a single device.

2. Political and/or legal challenges

Any legitimate limit on freedom of expression or privacy should be narrowly defined, proportionate and justifiable to ensure that those doing journalism can still carry out their role providing and disseminating independent information that helps to inform society and government. Unfortunately, many stringent laws and policies exist with overly broad interpretations that can serve to unduly restrict freedom of expression and privacy. In addition, laws and policies are not keeping up with the rapid pace of technological change, leading to gaps in the protection of journalists and others doing journalism. Political and legal challenges facing journalists include ambiguous and opaque laws around data retention and surveillance, few export controls on technologies that have been used to repress human rights, and a lack of political will to address crimes against journalists.

In the wake of the 2013 surveillance revelations, the public, political actors, journalists and news organizations have shown an increased interest in digital security knowledge, tools and training courses; however, more awareness raising and normative consolidation needs to occur globally to ensure journalists and others who contribute to journalism have contextual backing to carry out their work as securely as possible.

This section will outline these challenges and proffer recommendations to mitigate them.

Challenge 2.1: Levels of knowledge and advocacy ability for the implementation of political and legal standards concerning digital security need to be increased.

- ***Recommendation*** (all stakeholders): Keep abreast of evolutions in international standards, such as resolutions at the UN Human Rights Council, civil society initiatives (e.g. Necessaryandproportionate.org), and industry measures (e.g. the Global Network Initiative). Use these for advocacy efforts to underline the importance of digital safety being promoted and respected.
- ***Recommendation*** (governments): Cognizance should be taken of the UN General Assembly resolutions on the Right to Privacy in the Digital Age.[214] These call on states to 'review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy.' They further call for all states to establish or maintain existing independent, effective, adequately resource and impartial domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data. Cognizance should also be taken of UNESCO's 37 C/Resolution 52, which notes that 'privacy is essential to protect journalistic sources, which enable a society to benefit from

investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference.'[215]

Challenge 2.2: Surveillance technologies are at times exported to countries with poor human rights records and reportedly used to target journalistic actors and members of civil society.

- ***Recommendation*** (governments): Monitor the classification of surveillance technology under the Wassenaar arrangements and act accordingly.
- ***Recommendation*** (international press protection/press freedom organizations): Advocate for governments and other actors to consider the International Principles on the Application of Human Rights to Communications Surveillance.
- ***Recommendation*** (international organizations): Encourage companies to acknowledge to which countries they sell surveillance technologies.
- ***Recommendation*** (corporations): Pledge to not sell surveillance technologies to clients where these might be abused.
- ***Recommendation*** (regional organizations and governments): Incorporate the promotion and protection of human rights online in foreign relations, including development and assistance programs, trade agreement negotiations and public tender processes where appropriate.

Challenge 2.3: Lack of political will to address crimes against those doing digital journalism, resulting in a climate of impunity.

- ***Recommendation*** (governments): As a prerequisite, condemn unequivocally all attacks and violence against journalists and media workers, as outlined in the UN Resolution on Safety of Journalists and the Issue of Impunity, adopted in December 2013.[216]
- ***Recommendation*** (UN and international organizations): Continue to advocate for governments to prevent attacks against journalists and those who contribute to journalism. Encourage full, impartial and prompt investigations by officials and analysts, as appropriate to the situation, and in accordance with national and international laws.
- ***Recommendation*** (governments): Create independently monitored national mechanisms that promote transparency, accountability and judicial process in regard to attacks against journalism, including in regard to digital attacks, and report on judicial follow-up in cases of lethal attack as requested by the UNESCO Director General on mandate of the Organization's member states.

Challenge 2.4: The integrity and security of networks should be respected and protected, and vulnerabilities fixed rather than exploited.

- ***Recommendation*** (governments): Authorities should refrain from exploiting vulnerabilities, and from creating 'back-doors' because such actions can enable abuse, overreach and opportunities for other actors to enter systems.

- ***Recommendation*** (governments): Where Internet service providers, including those operated by state telecos, are manipulated to redirect users to websites with fake content and to websites that have malware, governments should take action to stop this.

Challenge 2.5: Digital attacks, including surveillance and targeted malware are difficult to attribute, leading to increased impunity of attackers.

- ***Recommendation*** (international organizations): Encourage funding of organizations which have the technical capability to analyze digital attacks.
- ***Recommendation*** (journalism schools and educational institutions): Encourage journalism students to develop expertise in digital security and malware analysis to empower themselves and combat digital threats and attacks.
- ***Recommendation*** (UN): Urge governments to increase transparency surrounding the export of surveillance systems.
- ***Recommendation*** (journalists): If a digital attack is suspected, send equipment to recognized security technologists to be analyzed. They can identify the malware, clean the device and use the malware sample to improve malware detection software.

Challenge 2.6: Vast amounts of data may be easily stored and mined to reveal media actors' networks and sources.

- ***Recommendation*** (corporations and government): Review data retention policies with an eye toward privacy and data minimization associated with consumer accounts (e.g. limiting the length of time that data and activity logs are kept and tightening security against hacking).
- ***Recommendation*** (corporations): When appropriate, fight unreasonable data requests from governments or others seeking personal user data and seek guidance from reputable nonprofit organizations. Doing so can result in heightened public awareness of privacy issues and set norms for transparency.

Challenge 2.7: Sanctions can result in reduced availability of technology or software updates needed for journalistic actors to stay safe.

- ***Recommendation*** (UN and governments): Evaluate the cost of sanctions through both a human rights lens and a security lens, taking into account potential unintended consequences.

3. Psychosocial

Journalistic actors who are unaware of digital security best practices could find themselves unwittingly exposing their sources, even if they practice strict operational security. However, journalistic actors, including media organizations, also need to take it upon themselves to ensure that they adopt a security mindset to their journalism activities.

Operational and digital security cannot be a last minute addition to their work. Instead, they need to adopt a security mindset and ensure that their chain of communications and networks are protected. When doing so, media actors still need to adopt the appropriate level of security, so as to not become paralyzed with indecision or overwhelmed.[217]

The problem is that many journalists and online producers of journalism are ignorant of the digital security threats they may face when reporting or disseminating information. Others may be overwhelmed by the rapid pace of technological change and the need to continuously adapt to new distribution networks, business models and digital security threats.[218] Digital security tools are often complex and not user-friendly. A lack of easy-to-use tools combined with an overwhelming amount of information about digital security risks and different tools to use may result in ambivalence among media actors, leading to decision-fatigue and an all-or-nothing digital security approach. Adding to the disarray is a fundamental lack of understanding of how digital communications and networks work. It is easier for producers of journalism to not implement digital security tools if the repercussions are not obvious or appear unlikely. Journalists face many challenges, including a lack of understanding of how 'digital hygiene' can affect physical security and psychological well-being and how unaddressed traumatic experiences may reduce a journalist's ability to successfully carry out physical and digital security practices.

Challenge 3.1: Journalists may improperly apply or avoid implementing digital security tools because they are unaware in general of digital security threats, or unaware of the connection between digital security hygiene and physical safety and psychological well-being. They also may lack easy-to-use digital security tools.

- ***Recommendation*** (international organizations, journalism schools, educational and training institutions): Ensure digital security training is holistic and includes operational security and psychosocial care. Also include a gender-sensitive and trauma-sensitive lens during the training to best reach journalists who have experienced traumatic events related to their security, or who, because of their gender, have not received training before.
- ***Recommendation*** (corporations): Remind users to set their account security settings to ensure more secure browsing, receive login notifications for their accounts, and explain how they can monitor account activity.
- ***Recommendation*** (corporations): Encrypt software programs, applications and other technologies by default.

Challenge 3.2: Too few online media actors understand digital security principles and/or their application.

- ***Recommendation*** (journalistic actors): A logical starting point to any digital security practice is to conduct an individualized risk assessment and develop a security plan to carry it out to ensure a reasonable and feasible digital hygiene practice.[219]
- ***Recommendation*** (UN, international organizations, governments, journalists, journalism schools): Consider the integration of what UNESCO calls Media and

Information Literacy (MIL) as an essential competency for citizens, along with other literacies.[220] Doing so will help to inform and empower journalistic actors interfacing with digital technology and help them to make use of and protect their rights and freedoms. On a wider level, UNESCO has done considerable work in developing the 'Global Media and Information Literacy Assessment Framework,' which provides a conceptual and theoretical framework and introduces the rationale and methodology for conducting an assessment of country readiness and competencies at the national level. This information is relevant not only to journalism but to all public users of digital communications. The framework can help UNESCO member states monitor the effectiveness of current practices and policies, and design action-oriented plans that relate to country-specific contexts and conditions. A public that is MIL-savvy can only be a boon to journalists interacting with them, including through digital means. For this reason, journalists and digital safety trainers have an interest in encouraging society-wide safe practice.

- ***Recommendation*** (international organizations, news organizations, journalism schools, educational and training institutions): Provide an overarching framework explaining how networks and digital communications work and map how individual actions by digital producers of journalism might result in insecurity.
- ***Recommendation*** (news organizations): Provide digital security training to journalists, in order to mitigate the threat of phishing and other attacks.
- ***Recommendation*** (news organizations): Adopt a culture favorable to information security and encourage digital hygiene practices.
- ***Recommendation*** (news organizations and journalists): Increase information sharing of digital security risks and training among media collectives, news organizations, independent journalists and other online producers of journalism (e.g. offer links on website to resources such as CPJ, Rory Peck Trust, etc., to make those who do journalism aware of what digital security resources are relevant and available).
- ***Recommendation*** (news organizations): Encourage media actors to share peer-to-peer digital security recommendations.
- ***Recommendation*** (news organizations and journalists): Form networks or associations to present consolidated positions on policies and acts impacting digital safety and legislation that protects the safety of digital journalism and media actors, their sources and their work on all platforms.
- ***Recommendation*** (news organizations): Invest in online security resources, including hiring staff technologists who can help to detect and analyze malware and other digital security concerns.
- ***Recommendation*** (international organizations): Provide freelance reporters and other informal actors generating journalism with resources and knowledge necessary to report or file stories from locales that do not compromise their safety.
- ***Recommendation*** (news organizations): Train journalists on ways to safely and securely upload files from the field.

- ***Recommendation*** (news organizations and journalists): Maintain ownership over your domain name by locking the transfer of it and seek to choose a domain registry and registrar that is not vulnerable to interference.
- ***Recommendation*** (journalistic actors, news organizations): Provide specific feedback to technologists about digital security tools – what works, what is too complicated and why.
- ***Recommendation*** (journalistic actors): Make 'digital hygiene' a habit, and keep abreast of changing threats.
- ***Recommendation*** (journalistic actors): Raise awareness of information security best practices among colleagues and sources.

Challenge 3.3: Most journalist sources are not adept at using encryption or other forms of secure communications.

- ***Recommendation*** (news organizations and journalistic actors): Adopt secure technologies for information and file sharing, which allow for anonymous, encrypted communication from sources to media actor on a news organization's or individual blogger's website. Sources need to be educated about the risks of digital communication.

Challenge 3.4: Traumatic experiences may result in those doing journalism making bad decisions that lead to greater insecurity.

- ***Recommendation*** (international organizations, news organizations, journalism schools, educational and training institutions): Ensure that journalistic actors understand the link between digital and physical security, and encourage them to consistently implement good practices.

Guidelines for Media Actors Doing Journalism in a Digital Context

In general, all journalistic actors interfacing with digital technology should:

1. Develop a risk assessment plan or 'threat model' and develop a personal security plan with tools and techniques necessary to successfully implement it;
2. Acknowledge that security is always a trade-off of resources and prioritize security needs based on individualized risk assessment – avoid the extremes of paranoia on the one hand, and a sense of futility on the other;
3. Understand that digital and physical security are linked and take steps to improve both;
4. Treat digital hygiene as a habit and practice;
5. Understand that expensive is not always better. Journalists should consider implementing open source technologies and other simple tactics; and

6. Realize that digital security is constantly changing. There is a need to keep up to date and to understand the strengths and weaknesses of browsers, email-providers, social media, software and hardware.

4. Digital security training

Digital security trainers should consider approaching training holistically and include normative, psychosocial and physical training alongside digital training because all components are essential in order to encapsulate the many dimensions of security. It is also important to ensure that those who do journalism learn about norms of digital safety and free expression, besides for being able to ensure that their operational security or their psychosocial state does not compromise their digital security practice.

In addition, trainers should emphasize the importance of changing behaviors that put people and data at risk. Further, they should focus on contingency planning and security protocols. All this is in addition to specific tools that can keep journalistic work safe.[221]

Challenge 4.1: Digital security training is often taught ad-hoc, if at all, and needs to be more systematic and holistic to be effective for journalists.

- ***Recommendations*** (news organizations, international organizations, journalism institutions):
    - Teach digital security in a holistic fashion. For example, include physical and psychological safety considerations as digital security intersects with both.
    - Include an overview of the Internet and networks in digital security training courses in order to successfully set the context for digital security concerns.
    - Use a balanced and gentle approach to teaching. Avoid overly technical language, which may overwhelm the journalist and lead him or her to not implement digital tools and techniques.
    - Encourage research on digital security training courses best practices.

Challenge 4.2: Digital security guides duplicate, become outdated and are in limited languages.

- ***Recommendations*** (news organizations, international organizations, journalism institutions):
    - Instead of pushing resources into the creation of more training guides, organizations should consider investing resources to update existing guides, translate them into more languages, and raise awareness of them. This may lead to less confusion among journalists and other actors doing journalism, and could also generate more current information, thereby lessening the chance that journalistic actors might operate with a false sense of security.

Ideally, digital security trainers need to be equal parts:

- cheerleader, ensuring that individuals are reinforced in the norms of free and safe expression
- doctor, diagnosing a person's digital vulnerabilities and symptoms,
- translator, turning technological knowledge into user-friendly language that connects with their audiences.

This mix of roles can help ensure that participants can leave training courses capable of implementing security protocols for their context-specific situation.

Because digital security for journalism is not an exclusively technical question, digital security training courses can profitably include Media and Information Literacy (MIL) dimensions in their programs. Many journalists lack basic awareness of appropriate digital behavior – for example, making themselves vulnerable by their social media posts. They thus make simple errors that might result in costly consequences. MIL seeks to change this by providing basic awareness on how to act online and educating users on dangers that can be easily avoided.

A variety of organizations have written extensively about tools and tactics that journalists should use for digital security. However, over-arching guidelines that those doing journalism should consider implementing are less evident. Here are some suggestions:

Guidelines for improved digital security training courses

When conducting digital security training courses, trainers should include:

1. An introduction to international normative standards. As outlined earlier in this publication, there are many UN – as well as regional – declarations that are directly relevant to freedom of expression, press freedom and the safety of journalists, and which should apply to journalism across all technologies. For example, one that is particularly relevant is the already cited reference within a UNESCO resolution on Internet issues in November 2013: 'Privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law.'[222] Also particularly relevant to digital safety is the UN Human Rights Council in September 2014 which acknowledged 'the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or interception of communications in violation of their rights to privacy and to freedom of expression'.[223] Training should ensure that journalists are empowered to know and use these statements, and those cited earlier, in their monitoring, reporting and advocacy activities.

2. A comprehensive approach to digital security, including the legal landscape and a thorough grounding of how networks work and of the structure of the Internet. Legal protections for journalists have not kept up with technological change and journalists are often unaware of how networks interface with one another or the infrastructure

of the Internet – both are needed to ensure the right digital security tools are used to protect information.

3. A risk assessment or threat model exercise. Journalists need to develop a personalized risk assessment to ensure the digital security tools and practices they use are effective to their particular situation. Trainers can empower journalists to adapt to new security environments by teaching journalists how to conduct a risk assessment and develop responses for their particular situation.

4. Adding threat modeling or risk assessment questions to training courses means that journalists can take away a set of adaptable skills that can be adjusted to meet their specific security situation.

5. A gender-sensitive approach. Threats facing women who do journalism may sometimes differ from the threats facing men who do journalism, so it is important that trainers adjust their instruction and ensure they teach with a gender-sensitive approach. This should also be applied to the logistical arrangements of training courses as accessibility may vary for men and women depending on where the training is organized, how it is conducted and in some cases whether or not trainers of the same sex are available.

6. Updated material that reflects a changing reality. Technology changes quickly, as do the tactics of digital attackers. Digital security trainers and journalists must adapt if they do not want their skills and tools to be irrelevant. Therefore, it is important that trainers keep their materials up-to-date to adapt to the changing security landscape.

7. Include mitigation strategies as part of the training. Once a person becomes aware that digital security or technological integrity is compromised, he or she should know what measures to take and what alternative options are available.

4. SELECTED ORGANISATIONS

Below are descriptions of some of the organizations and initiatives referenced in this report. The list does not claim to be comprehensive, but is aimed to serve as a basic resource as well as a stimulus for further research and listing of additional actors.

Access. An international NGO that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, Access fights for open and secure communications for all.

Article 19. Established in 1987, Article19 is an international NGO focused on protecting freedom of expression and opinion.

Association for Progressive Communications. An international association and a network working to empower and support organizations, social movements and individuals in and through the use of information and communication technologies (ICTs).

BoloBhi. A Pakistani-based not-for-profit organization geared towards advocacy, policy and research in the areas of gender rights, government transparency, Internet access, digital security and privacy.

Bytes for All Pakistan. A Pakistani-based organization focused on Information and Communications Technologies (ICT) for development, democracy and social justice.

Centro de Formación en Periodismo Digital (CFPD). The Digital Journalism Training Centre at the University of Guadalajara supports journalists in learning to work with new media and promotes the training of citizen journalists. It offers courses and workshops as well as classroom instruction and online resources.

Center for Democracy and Technology (CDT). A US-based organization dedicated to driving policy outcomes that keep the Internet open, innovative and free. CDT works inclusively across sectors and the political spectrum to find tangible solutions to today's most pressing Internet policy challenges.

Citizen Lab. An interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, in Canada focusing on advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security.

Committee to Protect Journalists (CPJ). A New York-based, nonprofit organization founded in 1981 that promotes press freedom worldwide by defending the rights of journalists to report the news without fear of reprisal.

CommunityRED. An organization that works to improve the security of journalists, activists and citizen reporters in conflict zones, and promote information sharing where it's needed most without endangering lives or livelihoods.

Dart Center for Journalism & Trauma. A global network of journalists, journalism educators and health professionals dedicated to improving media coverage of trauma, conflict and tragedy.

Deutsche Welle Akademie. Germany's leading organization for international media development. DWA trainers and consultants have been promoting free and independent media since 1965.

Digital Rights Foundation. A Pakistani research-based advocacy not-for-profit organization focusing on Information and Communication Technologies (ICTs) to support human rights, democratic processes and digital governance.

Electronic Frontier Foundation. A US-based NGO that fights to protect civil liberties in the digital age. Blending the expertise of lawyers, policy analysts, activists, and technologists, it fights for freedom primarily in the courts, bringing and defending lawsuits against government agencies and corporations.

eQualit.ie. Founded in 2006, eQualit.ie provides digital security and information management expertise to front line civil society and independent media organizations with limited resources, working in acutely hostile Internet environments. EQualit.ie's program, Deflect, provides free help against DDoS attacks.

Foundation for a Free Press (FLIP). A Bogotá-based organisation that monitors press freedom and journalist safety in Colombia through its alert and protection network. FLIP also provides free counseling to journalists who have been the victims of attack or assault or who are suffering from stress.

Freedom House. An independent watchdog organization dedicated to the expansion of freedom around the world.

Freedom of the Press Foundation. A US-based NGO dedicated to helping support and defend public-interest journalism focused on exposing mismanagement, corruption, and law-breaking in government.

Free Press. An organization that is building a powerful nationwide movement to change media and technology policies, promote the public interest and strengthen democracy. Free Press advocates for universal and affordable Internet access, diverse media ownership, vibrant public media and quality journalism.

Free Press Unlimited. Established in the Netherlands in 2011 as a merger of three Dutch nonprofit groups, Free Press Unlimited is a non-profit organization that supports local media professionals and journalists and aims to help people gain and keep access to the information they require to survive and develop. Recently, it developed the Internet Protection Lab, which offers concrete and targeted support to journalists, bloggers and activists who are threatened around the world.

Front Line Defenders. Founded in Dublin in 2001, Front Line Defenders works to provide fast and effective action to help protect human rights defenders at risk so they can continue their work as key agents of social change.

Frontline Freelance Register (FFR). Established in 2013, the FFR is a representative body for freelancers, created and run by freelancers to support the physical and mental well-being of freelance journalists.

Global Journalist Security. A for-profit organization that draws from cutting edge civilian, law enforcement and military practices to provide safety training for journalists, citizen journalists, human rights activists and NGO workers.

Global Voices. A virtual community of more than 500 bloggers and translators around the world who work together to disseminate reports from around the world, with an emphasis on voices not ordinarily heard in international media.

Humanist Institute for Development Cooperation (Hivos). A Netherlands-based organisation guided by humanist values that works with local civil society organisations in developing countries to contribute to a free, fair and sustainable world.

Index on Censorship. A London-based organisation that promotes and defends the right to freedom of expression.

Institute of War and Peace Reporting (IWPR). A London-based organization that forges the skills and capacity of local journalism, strengthens local media institutions and engages with civil society and governments to ensure that information achieves impact.

International Federation of Journalists (IFJ). An organization that promotes international action to defend press freedom and social justice through strong, free and independent trade unions of journalists.

International Freedom of eXchange (IFEX). A Toronto-based non-profit network of some 95 independent organizations that works to rapidly expose free expression violations around the world.

International Media Support (IMS). A non-profit organization working to support local media in countries affected by armed conflict, human insecurity and political transition.

International News Safety Institute (INSI). A coalition of news organizations, journalist support groups and individuals exclusively dedicated to the safety of news media staff working in dangerous environments

International Press Institute (IPI). A Vienna-based global network of editors, media executives and leading journalists. Founded at Columbia University in New York in 1950, IPI is dedicated to the furtherance and safeguarding of press freedom, free expression and the improvement of the practices of journalism.

International Women's Media Foundation (IWMF). A global network dedicated to strengthening the role of women in the news media worldwide as a means to further freedom of the press.

Internews. An international non-profit organization whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect and the means to make their voices heard.

International Research & Exchanges Board (IREX). An international non-profit organization founded in Washington in 1968 that provides thought leadership and innovative programs to promote positive lasting change globally.

Iraqi Journalists Rights Defense Association (IJRDA). An Iraq-based organization focused on the safety of journalists.

Journaliste en Danger. An independent organization created in Kinshasa by a group of Congolese journalists dedicated to the defence and the promotion of the press freedom.

M-Lab. A Google research initiative that provides the largest collection of open Internet performance data on the planet. As a consortium of research, industry, and public interest partners, M-Lab is dedicated to providing an ecosystem for the open, verifiable measurement of global network performance.

National Press Foundation. A Washington DC-based foundation that increases journalists' knowledge of complex issues in order to improve public understanding. The foundation recognizes and encourages excellence in journalism through its awards and programs.

Open Society Foundations. A group of private, grant giving foundations, the first of which was established by the philanthropist George Soros in 1984. Open Society Foundations Journalism Program assists in the development and establishment of media systems marked by freedom, pluralism, and the inclusion of minority voices and opinions, as it promotes independent and viable media and professional, quality journalism in countries undergoing a process of democratization and building functioning media markets.

Open Net Initiative. A collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa), with the aim to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion.

PEN International. An international literacy and human rights organization that works to promote freedom of expression and resist censorship worldwide.

Privacy International. A London-based organization that defends the right to privacy across the world and fights surveillance and other intrusions into private life by governments and corporations.

Reporters Without Borders. A international non-profit organization that fights for press freedom.

RiseUp. An organization that provides online communication tools for people and groups working on liberatory social change.

SKeyes Center for Media and Cultural Freedom. A Lebanon-based organization that monitors violations of freedom of the press and culture and defends the rights and freedom of expression of journalists and intellectuals.

Small World News. A US-based organized created in 2005 that supports, equips and trains underserved populations to become journalists, storytellers and documentarians.

Tactical Technology Collective (Tactical Tech). An organisation dedicated to the use of information in activism. Tactical Tech focuses on the use of data, design and technology in campaigning and helps activists understand and manage their digital security and privacy risks.

The Guardian Project. An organization that creates easy-to-use open source apps, mobile OS security enhancements, and customized mobile devices for people around the world to help them communicate more freely, and protect themselves from intrusion and monitoring.

The Open Internet Tools Project (OpenITP). An organization that supports the software creators and communities behind open source anti-surveillance and anti-censorship tools that enable citizens to communicate directly and freely with each other, on their own terms.

The Rory Peck Trust. A London-based organization that gives direct practical support to freelancers and their families in need.

The Tor Project. An organization and web service that helps whistleblowers and dissidents communicate more safely.

Tow Center for Digital Journalism at Columbia Journalism School. The Tow Center explores how the development of technology is changing journalism, its practice and its consumption — particularly as consumers of news seek ways to judge the reliability, standards and credibility of information.

Witness. An international nonprofit organization that has been using the power of video and storytelling for 20 years to open the eyes of the world to human rights abuses.

5. INTERVIEWS

Thank you to everyone who agreed to be interviewed for this report. Please note that even if specific quotes were not used from every interview, the interviews provided helpful background and contacts to the researchers.

Anonymous, Associate, Management and technology consulting firm

Anonymous, CEO, Management and technology consulting firm

Anonymous, Chief Cybersecurity Officer, Cybersecurity firm

Anonymous, Digital Security Trainer and Expert, International organization

Aaron Brauer Rieke, Director of Tech Policy Projects, Robinson + Yu

Andrew Ford Lyons, Digital Producer and Project Manager, Rory Peck Trust

Arzu Geybullayeva, Blogger and Regional Analyst, Azerbaijan

Ayman Mhanna, Executive Director, SKeyes Center for Media and Cultural Foundation

Carole Kimutai, Editor, Management Magazine, Kenya

Christopher E. Pogue, Director, SpiderLabs US West, Trustwave

Chris Riley, Senior Policy Engineer, Mozilla Corporation

Dalia Haj Omar, Sudanese Human Rights Activist

Dan Meredith, Director, Radio Free Asia's Open Technology Fund

Daniel Ó Clunaigh, Programme Coordinator, Tactical Technology Collective

Danilo Bakovic, Director, Internet Freedom, Freedom House

Danny O'Brien, International Director, Electronic Frontier Foundation

Deji Olukotun, Freedom to Write Fellow, PEN American Center

Diana del Olmo Campos, Communications Manager, The Guardian Project

Dmitry Vitaliev, Executive Director, eQualit.ie

Dr. Doug Belshaw, Web Literacy Lead, Mozilla Foundation

Elisa Muñoz, Executive Director, International Women's Media Foundation

Ellery Roberts Biddle, Editor, Global Voices Advocacy

Ernest Sagaga, Head of Human Rights and Safety, International Federation of Journalists

Eva Galperin, Global Policy Analyst, Electronic Frontier Foundation

Faisal Kapadia, Blogger, Global Voices

Frank Smyth, Director, Global Journalist Security

Gayathry Venkiteswaran, Executive Director, Southeast Asian Press Alliance

Gerard Harris, Communications and Outreach, eQualit.ie

Gigi Alford, Senior Program Officer, Internet Freedom, Freedom House

Gus Andrews, Senior Program Associate, Open Internet Tools Project

Gustaf Björksten, Technology Director, Access

Hannah Storm, Director, International News Safety Institute

Hauke Gierow, Head, Internet Freedom Desk, Reporters Without Borders

Ibrahim Al-Sragey, Director, Iraqi Journalists Rights Defense Association

Jon Camfield, Senior Technologist, Internews

Jonathan Stray, Fellow, Tow Center for Digital Journalism

Josh Levy, Internet Campaign Director, Free Press[224]

Josh Stearns, Journalism and Public Media Campaign Director, Free Press[225]

Kirsty Hughes, Former Chief Executive, Index on Censorship

Lamiya Adilgizi, Journalist, *Today's Zaman* and writer at the *Turkish Review*

Lindsay Beck, Program Officer, ICT Programs, National Democratic Institute[226]

Melissa Chan, Journalist, Al Jazeera America

Michael Carbone, Manager of Tech Policy and Programs, Access

Mindy Ran, Co-Chair, Gender Council, International Federation of Journalists

Nicolas Rouger, Programme Officer, Sub-Saharan Africa, Rory Peck Trust

Nighat Dad, Director, Digital Rights Foundation, Pakistan

Oktavia Jónsdóttir, Director, S.A.F.E., International Research and Exchanges Board

Paul Mooney, Freelance Journalist[227]

Paula Martins, Coordinator, Article 19 Brazil

Peter Nkanga, West Africa Consultant, Committee to Protect Journalists

Peter Noorlander, CEO, Media Legal Defence Initiative

Rebecca MacKinnon, Director, Ranking Digital Rights Project, New America Foundation

Robert Guerra, Senior Advisor, Citizen Lab

Roxana Geambasu, Assistant Professor of Computer Science, Columbia University

Sarah Giaziri, Programme Officer, Middle East and North Africa, Rory Peck Trust

Seamus Tuohy, Technical Program Associate, Open Technology Institute, The New America Foundation[228]

Shauna Dillavou, Executive Director, CommunityRED

Sheryl Mendez, Senior Program Officer, Global Human Rights Program, Freedom House

Shiva Gaunle, President, Federation of Nepali Journalists

Steve Kelley, Senior Vice President, Product and Corporate Marketing, Trustwave

Susan McGregor, Assistant Professor and Assistant Director, Tow Center for Digital Journalism

Tom Rhodes, East Africa Representative, Committee to Protect Journalists

Wafa Ben Hassine, Blogger, Tunisia

With correspondence from:

Twitter correspondence with the BBC Academy College, 20 March 2014

Email from Erin Murrock, 3 April 2014

Email from Henrik P. Berggreen, 27 February 2014

Email from Ismail Hakki Polat, 23 March 2014

Email from Jane E. Kirtley, 13 January 2014

Twitter correspondence with Jorge Luis Sierra, 19 March 2014

Email from Dr. Michel Cukier, 11 April 2014

Email from Privacy International, 15 January 2014

Email from Sandeep Junnarkar, 16 January 2014

Additional questionnaire responses from International Media Support, Committee to Protect Journalists, Reporters Without Borders, Bytes for All, Article 19 and the International Federation of Journalists.

APPENDIX 1: SURVEY METHODOLOGY

Objective

The objective of this research study is to better understand the safety of media actors doing journalism with digital technology by examining the specific challenges and dangers they face in a complex technological and political climate. To fully address these concerns, and provide the information for the subsequent chapters, the researchers have:

1. Described some of the diverse stakeholders and initiatives that address online safety,
2. Mapped out some of the various journalism-training institutions that discuss online safety with their constituents,
3. Mapped some of the digital threats and challenges that journalists face,
4. Explored some of the best practices and guidelines that diverse stakeholders can use to address these challenges,
5. Offered recommendations to key stakeholders to help them meet these challenges.

The authors used qualitative and quantitative research methods in developing this report, including interviews and surveys. Between October 2013 and April 2014, the researchers interviewed more than 50 press freedom experts, technologists, academics, and journalists in person, electronically or by phone. The researchers also crafted two surveys for this research. The first and primary one was a 52-question, multilingual[229] electronic survey that was disseminated to a network of international organizations, news associations and relevant professional networks.[230] The survey was first fielded to a small pilot group in September 2013. Following feedback to the pilot study, the researchers updated the survey and introduced it into the field in November 2013. The survey link remained active until August 2014, although outreach for the survey stopped in March 2014.

Approximately 2,645 people viewed the study, 478 started it and 167 completed it.[231] The number of completes does not include pilot study respondents or individuals who self-reported that they did not engage in newsgathering (and therefore had their answers removed from the total number of respondents.) The survey took participants an average of 13 minutes to complete.

The second electronic survey was 10 questions and focused on digital security training among journalism institutions. The researchers sent it to contacts at Radio Television Digital News Association, Association for Education in Journalism and Mass Communication,

Broadcast Education Association, International Center for Journalists, College Media Advisors, and the International Journalists' Network, although the researchers did not receive responses from all organizations. Respondents to the survey included individuals from Pakistan, France, Nigeria, Mongolia, Colombia and the United States. A total of 356 individuals viewed the report, 46 started it and 14 completed it. The survey was actively fielded from January 14, 2014 – February 4, 2014, although the link was available until August 2014.

Survey limitations

The survey on the safety of online media actors doing journalism was disseminated via NGOs, news associations, and the researchers' professional network via the Internet and it does not represent a random sample of the population. The response rate may have been influenced by the following:

- **Length and complexity of the survey**. The survey contained 52 questions, many of which involved written responses. This request for in-depth participation may have contributed to the number of drop-outs (293) from the survey.
- **Digital Security Complexity**. On the survey's introduction page, the researchers advised respondents who felt at risk to download an anonymizing proxy service such as Tor before responding to the survey. The researchers also proffered the option of a secure interview in lieu of the survey via an encrypted communication channel, should they be worried about their safety.

  While these warnings were intended to create a safer digital environment for participants as well as engender trust and participation, the researchers believe the specific digital security terminology may have resulted in less participation. Some participants may not have considered themselves at risk until the researcher's warning, while other participants may have been intimidated by the extra steps the researchers suggested they take. Following these internally made conclusions, the researchers shortened the introduction page and removed some of the technological language in order to engender more responses. Additionally, the researchers worked in partnership with the survey-host company, QuestionPro, to send the survey to journalists who lived and worked in countries in the Middle East, Asia and Latin America, as the researchers had difficulty gaining responses via their networks for participants in those countries.
- **Request for biographical data**. To prevent data duplications, the researchers originally required respondents to answer questions asking them for biographical information, including first name, last name, email address, etc. After one organization expressed reservations about sharing the survey with its network because of the mandatory biographical questions, the researchers made the biographical questions voluntary. To prevent potential data duplication, the researchers evaluated each response individually based on responses to questions more generally.

- **Limitations of outreach**. At least one organization chose not to disseminate the survey online, despite open support of the researchers' project and intentions, because the organization works with at-risk journalists in highly volatile situations and worried about the vulnerabilities of this population should they fill it out online, despite the survey company's strict data removal policy and assurance of anonymity.

Notwithstanding these qualifications, the research findings have been valuable in providing case material, and for extrapolating the kinds of threats and responses entailed. The result is an enhanced understanding of how digital issues impact on the safety and security of journalism.

APPENDIX 2:
SURVEY QUESTIONNAIRE

Below is the survey questionnaire the researchers disseminated to participants. Please note the introduction language changed following feedback from participants and others. Participants first received two screener questions before they could continue to the survey.

Hello: You are invited to participate in a UNESCO-sponsored global survey on the safety of online media actors engaged in journalism. Your participation in this study is completely voluntary and your survey responses will be confidential. Data from this research will be reported primarily in the aggregate. If we decide to use any quotations from the research, we will cite an anonymous source, or contact you first for your approval. If, at any point, you feel uncomfortable answering one or more questions, you can withdraw from the survey, or you may contact Individual Specialist for UNESCO, Jennifer Henrichsen, at JournalistSafety@gmail.com (GPG Key: 0xD4D03F57) to set up a confidential interview. As a thank you for your participation in filling out the survey, you will have the opportunity to win a pre-paid, anonymous subscription to Silent Circles Global Mobile Encryption Service. We will randomly select a winner in February 2014. (Please note, Silent Circle is not involved in this survey or research in any way).Thank you for taking the time to share your insights and experiences on this important topic. Please start the survey by clicking Continue below.

1. What is your first name? (Optional)

2. What is your last name? (Optional)

3. At what email address may we contact you at should we need to clarify something or seek further elaboration? (Optional)

4. At what phone number may we reach you at should we need to clarify something or seek further elaboration? (Optional)

5. What is your gender?

- Male
- Female
- Transgender

6. What is your nationality?

7. What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65-74
- 75 or older
- If Other, please specify:

8. In what country do you currently live?

9. In which area of media do you work? (Select all that apply)

- TV
- Radio
- Newspaper
- Magazine
- Internet
- If Other, please specify:

10. How are you employed? (Select all that apply.)

- Freelancer
- Staff Journalist
- Professional Blogger
- Citizen Journalist/Blogger (Voluntary/Not paid)
- If Other, please specify:

11. What is the name of the publication, blog or news outlet, you do reporting for?

12. How much of your income is derived from your journalism activities? (Please estimate.)

- 0-25%
- 26-45%
- 46-65%
- 66-85%
- More than 85%

13. During the last 12 months, how much of your time has been spent on newsgathering activities? (Please estimate.)

    - o 0-25%
    - o 26-45%
    - o 46-65%
    - o 66-85%
    - o More than 85%

14. Please describe the type of stories you primarily cover:

    - o Politics and Governance
    - o War and/or Security
    - o Crime
    - o Accidents and Disasters
    - o Human Rights (including women, children, minority, and LGBT rights)
    - o Health
    - o Education
    - o Business
    - o Arts and Entertainment
    - o Technology and Innovation
    - o Religion and Culture
    - o Sports
    - o If Other, please specify:

15. Which technologies and tools do you use when researching, distributing, or writing a story? (Select all that apply.)

- ○ Desktop computer
- ○ Laptops/Tablets
- ○ Mobile Phones
- ○ Email
- ○ Collaborative tools (e.g. Google Docs)
- ○ Cloud storage (e.g. Dropbox)
- ○ USB devices
- ○ General websites, including search engines
- ○ Networking websites (e.g. Facebook, LinkedIn, Weibo, Twitter, etc.)
- ○ GPS
- ○ Video/Audio recording devices
- ○ If Other, please specify:

16. How often do you use email when you are:

	Never	Rarely	Sometimes	Often	Almost always
Researching a story					
Organizing Interviews					
Interviewing subjects					
Liaising with a media outlet (If not applicable, leave slider to the far left)					
Discussing the story with colleagues					
Distributing the story (If not applicable, leave slider to the far left)					

17. Which email service(s) do you use for your work-related interactions? (Select all that apply)

    - o Gmail
    - o Hotmail
    - o Yahoo
    - o An email account through your media organization
    - o If Other, please specify:

18. Are you aware of email services that offer encrypted communications?

    - o Yes
    - o No

19. If yes, which one(s)?

20. Do you use social networking platforms such as Facebook, Twitter, LinkedIn, etc. when researching a story?

	Never	Rarely	Sometimes	Often	Almost always
Facebook					
YouTube					
Twitter					
LinkedIn					
Google+					
Flickr					
Orkut					
Weibo					
Other					

21. If you chose Other in response to the previous question, please specify the platform(s).

22. Do you use social networking platforms such as Facebook, Twitter, LinkedIn, etc. when distributing a story? (If not applicable, please leave blank.)

	Never	Rarely	Sometimes	Often	Almost always
Facebook					
YouTube					
Twitter					
LinkedIn					
Google+					
Flickr					
Orkut					
Weibo					
Other					

23. If you chose Other in response to the previous question, please specify the platform(s).

24. Does your journalism/blogging include meeting sensitive contacts/sources?

- ○ Yes
- ○ No
- ○ Don't know

25. If yes, do you modify how you engage with your sensitive contacts/source(s)? If so, please explain how. (e.g. Only use encrypted email, meet only in person, etc.)

26. As a journalist, what types of issues are of concern to you? (Select all that apply.)

- o Personal safety
- o Safety of information
- o Safety of people I work with
- o Safety of sources
- o Safety of family
- o Don't know
- o If Other, please specify:

27. What are the top three threats you might face in your capacity as a journalist?

- o Illegal arrest
- o Threats in person
- o Threats by email
- o Threats by SMS/Voicemail
- o Physical attack
- o Surveillance of your online activities
- o Threats to friends and/or family
- o Virus in computer that harms data
- o Exposed identity (against your wishes)
- o Personal website/blog or news organizations website/blog hacked/attacked
- o Intercepted emails
- o Stolen data, including data stored in the cloud
- o Tapped phone or recorded calls
- o Impersonation online
- o Online disinformation campaign
- o Don't know
- o If Other, please specify:

28. What do you think motivates actors to carry out these threats?

29. Who do you think might be behind these types of attacks? Why?

30. In the past 18 months, have you experienced any negative consequences because of your journalism and/or blogging activities?

    - Yes
    - No
    - Don't Know

31. If yes, what did you experience? (Please select all that apply.)

    - I was illegally arrested
    - I was threatened in person
    - I was threatened by email
    - I was threatened by SMS/Voicemail
    - I was physically attacked
    - My online activities were surveilled
    - My friends or family were threatened
    - My computer got a virus and my data was harmed
    - My identity was exposed against my wishes
    - My publication, website or blog was attacked or hacked (e.g. DDOS, phishing/spear phishing attacks)
    - I had my emails intercepted
    - My data was stolen
    - My phone was tapped and/or my calls were recorded
    - Someone impersonated me online
    - Someone conducted an online disinformation campaign against me
    - If Other, please specify:

32. Please provide a brief description of what you experienced. If you prefer to discuss your experience(s) directly with UNESCO Individual Specialist, Jennifer Henrichsen, please indicate that here or email her (JournalistSafety@gmail.com, GPG Key: 0xD4D03F57) to set up a secure interview.

33. Do you click on any web links contained in an email message, if the sender is unknown?

- o No
- o Rarely
- o Sometimes
- o Often
- o Almost Always
- o Yes, but only after checking the link location
- o Don't know
- o If Other, please specify:

34. Do you click on any web links contained in an email message, if the sender is known?

- o No
- o Rarely
- o Sometimes
- o Often
- o Almost Always
- o Yes, but only after checking the link location
- o If Other, please specify:

35. How often do you click on email attachments if you know the sender?

- Never
- Rarely
- Sometimes
- Often
- Almost Always
- If Other, please specify:

36. How often do you click on email attachments if you Don't know the sender?

- Never
- Rarely
- Sometimes
- Often
- Almost Always
- If Other, please specify:

37. There are a range of ways to increase the security of information and individuals using online platforms and tools. Do you know of any such methods?

- Yes
- No
- Don't know

38. If yes, which of the following do you use to protect your data and/or your sources?

- o Using strong passwords for your email and other Internet accounts
- o Encrypting data, including emails
- o Using open-source anti-virus software
- o Keeping your operating system updated with the latest security patches and updates
- o Using IP disguisers/blockers
- o Using anti-censorship software (A software application that allows a user to bypass network filters and access Internet resources that would normally be banned by their Internet Service Provider.)
- o Using a VPN (Virtual Private Network—a virtual version of a secure, physical network. Essentially, it's a web of computers linked together to share files and other resources.)
- o If Other, please specify:

39. What is the most important feature you look for when personally selecting or receiving an email service from your media organization?

- o Security
- o Storage space
- o Ease of use
- o Not applicable
- o If Other, please specify:

40. What is the most important feature you look for when selecting or receiving a blogging or micro-blogging service from your media organization?

    - Popularity
    - Design/Appearance
    - Ability to customize
    - Costs
    - Security/Privacy
    - Ease of use
    - Not Applicable
    - If Other, please specify:

41. Have you heard about the concept of Anonymous Blogging?

    - Yes, I use it
    - Yes, but I've never used it
    - No

42. Have you heard of the concept of threat modeling as it relates to protecting yourself online?

    - Yes
    - Yes, but I don't remember what it means
    - No
    - Don't Know
    - If Other, please specify:

43. How do you prevent unauthorized manipulation of your content?

- o Using strong passwords for your email or other Internet accounts
- o Using two-factor authentication for your email and other Internet accounts
- o Encrypting data
- o Using open-source anti-virus software
- o Keeping your operating system updated with the latest security patches and updates
- o Using IP disguisers/blockers
- o Using anti-censorship software (A software application that allows a user to bypass network filters and access Internet resources that would normally be banned by their Internet Service Provider.)
- o Using a VPN (Virtual Private Network—a virtual version of a secure, physical network. Essentially, it's a web of computers linked together to share files and other resources.)
- o Firewall protection
- o Safe deletion of data
- o Secure backups to prevent any information loss
- o If Other, please specify:

44. Please indicate the level of digital security you believe is offered by each of the following strategies. (1=Don't know, 2=Not secure, 3=Somewhat insecure, 4=Somewhat secure, 5=Totally secure.)

	1	2	3	4	5
Using strong passwords for your email and other Internet accounts					
Using two-factor authentication for your email and other Internet accounts					
Encrypting data					
Using open-source anti-virus software					
Keeping your operating system updated with the latest security patches and updates					
Using IP disguisers/blockers					
Using anti-censorship software					
Using a VPN					

45. What security tools do you use to secure the data on your computer? (Select all that apply.)

    - Password protection
    - Safe deletion of data
    - Securing the data in external drives
    - Encryption
    - Open-source anti-virus software
    - If Other, please specify:

46. What security measures, if any, do you employ to secure the data on your mobile phone? (Select all that apply.)

    - Password protection
    - Safe deletion of data
    - Encryption
    - Open-source anti-virus software
    - If Other, please specify:

47. Have you participated in any digital security training courses which taught you how to use the Internet securely and how to protect your data?

    - Yes – in the last 12 months
    - Yes – but it was over 12 months ago
    - No

48. If yes, what type of training or guidance did you receive? (Select all that apply.)

- o Peer recommendations
- o In class course(s) by a reputable organization
- o Online course(s) by a reputable organization
- o Employer recommendations
- o Self-taught
- o If Other, please specify:

49. If you took a course, what was the name of the organization that sponsored it?

50. How satisfied were you with the courses teaching of the following?

	Very unsatisfied	Unsatisfied	Don't know	Satisfied	Very satisfied	Not applicable
Password security						
Encrypting data						
Using anti-virus software						
Keeping your operating system updated with the latest security patches						
Using IP disguisers/ blockers						
Using anti-censorship software						
Using a VPN						

51. On a scale of 1 to 5, how would you rate your overall knowledge of secure digital practices? (1 = Poor, 5=Excellent)

	Poor	Fair	Good	Above average	Excellent

52. What support could employers or policymakers give to journalists to help them be safer as they practice their profession online?

Endnotes

1. Samantha Barry's title has changed since her involvement with this project and in 2014 she was Head of Social News and Senior Director of Strategy for News and Social Media at CNN.
2. UNESCO. (2014.) 'World Trends in Freedom of Expression and Media Development.' UNESCO. http://unesdoc.unesco.org/images/0022/002270/227025e.pdf (Accessed 12 August 2014.)
3. Kovach, B. and Rosensteil, R., *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect*, 2nd ed. (New York: Three Rivers, 2007.) p. 5-6
4. Norris, P. 2006. The role of the free press in promoting democratization, good governance, and human development. Paper presented at the Midwest Political Science Association Annual Meeting, 20-22nd April, 2006, Chicago, Palmer House
5. World Bank. 2002. The right to tell. the role of mass media in economic development. http://elibrary.worldbank.org/doi/pdf/10.1596/0-8213-5203-2
6. UNESCO: The International Programme for the Development of Communication. (15 March 2014.) 'Why free, independent and pluralistic media deserve to be at the heart of a post-2015 development agenda.' http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/free_media_post_2015.pdf (Accessed 12 August 2014.)
7. *Journalism Ethics: A Philosophical Approach*, edited by Christopher Meyers. Oxford University Press. New York: New York, 2010. p. 78
8. International Telecommunications Union. (2013.) 'The World in 2013: ICT Facts and Figures.' http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf (Accessed 13 December 2013.)
9. *Journalism Ethics: A Philosophical Approach*, edited by Christopher Meyers. Oxford University Press. New York: New York, 2010. p. 111.
10. Tehranian, M. 'Peace Journalism: Negotiating Global Media Ethics,' *Harvard International Journal of Press/Politics* 7, no. 2 (2002): 58-83.
11. Interview with Oktavía Jónsdóttir, 18 November 2013.
12. La Rue, F. (4 June 2012.) Report of the Special Rapporteur on the promoton and protection of the right to freedom of opinion and expression, A/HRC/20/17 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-17_en.pdf (Accessed 19 March 2014.)
13. UNESCO. (12 April 2012.) 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity.' http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/UN_plan_on_Safety_Journalists_EN.pdf (Accessed 15 March 2014.)
14. UNESCO. (4 November 2013.) 'Journalists' Safety Indicators: National Level.' http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Final_Journalists_Safety_Indicators_National_Level.pdf (Accessed 14 March 2014.)
15. Office of the High Commissioner for Human Rights. (1 July 2013.) 'The Safety of Journalists: Report of the Office of the United Nations High Commissioner for Human Rights.' http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/24/23 (Accessed 24 July 2014.)
16. Interview with Tom Rhodes, 2 January 2014.
17. UNESCO. (12 April 2012.) UN Plan of Action on the Safety of Journalists and the Issue of Impunity. http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/safety-of-journalists/un-plan-of-action/ (Accessed 15 March 2014.)
18. United Nations. (12 April 2012.) UN Plan of Action on the Safety of Journalists and the Issue of Impunity: Implementation Strategy 2013-2014. http://en.rsf.org/IMG/pdf/implementation_strategy_2013-2014-2.pdf (Accessed 8 March 2014.)
19. McGregor, S. and Ag., M. (17 March 2014.) 'TA3M on JournoSec with Susan McGregor of Columbia and Magnus Ag of Committee to Protect Journalists.' https://www.youtube.com/watch?v=tu0_ySgLgys&feature=youtu.be (Accessed 20 March 2014.)
20. Beiser, E. (18 December 2013.) Second worst year on record for jailed journalists. *Committee to Protect Journalists*. http://cpj.org/reports/2013/12/second-worst-year-on-record-for-jailed-journalists.php (Accessed 18 March 2014.)
21. Interview with Gustaf Björksten, 20 December 2013.
22. Internews. (7 August 2012.) Digital Security and Journalists: A Snapshot of Awareness and Practice in Pakistan. Internews. http://innovation.internews.org/research/digital-security-and-journalists-snapshot-awareness-and-practice-pakistan (Accessed 2 January 2014.)
23. These organizations requested that they not be identified for this report.

24. Symantec Corporation. (April 2013.) 'Internet Security Threat Report 2013.' Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (Accessed 2 March 2014.)
25. Marquis-Boire, M. (10 October 2012.) 'Backdoors are Forever: Hacking Team and the Targeting of Dissent?' The Citizen Lab. https://citizenlab.org/wp-content/uploads/2012/10/12-2012-backdoorsareforever.pdf (Accessed 2 January 2014.)
26. Deibert, R. (2013.) Black Code: Surveillance, Privacy, and the Dark Side of the Internet. McClelland & Stewart. Toronto: Ontario. P. 165.
27. Ibid.
28. Björksten, G. (27 March 2014.) 'Innovating our future: Gustaf Björksten.' Innovating Our Future. https://www.youtube.com/watch?v=pMae8pZC4DE (Accessed 31 March 2014.)
29. Wagstaff, J. (28 March 2014.) Journalists, media under attack from attackers: Google researchers. http://www.reuters.com/article/2014/03/28/us-media-cybercrime-idUSBREA2R0EU20140328?irpc=932 (Accessed 2 April 2014.)
30. Wagstaff, J. (28 March 2014.) Journalists, media under attack from attackers: Google researchers. http://www.reuters.com/article/2014/03/28/us-media-cybercrime-idUSBREA2R0EU20140328?irpc=932 (Accessed 2 April 2014.)
31. Ibid.
32. Access. (January 2012) Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society. https://s3.amazonaws.com/access.3cdn.net/49632318adb472e369_yhm6ibn8c.pdf (Accessed 2 April 2014.)
33. Citizen Lab. (21 October 2013.) 'Monitoring Information Controls During the Bali IGF.' https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (Accessed 21 July 2014.)
34. Citizen Lab. (21 October 2013.) 'Monitoring Information Controls During the Bali IGF.' https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (Accessed 21 July 2014.)
35. La Rue, F. (17 April 2013.) A/HRC/23/40. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. http://en.rsf.org/IMG/pdf/surveillance_report_-_a.hrc.23.40_en.pdf (Accessed 1 April 2014.); Citizen Lab. (21 October 2013.) 'Monitoring Information Controls During the Bali IGF.' https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (Accessed 21 July 2014.)
36. Privacy International. Big Brother Inc. https://www.privacyinternational.org/projects/big-brother-inc?page=7 (Accessed 1 April 2014.)
37. Wikileaks. Spy Files 3. http://wikileaks.org/spyfiles3p.html (Accessed 1 April 2014.)
38. Human Rights Council, twenty-fifth session, A/HRC/25/L.12
39. A /HRC/27/37
40. Bell, E., Coronel, S., Stray, J., Schudson, M., and Zuckerman, E. (4 October 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (Accessed 3 April 2014.)
41. Bell, E., Coronel, S., Stray, J., Schudson, M., and Zuckerman, E. (4 October 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (Accessed 3 April 2014.) ; Downie Jr., L. (10 October 2013.) The Obama Administration and the Press: Leak investigations and surveillance in post 9/11 America. https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php (Accessed 3 March 2014.)
42. Pen American Center. (12 November 2013.) 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor.' http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (Accessed 4 April 2014.)
43. Bell, E., Coronel, S., Stray, J., Schudson, M., and Zuckerman, E. (4 October 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (Accessed 3 April 2014.)
44. Privacy International, in conjunction with Access, the Electronic Frontier Foundation, Article 19, the Association for Progressive Communications, Human Rights Watch and the World Wide Web Foundation; Privacy International. (2 April 2014.) UN must reject mass surveillance to protect global privacy rights. https://www.privacyinternational.org/blog/un-must-reject-mass-surveillance-to-protect-global-privacy-rights?utm_source=hootsuite&utm_campaign=hootsuite (Accessed 2 April 2014.)
45. Gallagher, R. and Greenwald, G. (12 March 2014.) 'How the NSA Plans to Infect 'Millions' of Computers with Malware.' The Intercept. https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ (Accessed 22 July 2014.)
46. Please note Seamus Tuohy's title and affiliation has changed since this interview occurred and in 2014 he was Technical Advisor at Internews.

47. Citizen Lab. (15 January 2013.) Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/ (Accessed 22 July 2014.); Citizen Lab. (25 October 2013.) 'IGF 2013: Exploring Communications Surveillance in Indonesia. (Part 3 of 4). https://citizenlab.org/2013/10/igf-2013-exploring-communications-surveillance-indonesia/ (Accessed 22 July 2014.); Silver, V. (25 July 2012.) 'Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma.' http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html (Accessed 1 April 2014.); Marquis-Boire, M. (25 July 2012.) 'From Bahrain With Love: FinFisher's Spy Kit Exposed?' Citizen Lab. https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (Accessed 2 April 2014.)
48. Marquis-Boire, M., Marczak, B., Guarnieri, C., and Scott-Railton, J. (30 April 2013.) 'For Their Eyes Only: The Commercialization of Digital Spying.' https://citizenlab.org/2013/04/for-their-eyes-only-2/ (Accessed 29 July 2014.)
49. Wikileaks. Spy Files 3. http://wikileaks.org/spyfiles3p.html (Accessed 1 April 2014.)
50. Electronic Frontier Foundation. (2014.) 'Pen Registers' and 'Trap and Trace Devices'. Electronic Frontier Foundation. https://ssd.eff.org/wire/govt/pen-registers (Accessed 5 February 2014.); Electronic Frontier Foundation. (2014.) Surveillance Self-Defense. Electronic Frontier Foundation. https://ssd.eff.org/wire/govt (Accessed 7 February 2014.)
51. Bu, Z. (24 April 2014.) Zero-Day Attacks are not the same as Zero-Day Vulnerabilities. http://www.fireeye.com/blog/corporate/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html (Accessed 30 July 2014.)
52. Interview with Oktavía Jónsdóttir, 18 November 2013.
53. de Montjoye, YA., Hidalgo, C., Verleysen, M. and Blondel, V. (25 March 2013.) 'Unique in the Crowd: The privacy bounds of human mobility.' *Nature*. http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html (Accessed 14 May 2014.)
54. Morisy, M. 3 July 2014. 'NSA's Xkeyscore program targeted visitors to MIT server, Tor project for enhanced security.' *BetaBoston*. http://betaboston.com/news/2014/07/03/nsas-xkeyscore-program-targeted-visitors-to-mit-server-tor-project-for-enhanced-scrutiny/ (Accessed 29 July 2014.)
55. Email from Eva Galperin, 21 April 2014.
56. Interview with Nighat Dad, 5 April 2014.
57. Galperin, E. and Marquis-Boire, M. (29 March 2012.) Syrian Activists Targeted with Facebook Phishing Attack. Electronic Frontier Foundation https://www.eff.org/deeplinks/2012/03/pro-syrian-government-attackers-target-syrian-activists-facebook-phishing-attack (Accessed 17 February 2014.)
58. Interview with Seamus Tuohy, Associate Technologist, Open Technology Institute, 16 April 2014.
59. Rights Con 2014. (4 March 2014.) Panel Session. 'Watching the Observers: The Impact of Surveillance on Human Rights.' https://www.youtube.com/watch?v=rbqHyNtj9XU&list=PLprTandRM9601CNiMd4VVTglZ1YSglKGx (Accessed 30 March 2014.)
60. Access. One of these things is not like the other: A report on fake domain attacks. *Access*. https://s3.amazonaws.com/access.3cdn.net/a80a7cabdf0ddadc85_vdm6brria.pdf p.8 (Accessed 30 March 2014.)
61. Ibid. p.10
62. Ibid. p.7
63. Björksten, G. (4 March 2014.) 'Reports from the Frontlines' Panel. RightsCon.
64. Access. 'Fake Domain Detective.' http://fakedomains.Access.org/ (Accessed 2 April 2014.)
65. Access. One of these things is not like the other: A report on fake domain attacks. Access. https://s3.amazonaws.com/access.3cdn.net/a80a7cabdf0ddadc85_vdm6brria.pdf (Accessed 30 March 2014.)
66. Fisher, D. (10 April 2013.) 'What is a Man-in-the-Middle Attack?' *Kaspersky Lab Daily*. http://blog.kaspersky.com/man-in-the-middle-attack/ (Accessed 3 April 2014.)
67. Ibid.
68. Access. (January 2012) Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society. https://s3.amazonaws.com/access.3cdn.net/49632318adb472e369_yhm6ibn8c.pdf (Accessed 2 April 2014.); Email from Eva Galperin, 21 April 2014.
69. McDowell, M. (6 February 2013.) Security Tip (ST04-015) Understanding Denial-of-Service Attacks. *United States Computer Emergency Readiness Team*. https://www.us-cert.gov/ncas/tips/ST04-015 (Accessed 29 March 2014.)
70. Martinez, J. (17 April 2014.) 'DDoS attacks increase 47% in Q1: Akamai.' *TechRadar Pro*. http://www.techradar.com/us/news/internet/ddos-attacks-increase-47-in-q1-akamai-1243471 (Accessed 14 May 2014.); Arbor Networks. (14 February 2014.) 'Worldwide Infrastructure Security Report.' http://www.arbornetworks.com/resources/infrastructure-security-report (Accessed 14 May 2014.)
71. Perlroth, N. and Wortham, J. (3 April 2014.) 'Tech Start-Ups Are Targets of Ransom Cyberattacks.' http://bits.blogs.nytimes.com/2014/04/03/tech-start-ups-are-targets-of-ransom-cyberattacks/?ref=technology (Accessed 4 April 2014.)

72. Security-FAQs. 'DoS vs DDoS – What is the difference?' http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html (Accessed 27 July 2014.)
73. Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. (September 2009.) Access Contested: Toward the Fourth Phase of Cyberspace Controls. Ch. 7, p. 139. http://citizenlab.org/wp-content/uploads/2011/09/Access-Contested-Part-1.pdf (Accessed 28 July 2014.)
74. Interview with a digital security trainer of an international organization, who wishes to remain anonymous, January 2014.
75. Björksten, G. (4 March 2014.) 'Reports from the Frontlines' Panel. RightsCon.
76. Whitcomb, D. (2 January 2014.) Syrian Electronic Army Says It Hacked Into Skype's Twitter. *Reuters*. http://www.huffingtonpost.com/2014/01/02/syrian-electronic-army-skype_n_4529292.html (Accessed 29 March 2014.)
77. Fisher, D. (10 April 2013.) 'What is a Man-in-the-Middle Attack?' *Kaspersky Lab Daily*. http://blog.kaspersky.com/man-in-the-middle-attack/ (Accessed 3 April 2014.)
78. Schneier, B. (22 September 2009) 'Hacking Two-Factor Authentication.' *Schneier on Security*. https://www.schneier.com/blog/archives/2009/09/hacking_two-fac.html (Accessed 3 April 2014.)
79. Ibid.
80. Honan, M. (3 August 2012.) 'Yes, I was hacked. Hard.' *Emptyage*. http://www.emptyage.com/post/28679875595/yes-i-was-hacked-hard (Accessed 31 March 2014.)
81. Popkin, H. (23 April 2013.) AP latest victim in string of Twitter break-ins by Syrian Electronic Army. NBCNews.com. http://news.ca.msn.com/top-stories/ap-latest-victim-in-string-of-twitter-break-ins-by-syrian-electronic-army (Accessed 2 February 2014.)
82. Interviews with Committee to Protect Journalists, Reporters Without Borders, International Federation of Journalists, International News Safety Institute, January 2014.
83. Committee to Protect Journalists. (2014.) 1046 Journalists Killed since 1992. Committee to Protect Journalists. https://www.cpj.org/killed/. (Accessed 19 February 2014.) According to CPJ's methodology, 'threatened journalists' includes 'all forms of threats at any time before a journalist was murdered.'
84. Kyiv Post. (4 September 2013.) 'Ukrainska Pravda demands investigation of clone site, paper.' http://www.kyivpost.com/content/ukraine/ukrainska-pravda-demands-investigation-of-clone-site-paper-329009.html (Accessed 7 January 2014.)
85. Aikins, M. (3 May 2012.) 'The spy who came in from the code.' *Columbia Journalism Review*. http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all (Accessed 22 February 2014.)
86. Search SQLServer. 'Data mining.' http://searchsqlserver.techtarget.com/definition/data-mining (Accessed 31 March 2014.)
87. Rights Con 2014. (4 March 2014.) Panel Session. 'Watching the Observers: The Impact of Surveillance on Human Rights.' https://www.youtube.com/watch?v=rbqHyNtj9XU&list=PLprTandRM9601CNiMd4VVTglZ1YSglKGx (Accessed 30 March 2014.)
88. Czuchnowski, W. (8 October 2010.) Dziennikarze na celowniku służb specjalnych [Journalists Targeted by Special Forces]. *Gazeta Wyborcza*. http://wyborcza.pl/Polityka/1,103835,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html (Accessed 27 July 2014.); Helsinki Foundation for Human Rights. (13 October 2010.) 'Letter from the Helsinki Foundation for Human Rights to Donald Tusk, Prime Minister of Poland.' https://www.bof.nl/live/wp-content/uploads/Premier_HFPC_specs%C5%82u%C5%BCby_13.10.2010_eng.pdf (Accessed 28 July 2014.); Human Rights House. (14 January 2011.) 'Surveillance of Polish journalists case – new developments.' http://humanrightshouse.org/noop/page.php?p=Articles/15761.html&d=shdbylgzokyw (Accessed 27 July 2014.); Downie Jr., L. (10 October 2013.) The Obama Administration and the Press: Leak investigations and surveillance in post 9/11 America. https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php (Accessed 3 March 2014.)
89. Human Rights Council. The promotion, protection and enjoyment of human rights on the Internet A/HRC/20/L.13, 29 June, 2012
90. United Nations General Assembly (21 September 2012.) The Safety of Journalists. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/Themes/Freedom_of_expression/HumanRights_Council_UNGA.pdf (Accessed 17 March 2014.)
91. A/RES/68/163 Resolution adopted by the General Assembly on 18 December 2013 'The safety of journalists and the issue of impunity' http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/163 (Accessed 6 October 2014)
92. UNESCO. (2013.) San Jose Declaration. Safe to Speak: Securing Freedom of Expression in all Media. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/WPFD/WPFD-San-Jose-Declaration-2013-en.pdf (Accessed 20 July 2014.)
93. UNESCO General Conference 37th session, November 2013. Resolution on Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf

94. Office of the United Nations High Commissioner for Human Rights. (1 July 2013.) 'The Safety of Journalists – Report of the Office of the United Nations High Commissioner for Human Rights.' https://www.coe.int/t/dghl/standardsetting/media/CDMSI/Safety%20of%20Journalists%20report.pdf (Accessed 22 July 2014.)
95. Office of the United Nations High Commissioner for Human Rights. (30 June 2014.) 'The Right to Privacy in the Digital Age.' http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf (Accessed 29 July 2014.)
96. Ministers of the Freedom Online Coalition. (28 April 2014.) 'Recommendations for Freedom Online' https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf (Accessed 25 May 2014.)
97. Access. (2014.) RightsCon. https://www.rightscon.org/ (Accessed 25 May 2014.)
98. Global Voices. (1 January 2014.) The 4th Arab Bloggers Meeting. *Global Voices*. http://ab14.globalvoicesonline.org/english (Accessed 1 February 2014).
99. Foreign Affairs Council Meeting. (12 May 2014.) 'EU Human Rights Guidelines on Freedom of Expression Online and Offline.' http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/142549.pdf (Accessed 25 May 2014.)
100. Nils Muiznieks. (19 May 2014.) https://twitter.com/CommissionerHR/status/468298394092699648 (Accessed 19 July 2014.)
101. Organization for Security and Co-operation in Europe. (2 May 2014.) Safety of Journalists Guidebook (2nd Edition). http://www.osce.org/fom/118052?download=true. (Accessed 20 July 2014.)
102. UK National Commission for UNESCO. (2014.) http://www.unesco.org.uk/journalist_safety (Accessed 11 March 2014.)
103. Email from Privacy International, 15 January 2014.
104. African Commission on Human and Peoples' Rights. (2014.) 'Activity Report of Advocate Pansy Tlakula as the special rapporteur on freedom of expression and access to information in Africa. http://www.achpr.org/sessions/55th/intersession-activity-reports/faith-pansy-tlakula/ (Accessed 20 July 2014.)
105. Unwanted Witness. (February 1 2014.) About Us. *Unwanted Witness*. https://unwantedwitness.or.ug/about-us/ (Accessed 1 February 2014.)
106. African Media Initiative. (12 July 2014.) http://africanmediainitiative.org/about (Accessed 12 July 2014.)
107. Justin Arenstein. (12 July 2014.) http://www.linkedin.com/in/justinarenstein (Accessed 1 August 2014.)
108. Independent Media Centre Kurdistan. (16 January 2014.) Start training for Iraqi journalists on ethnic and religious minorities. *Independent Media Centre Kurdistan*. http://imckiraq.blogspot.com/ (Accessed 1 February 2014.)
109. https://www.internews.org/sites/default/files/resources/Internews_PK_Secure_Journalist_2012-08.pdf
110. See *The Safety of Journalists and the Danger of Impunity*. Report by the Director-General to the Intergovernmental Council of the IPDC (Twenty-Ninth Session). CI-14/CONF.202/4 Rev2. http://unesdoc.unesco.org/images/0023/002301/230101E.pdf
111. UNESCO. (10 March 2014.) 'Training on digital security for Tunisian journalists.' http://article.wn.com/view/2014/04/10/Training_on_digital_security_for_Tunisian_journalists_UNESCO/ (Accessed 28 July 2014.)
112. IREX. (1 February 2014.) S.A.F.E. – Securing Access to Free Expression. IREX. http://www.irex.org/project/safe-securing-access-free-expression (Accessed 1 February 2014.)
113. Article 19. (20 December 2012.) Kenya: Safety training for journalists in response to increasing dangers in region. *Article 19*. http://www.article19.org/resources.php/resource/3570/en/kenya:-safety-training-for-journalists-in-response-to-increasing-dangers-in-region (Accessed 1 February 2014.)
114. Global Journalist Security. (July 2014.) 'July Course: Digital Safety for National Security Reporters.' http://www.journalistsecurity.net/new-july-courses-digital-safety-for-national-security-reporters/ (Accessed 20 July 2014.)
115. International Press Institute. (17 January 2014.) 'IPI's News Innovation Platform Is Almost Here.' http://www.ipinewsinnovation.org/news/ipis-news-innovation-platform-is-almost-here.html (Accessed 20 July 2014.)
116. Interview with Andrew Ford Lyons, 13 December 2013.
117. International News Safety Institute. (5 February 2014.) Journalism Safety: Threats to Media Workers and Measures to Protect Them. *INSI*. http://www.newssafety.org/latest/news/insi-news/detail/insi-publishes-good-practice-safety-guide-for-journalists-and-media-workers-1354/ (Accessed 12 February 2014.)
118. Derechos Digitales. (2013.) Annual Report Derechos Digitales NGO 2013. http://www.derechosdigitales.org/wp-content/uploads/DDigitales-Annual-Report-2013.pdf (Accessed 12 March 2014.)

119. http://www.fopea.org/Agenda/Ciberseguridad_para_periodistas
120. http://periodismocide.org/curso-de-seguridad-digital/
121. http://www.sipiapa.org/portfolio/redes-sociales-seguras-su-uso-personal-profesional-e-institucional/
122. Reporters Without Borders. (1 February 2014.) Era of the digital mercenaries. *Reporters Without Borders*. http://surveillance.rsf.org/en/ (Accessed 1 February 2014.)
123. Committee to Protect Journalists. (2014.) Journalist Security Guide. http://www.cpj.org/reports/2012/04/information-security.php (Accessed 30 July 2014.); Lee, M. (2 July 2013.) Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance. https://pressfreedomfoundation.org/encryption-works (Accessed 30 July 2014.); Electronic Frontier Foundation. (2013.) Surveillance Self-Defense. https://ssd.eff.org (Accessed 30 July 2014.); Electronic Frontier Foundation. (2014.) Deeplinks. https://www.eff.org/deeplinks (Accessed 30 July 2014.)
124. The Association for Progressive Communications. (2014.) 'Digital Security First-Aid Kit for Human Rights Defenders.' https://www.apc.org/en/irhr/digital-security-first-aid-kit (Accessed 1 August 2014.)
125. SKeyes Center for Media and Cultural Freedom. (1 February 2014.) The Journalist Survival Guide: An Animated Video Guide. http://video.skeyesmedia.org/ (Accessed 1 February 2014.)
126. Aryal, M., Jones, D. (24 March 2014.) 'SaferJourno: Digital Security Resources for Media Trainers.' *Internews*. https://internews.org/saferjourno-toolkit-provides-digital-and-online-safety-resources-journalism-and-media-trainers (Accessed 2 April 2014.)
127. Internews. (24 March 2014.) SaferJourno Toolkit Provides Digital and Online Safety Resources for Journalism and Media Trainers. https://Internews.org/saferjourno-toolkit-provides-digital-and-online-safety-resources-journalism-and-media-trainers (Accessed 27 March 2014.)
128. Banda, F. (2013.) Model Curricula for Journalism Education: A Compendium of New Syllabi. UNESCO Series on Journalism Education. http://unesdoc.unesco.org/images/0022/002211/221199e.pdf (Accessed 2 April 2014.)
129. The researchers sent the survey to contacts at Radio Television Digital News Association, Association for Education in Journalism and Mass Communication, Broadcast Education Association, International Center for Journalists, College Media Advisors, and the International Journalists' Network. The majority of respondents were from the United States, but participants also came from Pakistan, France, Nigeria, Mongolia and Colombia. The survey was actively in the field from 14 January 2014 – 4 February 2014, although the link remained active until August 2014.
130. Disclosure: the lead author of this report in 2015 was part of the Tow Center for Digital Journalism at Columbia Journalism School.
131. McGregor, S. (29 October 2013.) Register for the Tow Center's Journalism Security Workshop. http://towcenter.org/blog/register-for-the-tow-centers-journalism-security-workshop/ (Accessed 24 July 2014.)
132. Benton, J. (26 March 2014.) Columbia's Year Zero, aiming to give journalists literacy in data, is now called the Lede Program. http://www.niemanlab.org/2014/03/columbias-year-zero-aiming-to-give-journalists-literacy-in-data-is-now-called-the-lede-program/ (Accessed 27 March 2014.)
133. Email from Jane E. Kirtley, 13 January 2014.
134. Email from Sandeep Junnarkar, 16 January 2014.
135. Kirchner, L. (15 November 2013.) CJR: Teaching j-school students cyber-security. *Columbia Journalism Review*. http://www.cjr.org/behind_the_news/teaching_cybersecurity_in_jsch.php?page=all (Accessed 1 February 2014.)
136. Ibid.
137. Email from Ismail Hakki Polat, 23 March 2014.
138. Kadir Has University. Syllabus for NM 204 Information Security. http://www.khas.edu.tr/en/uploads/makser/NM204_syllabus_2012.pdf (Accessed 22 March 2014.)
139. Twitter correspondence with Jorge Luis Sierra, 19 March 2014.
140. Email from Henrik P. Berggreen, Uddannelsesleder, Danmarks Medie – Og Journalist Hojskole, 27 February 2014.
141. Twitter correspondence with the BBC Academy College, 20 March 2014.
142. Smyth, F. (2013.) Digital Security Basics for Journalists. Medill National Security Zone: A Resource for Covering National Security Issues. http://nationalsecurityzone.org/site/digital-security-basics-for-journalists/ (Accessed 5 January 2014.)
143. International Committee of the Red Cross. (1 January 2006.) ICRC hotline for journalists in conflict zones. http://www.icrc.org/eng/resources/documents/misc/hotline-010106.htm (Accessed 30 July 2014.)
144. Email from Erin Murrock, 3 April 2014.
145. Hammad, A. (18 February 2014.) Hackathon Hacking for a Better World. *Guardian Liberty Voice*. http://guardianlv.com/2014/02/hackathon-hacking-for-a-better-world/ (Accessed 18 February 2014.)

146. Open ITP. 18 February 2014. About Us. *Open ITP*. https://openitp.org/openitp/about-the-open-internet-tools-project.html (Accessed 18 February 2014.)
147. Open ITP Wiki. (12 February 2014.) Techno-Activism 3rd Mondays. *Open ITP*. https://wiki.openitp.org/doku.php?id=events:techno-activism_3rd_mondays (Accessed 1 February 2014.)
148. Hacks/Hackers. (18 February 2014.) About. *Hack/Hackers*. http://hackshackers.com/about/ (Accessed 18 February 2014.)
149. Ibid.
150. 'Hancel: Creating networks to protect journalists.' http://hanselapp.com/indexEN.html (Accessed 12 August 2014.)
151. Romero, C. (February 2014.) What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World. Freedom House. http://freedomhouse.org/sites/default/files/What's%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf (Accessed 29 July 2014.)
152. PEN America (13 November 2013.) The Rise of Digital Repression: a PEN Interactive Report. http://www.pen.org/infographic/rise-digital-repression-pen-interactive-report (Accessed 30 July 2014.)
153. Committee to Protect Journalists. (12 February 2014.) Attacks on the Press: Journalism on the front lines in 2013. http://cpj.org/2014/02/attacks-on-the-press-in-2013.php (Accessed 29 July 2014.) Phillips, K. (6 February 2014.) CPJ Risk List: Where Press Freedom Suffered. http://www.cpj.org/2013/02/attacks-on-the-press-cpj-risk-list.php (Accessed 30 July 2014.)
154. Ritchin, A. (21 March 2013.) 'Attacks on Women Journalists the Focus of UN Panel.' *Dart Blog*. http://dartcenter.org/blog/attacks-on-women-journalists-focus-un-panel#.Uu1atHddVgL (Accessed 1 April 2014.)
155. International News Safety Institute and International Women's Media Foundation. (10 March 2014.) *Violence and Harassment Against Women in the News Media: A Global Picture*. http://www.iwmf.org/executive-summary/ (Accessed 2 April 2014.)
156. Sexual harassment was defined with the following acts: 1) Unwanted physical contact (such as groping or other touching of sensitive areas), 2) Invasion of personal space, 3) Suggestive remarks or sounds, 4) Unwanted comments on dress and appearance, 5) Jokes of a sexual nature, 6) Display of sexually offensive material, 7) Inappropriate downloading of pornographic or sexually exploitive and degrading material by computer, 8) Verbal threats (of a sexual nature), 9) Other
157. International News Safety Institute and International Women's Media Foundation. (10 March 2014.) *Violence and Harassment Against Women in the News Media: A Global Picture*. http://www.iwmf.org/executive-summary/ (Accessed 2 April 2014.)
158. Wolfe, L. (February 2012.) 'More Discussion but Few Changes on Sexual Violence.' *Committee to Protect Journalists*. https://www.cpj.org/2012/02/attacks-on-the-press-in-2011-the-changing-views-on.php (Accessed 2 April 2014.); Wolfe, L. (7 June 2011.) 'The silencing crime: Sexual violence and journalists.' *Committee to Protect Journalists*. https://www.cpj.org/reports/2011/06/silencing-crime-sexual-violence-journalists.php (Accessed 2 April 2014.)
159. Padte Kaul, R. (5 July 2013.) 'Walking Down A Virtual Boulevard.' http://richakaulpadte.com/category/gender/ (Accessed 31 March 2014.)
160. Padte Kaul, R. (29 June 2013.) 'Keeping women safe? Gender, online harassment and Indian law.' http://internetdemocracy.in/media/keeping-women-safe-gender-online-harassment-and-indian-law-2/ (Accessed 31 March 2014.)
161. Working to Halt Abuse. (2000-2012.) 'Comparison Statistics 2000-2012.' *Working to Halt Abuse*. http://www.haltabuse.org/resources/stats/Cumulative2000-2012.pdf (Accessed 29 March 2014.)
162. Meyer, R. and Cukier, M. (2006.) 'Assessing the Attack Threat due to IRC Channels.' *Proceedings of the International Conference on Dependable Systems and Networks*. http://www.umiacs.umd.edu/publications/assessing-attack-threat-due-irc-channels (Accessed 2 April 2014.)
163. Email from Dr. Michel Cukier, 11 April 2014.
164. International News Safety Institute and International Women's Media Foundation. (March 10, 2014.) *Violence and Harassment Against Women in the News Media: A Global Picture*. http://www.iwmf.org/intimidation-threats-and-abuse/ (Accessed 2 April 2014.)
165. Citron Keats, D. (25 November 2009.) 'Law's Expressive Value in Combating Cyber Gender Harassment.' *Michigan Law Review*. http://www.michiganlawreview.org/assets/pdfs/108/3/citron.pdf (Accessed 1 April 2014.)
166. Citron Keats, D. (25 November 2009.) 'Law's Expressive Value in Combating Cyber Gender Harassment.' *Michigan Law Review*. http://www.michiganlawreview.org/assets/pdfs/108/3/citron.pdf (Accessed 1 April 2014.)
167. Ibid.
168. Index on Censorship. (1 April 2014.) 'Twitter trolls in India: Sexist abuse as a tool to muzzle women.' (Accessed 5 April 2014.) https://www.ifex.org/india/2014/04/04/trolls_muzzle_women/
169. Ibid.

170. Anand, A. (8 February 2014.) 'Kavita Krishnan: 'I was accused by one minister of standing for free sex.' *The Observer* http://www.theguardian.com/politics/2014/feb/09/kavita-krishnan-communist-india-accused-minister-free-sex (Accessed 2 April 2014.)
171. Penny, L. (4 November 2011.) 'Laurie Penny: A woman's opinion is the mini-skirt of the Internet' *The Independent*. http://www.independent.co.uk/voices/commentators/laurie-penny-a-womans-opinion-is-the-miniskirt-of-the-internet-6256946.html (Accessed 3 April 2014.)
172. Index on Censorship. (1 April 2014.) 'Twitter trolls in India: Sexist abuse as a tool to muzzle women.' https://www.ifex.org/india/2014/04/04/trolls_muzzle_women/ (Accessed 5 April 2014.)
173. Wallace, Amy. (19 January 2014.) 'Life as a Female Journalist: Hot or Not?' *New York Times*. http://www.nytimes.com/2014/01/20/opinion/life-as-a-female-journalist-hot-or-not.html (Accessed 22 February 2014.)
174. Ibid.
175. Vittal, V. (27 July 2013.) 'Online Abuse of Women: Why trolls have it so easy.' http://indiatogether.org/internet-women (Accessed 4 April 2014.)
176. Masters, J. (6 March 2014.) 'Sexism in sport: Why do Internet trolls target women?' *CNN*. http://edition.cnn.com/2014/03/06/sport/sexism-in-sport-female-journalists-abuse/ (Accessed 4 April 2014.)
177. Food Democracy Now! 'New York Times Writer Amy Harmon travels to Hawaii…falls in love with GMOs.' *Food Democracy Now! Facebook page*. https://www.facebook.com/photo.php?fbid=10152209502794388&set=a.10150644870149388.450934.162878479387&type=1&theater (Accessed 20 March 2014.)
178. Wallace, Amy. (19 January 2014.) 'Life as a Female Journalist: Hot or Not?' *New York Times*. http://www.nytimes.com/2014/01/20/opinion/life-as-a-female-journalist-hot-or-not.html (Accessed 22 February 2014.)
179. IREX. (21 November 2013.) 'Gender-Based Violence Against Journalists: Realities and Responses.' http://www.irex.org/news/gender-based-violence-against-journalists-realities-and-responses (Accessed 22 January 2014.)
180. Committee to Protect Journalists. (2013.) 'Janet Hinostroza, Ecuador: 2013 CPJ International Press Freedom Awardee.' https://www.cpj.org/awards/2013/janet-hinostroza-ecuador.php (Accessed 12 March 2014.)
181. Freeman, H. (30 July 2013.) How to use the Internet without being a total loser. *The Guardian*. http://www.theguardian.com/commentisfree/2013/jul/30/how-use-internet-loser-twitter (Accessed 29 July 2014.)
182. Williams, H. (9 August 2013.) 'Twitter bomb threats: Online and offline, female journalists face abuse 'all the time." *Reuters*. http://www.trust.org/item/20130809124626-79zhw/?source=shtw (Accessed 9 February 2014.)
183. Email conversation with digital security technologist who asked to remain anonymous.
184. Cyberstalking can also include: repeated threats or false accusations via email or mobile phone, making threatening or false posts on websites, stealing a person's identity or data or spying and monitoring a person's computer and Internet use. Sometimes the threats can escalate into physical spaces.
185. Kee, J. 'Cultivating Violence through Technology? Exploring the Connections between Information Communication Technologies (ICT) and Violence Against Women (VAW.) *Association of Progressive Communications Women's Networking Support Programme*. http://www.genderit.org/sites/default/upload/VAW_ICT_EN.pdf. (Accessed 12 March 2014.)
186. Strawhun, J., Adams, N., Huss, M. (2013.) 'The Assessment of Cyberstalking: An Expanded Examination Including Social Networking, Attachment, Jealousy, and Anger in Relation to Violence and Abuse. *Violence and Victims*. Springer Publishing Company. 28.4: 715-30.
187. Strawhun, J., Adams, N., Huss, M. (2013.) 'The Assessment of Cyberstalking: An Expanded Examination Including Social Networking, Attachment, Jealousy, and Anger in Relation to Violence and Abuse. *Violence and Victims*. Springer Publishing Company. 28.4: 715-30.Anonymous. (April 2000.); 'Beware of cyberstalking—the latest workplace threat.' HR Focus 77.4 Accessed through ProQuest.
188. Association for Progressive Communications (APC) Women (1 November 2010.) 'How Technology is Being Used to Perpetrate Violence against Women – and to Fight It. http://www.comminit.com/content/how-technology-being-used-perpetrate-violence-against-women-and-fight-it (Accessed 3 April 2014.)
189. Moore, A. (3 February 2014.) 'Cyberstalking and Women – Facts and Statistics: Few Laws in Place to Deal With This Rapidly Growing Threat.' http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm (Accessed 2 April 2014.)
190. Sam Houston State University. (9 February 2013.) 'New Study Compares Stalking, Cyberstalking.' US Fed News Service. HT Media Ltd. Accessed through ProQuest.
191. Rupley, S. (17 June 2003.) 'Cyberstalking On the Rise; Stay alert when online. *PC Magazine*. Ziff-Davis Media Inc. Vol. 22 Issue 10. Accessed through ProQuest.

192. Pittaro, M. (2007) 'Cyberstalking: An Analysis of Online Harassment and Intimidation.' *International Journal of Cyber Criminology*. Vol. 1 (2): 180-197. http://www.cybercrimejournal.com/pittaroijccvol1is2.htm (Accessed 1 April 2014.)
193. Ginty, M. (2 May 2011.) 'Cyberstalking Turns Web Technologies into Weapons.' *WeNews*. http://womensenews.org/story/crime-policylegislation/110501/cyberstalking-turns-web-technologies-weapons?page=0,1#.UvjrKkJdUeY (Accessed 12 March 2014.)
194. Quick, A. (2012.) 'TheVillage Founder, Vickie Newton, Targeted by Internet Stalker.' *The Village Celebration*. http://www.thevillagecelebration.com/thevillage-founder-vickie-newton-targeted-by-internet-stalker/ (Accessed 11 March 2014.)
195. International News Safety Institute and International Women's Media Foundation. (10 March 2014.) *Violence and Harassment Against Women in the News Media: A Global Picture*. http://www.iwmf.org/intimidation-threats-and-abuse/ (Accessed 2 April 2014.)
196. Friedersdorf, C. (7 January 2014.) 'When Misogynist Trolls Make Journalism Miserable for Women.' *The Atlantic*. http://www.theatlantic.com/politics/archive/2014/01/when-misogynist-trolls-make-journalism-miserable-for-women/282862/ (Accessed 12 March 2014.)
197. Hess, A. (6 January 2014.) 'Why Women Aren't Welcome on the Internet.' *Pacific Standard*. http://www.psmag.com/navigation/health-and-behavior/women-arent-welcome-internet-72170/ (Accessed 14 March 2014.)
198. Ibid.
199. Swim, J. K., Hyers, L. L, Cohen, L. L, & Ferguson, M. J. (2001). Everyday sexism: Evidence for its incidence, nature, and psychological impact from three daily diary studies. *Journal of Social Issues*, 57, 31-53.
200. Vittal, V. (27 July 2013.) 'Online Abuse of Women: Why trolls have it so easy.' http://indiatogether.org/internet-women (Accessed 4 April 2014.)
201. Halvorson, H. (6 September 2011.) 'Reasons Why It Pays to Not Let Sexist Comments Slide.' *Forbes*. http://www.forbes.com/sites/heidigranthalvorson/2011/09/06/3-reasons-why-it-pays-to-not-let-sexist-comments-slide/2/ (Accessed 20 March 2014.); Hillard, A. (1 July 2011.) 'Why Confronting Sexism Works: Applying Persuasion Theories to Confronting Sexism.' University of Nebraska-Lincoln. http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1035&context=psychdiss (Accessed 3 April 2014.)
202. Hyers, L. L. (2007). Resisting prejudice every day: Exploring women's assertive responses to anti-Black racism, anti-Semitism, heterosexism, and sexism. *Sex Roles*, 56, 1-12.
203. Tiger Beatdown. 'But How Do You Know It's Sexist? The #MenCallMeThings Round-up' http://tigerbeatdown.com/2011/11/10/but-how-do-you-know-its-sexist-the-mencallmethings-round-up/ (Accessed 29 March 2014.)
204. Chemaly, S. (28 January 2013.) 'The Digital Safety Gap and the Online Harassment of Women.' *Huffington Post*. http://www.huffingtonpost.com/soraya-chemaly/women-online-harassment_b_2567898.html?utm_hp_ref=tw (Accessed 29 March 2014.)
205. Padte Kaul, R. (5 July 2013.) 'Walking Down A Virtual Boulevard'. http://richakaulpadte.com/category/gender/ (Accessed 1 April 2014.)
206. Tactical Technology Collective. 'About the Campaign: What is Take Back the Tech?' https://www.takebackthetech.net/page/about-campaign (Accessed 2 April 2014.)
207. Association for Progressive Communications. 'How Technology is Being Used to Perpetrate Violence Against Women – *And to Fight it*.' https://www.apc.org/en/system/files/How+Technology+is+Being+Used+to+Perpetrate+Violence+Against+Women+–+And+to+Fight+it.pdf (Accessed 14 March 2014.)
208. Association for Progressive Communications. 'Cyberstalking and how to prevent it.' *Take Back the Tech*. https://www.takebackthetech.net/be-safe/2-cyberstalking-and-how-prevent-it (Accessed 12 March 2014.)
209. Association for Progressive Communications. 'Map it. End it.' *Take Back the Tech*. https://www.takebackthetech.net/mapit/ (Accessed 12 March 2014.)
210. HarassMap. 'What We Do.' http://harassmap.org/en/what-we-do/ (Accessed 4 April 2014.)
211. Tumblr. (27 January 2014.) 'Community Guidelines.' http://www.tumblr.com/policy/en/community (Accessed 21 March 2014.)
212. Fernando, A. (31 January 2014.) 'How to Stop the Online Harassment of Female Journalists.' *10,000 Words*. http://www.mediabistro.com/10000words/harassment-female-journalists_b25653 (Accessed 22 March 2014.)
213. These recommendations draw on in-depth interviews with a variety of sources as well as publications from Access, European Digital Rights (EDRi), Reporters without Borders, Committee to Protect Journalists, and Edward Snowden's March 2014 TED talk (as reported by *Wired*).
214. UN General Assembly Resolutions A/RES/68/167 and A/RES/69/116
215. UNESCO General Conference. (November 2013.) 'Resolution on Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions

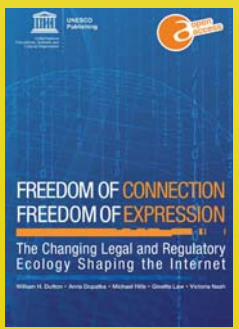
of the information society.' http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf (Accessed 29 July 2014.)
216. United Nations. (21 February 2014.) The safety of journalists and the issue of impunity. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/163 (Accessed 30 July 2014.)
217. Björksten, G. (27 March 2014.) 'Innovating our Future: Gustaf Björksten.' Innovating Our Future. https://www.youtube.com/watch?v=pMae8pZC4DE (Accessed 31 March 2014.)
218. McGregor, S. and Ag, M. (17 March 2014.) 'TA3M on JournoSec with Susan McGregor of Columbia and Magnus Ag of Committee to Protect Journalists.' https://www.youtube.com/watch?v=tu0_ySgLgys&feature=youtu.be (Accessed 20 March 2014.)
219. Stray, J. (21 August 2014.) Security for Journalists, Part Two: Threat Modeling. https://source.opennews.org/en-US/learning/security-journalists-part-two-threat-modeling/ (Accessed 22 August 2014.)
220. Banda, F. 2013. Model Curricula for Journalism Education: A Compendium of New Syllabi. UNESCO Series on Journalism Education. http://unesdoc.unesco.org/images/0022/002211/221199e.pdf (Accessed 30 July 2014.)
221. Romero, C., (February 2014.) 'Conference Report: What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World.' Freedom House. http://www.freedomhouse.org/report/special-reports/what-next-quest-protect-human-rights-defenders-and-journalists-digital-world#.U_D45FbrPa5 (Accessed 8 March 2014.)
222. UNESCO General Conference. (November 2013.) 'Resolution on Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society.' http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf (Accessed 1 August 2014.)
223. General Assembly resolution A/HRC/27/L.7, adopted at the Human Rights Council, twenty-seventh session.
224. Josh Levy in 2014 was Advocacy Director at Access.
225. Josh Stearns in 2014 was Director of Journalism and Sustainability at the Geraldine R. Dodge Foundation.
226. Lindsey Beck in 2014 was Program Manager for Radio Free Asia's Open Technology Fund.
227. Paul Mooney in 2014 was Bureau Chief with Reuters in Yangon.
228. Seamus Tuohy in 2014 was Technical Advisor at Internews.
229. The survey was offered in English, French, Chinese, Arabic and Spanish.
230. The researchers asked their contacts at the following organizations to disseminate the survey: International News Safety Institute, International Research and Exchanges Board, Committee to Protect Journalists, Global Voices, International Federation of Journalists, CommunityRED, Tow Center for Digital Journalism, Online News Association, Poynter, PEN International, Society of Professional Journalists, Open ITP. QuestionPro also disseminated the survey to its panelists in a variety of countries.
231. There were 18 pilot study respondents who completed the survey.

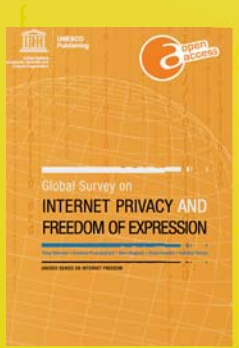
In order to improve global understanding of emerging safety threats linked to digital developments, UNESCO commissioned this research within the Organization's on-going efforts to implement the UN Inter-Agency Plan on the Safety of Journalists and the Issue of Impunity, spearheaded by UNESCO. The UN Plan was born in UNESCO's International Programme for the Development of Communication (IPDC), which concentrates much of its work on promoting safety for journalists.

The safety for journalists, including digital safety, is a matter of public concern that is wide-ranging. It is vital for those who practice journalism, for their families and for their sources. It is essential for the wellbeing of media institutions, civil society, academia and the private sector more broadly. If we value the free flow of information for citizens, their governments and their international organisations, then the safety of journalists is central.

Getachew Engida
Deputy Director-General of UNESCO

UNESCO SERIES ON INTERNET FREEDOM





United Nations
Educational, Scientific and
Cultural Organization

Communication and Information Sector

9 789231 000874