CPJ

JOURNALIST SECURITY GUIDE

COVERING THE NEWS IN A DANGEROUS AND CHANGING WORLD

By Frank Smyth/CPJ Senior Adviser for Journalist Security

With a chapter on Technology Security by CPJ Staff Technologist Tom Lowenthal and Danny O'Brien

Committee to Protect Journalists

CPJ

Contents

Introduction: A New World of News

The world is an increasingly dangerous place for journalists. On average, more than 30 journalists are murdered every year, and the murderers go unpunished in nearly nine of 10 cases. Hundreds of journalists each year are attacked, threatened, or harassed. Many are followed or have their phone calls and Internet communications intercepted. More than 150 are behind bars at any given time, some without being charged with a crime. The whereabouts of at least 35 journalists are unknown. Throughout the profession, journalists face emotional stress whenever they cover stories involving pain or loss of life, from the sexual abuse of children to terrorist attacks against civilians.

The world is a smaller place for journalists, too. Digital technology enables nearly everyone to follow not only events in real time, but also reporting by specific journalists and media outlets. Violent and corrupt actors worldwide understand not only how information shapes perceptions, but how the work of individual journalists can threaten their activities. In some countries, an unprecedented level of partisanship on cable, broadcast, and Internet news outlets has blurred the lines between reporters and advocates, putting even more stress on the notion that journalists are neutral or professional observers. The result is a more hostile environment for the press in places from sleepy small towns to international war zones. Journalists everywhere need to watch their own and each other's backs now more than ever before.

The business of news is also different. Newsroom cutbacks have resulted in more freelancers reporting on the frontlines of stories, from overseas tsunamis to local highway accidents, ocean oil spills to political demonstrations, armed conflicts to organized crime. Although many of these stringers carry press credentials from major media organizations, they are still contract employees who may be responsible for their own preparation, equipment, insurance, and care. Citizen journalists of all kinds are likely to face the same challenges. Unpaid contributors are reporting stories for evolving new-media networks with little or no support or training. Today, more journalists than ever are deciding what stories to cover and how to approach them. In other words, they are working largely on their own.

This guide details what journalists need to know in a new and changing world. It is aimed at local and international journalists of varied levels of experience. The guide outlines basic preparedness for new journalists taking on their first assignments around the world, offers refresher information for mid-career journalists returning to the field, and provides advice on complex issues such as digital security and threat assessment for journalists of all experience levels.

1. Basic Preparedness

Never have so many different types of journalists reported the news on so many different platforms. Yet no matter the form of journalism—from investigative to beat reporting, foreign correspondence to domestic coverage, blogging to photojournalism—thorough preparation is the starting point.

Carefully research your assignment or beat. Learn the terrain, history, players, dynamics, and trends by drawing on diverse viewpoints. (See the sections below on Foreign Correspondence and Domestic Journalism.) Be versed in the culture, mores, and idioms of any group being covered. Language skills are very helpful, especially knowing basic terms and phrases. Develop a list of potential news sources across a range of perspectives. Draft detailed contingency plans in case of emergencies, identifying exit routes and trusted contacts you will keep updated on your location, plans, and work details. (See Chapter 2 Assessing and Responding to Risk.) Other valuable preparatory steps include obtaining appropriate health insurance as well as vaccinations (as explained in the sections below on Insurance Coverage and Medical Care and Vaccinations), understanding information and communications security (as covered in Chapter 3 Technology Security), and receiving appropriate conflict training and equipment (as described in Chapter 4 Armed Conflict).

> *Understand the culture and be aware of your surroundings. Travel with colleagues and support staff. Stay close to the edges of crowds and have an exit route in mind.*

Foreign Correspondence

Thoroughly researching a foreign destination before traveling there is essential to staying safe. Closely review news reports reflecting a range of perspectives, diverse academic sources, travel and health advisories from the World Health Organization and other governmental or multilateral agencies, and reports on human rights and press freedom from both government and nongovernmental sources. Common travel guides can provide essential information about cultures and their mores. Before traveling to a location, especially for the first time, seek the advice of journalists with experience in that locale. Situation-specific advice from trusted colleagues is crucial in planning an assignment and assessing risks. If you are inexperienced in the profession or new to a particular location, you might also consider asking seasoned colleagues if you can accompany them for a time as they work.

Make every effort to learn basic expressions in native languages to enable daily interactions and to show respect, both of which can enhance your security. Research travel routes out of the area along with the status of available medical facilities. American University's Foreign Correspondence Network provides a list of diverse resources that can help in your preparation.

Always prepare a security assessment in advance of a potentially dangerous assignment. Before departing, establish clear points of contact with editors, colleagues, and family members or friends. Your contacts in the field should know how to reach your family members and editors; your relatives and editors, in turn, must know how to reach your local contacts. Research in advance where you might want to stay, the state of the communications infrastructure, and the possibility of surveillance. Decide how you intend to communicate with editors and others at home—by landline telephone, Voice over Internet Protocol, chat, or email—and whether to choose pseudonyms along with some kind of code system, forms of encryption, or other secure means of electronic communication. (See Chapter 3 Technology Security.) Before departure, arrange or develop specific leads for fixers, drivers, and translators. Use great care and diligence in vetting local support staff, and be sure to seek recommendations from colleagues. Because your safety is often in the hands of support staff, it's essential that you choose trustworthy, knowledgeable individuals.

Journalists aspiring to embed with military units should make contacts and arrangements before they go.

In many nations, it may be wise to have someone meet you at the airport and escort you to your initial lodging. That will allow you to acclimate and avoid unfamiliar hazards such as unsafe roads or criminals. Choose lodging in advance. Your choice of a hotel or other lodging depends in part on the profile you want to keep. Large hotels catering to business clientele often provide high levels of security but may tend to raise your profile. Large hotels also provide services such as wireless Internet, although connections can be compromised in repressive countries. Choosing a small hotel or private lodging allows you to keep a lower profile, which may enhance your ability to carry out an assignment. Such lodging, however, typically has lower levels of security or none at all. Avoid rooms or lodging with balconies or windows that can be accessed by intruders. Always plan exit routes in case of emergencies.

Recommended security training or equipment such as body armor should be obtained in advance. (See Chapter 4 Armed Conflict.) Prescription medication should be packed in original, labeled containers in carry-on luggage, the World Health Organization advises. You may wish to pack duplicate medications (along with contact information for your physician) in other bags in case your carry-on luggage is lost or stolen. Liquids over three ounces or 85 milliliters must be packed in stowed luggage to clear most airport security inspections. You should also carry an international vaccination card as well as official documentation of your blood type and any allergies or other medical conditions. Identify the availability of medical care in the reporting area, including the locations of hospitals, clinics, and primary-care physicians.

Appropriate clothing, including foul-weather gear, should also be purchased before departure. Journalists operating overseas should choose earth tones or dark colors that will not stand out at a distance and are distinct from the blue used by law enforcement or the army green or camouflage colors used by military units. Any journalist expecting to cover a moving story by foot must have supportive footwear, a sturdy backpack, and comfortable sleeping gear. Break in footwear before arriving on assignment. Pack gear that may be hard to find in less developed nations; such items could include batteries, flashlights, notebooks, tampons, dental floss, a compact first-aid kit, antiseptic, and athlete's foot cream, as well as pouches or devices to hide money. (See Appendix A Checklists for a more comprehensive list of gear.) Journalists should make sure that they have access to cash in either U.S. dollars or euros. The International Federation of Journalists recommends carrying a dummy wallet filled with official-looking cards and some cash in case you are robbed.

Your passport and any required visas should be up to date. The passport should have at least six months before expiration and enough blank pages for visa stamps. You may also wish to obtain an international driver's license in advance from a reputable provider. Having an international license, along with a license from your home jurisdiction, is required in some nations and may make it easier to rent cars in some locations.

Domestic Journalism

While foreign journalists face significant logistical and security challenges, domestic journalists face more severe threats to their lives and freedom. Nearly nine in 10 work-related fatalities since 1992 have involved local journalists covering news in their home countries, CPJ research shows. And more than 95 percent of journalists jailed worldwide are local reporters, photojournalists, bloggers, and editors, according to CPJ research. The need for thorough preparation and security planning is especially acute for domestic reporters.

If you are new to the profession, a beat, or a particular type of assignment, you may wish to seek out experienced colleagues for advice and potential mentoring. With permission, accompany a seasoned

colleague for a time as he or she works; you can gain valuable hands-on knowledge by watching a veteran at work. You should research all applicable press laws, including statutes governing access to public information, access to private property, libel and slander, and the restrictions on content that many repressive countries seek to impose. Countries such as Ethiopia, for example, consider the mere coverage of opposition groups to be an antistate crime. China imprisons writers who are critical of the central government or the Communist Party. Dozens of journalists each year are jailed worldwide on such antistate charges. Even if you choose to push content boundaries, you need to know the restrictions and the potentially significant implications of going beyond them.

Beat reporters covering politics, corruption, crime, and conflict are at particularly high risk of attack or imprisonment, CPJ research shows. If you are covering a beat, you should invest time in understanding the security implications of your topic; identifying the major actors and learning their motivations; and understanding the ramifications of going beyond red lines that are enforced through statute or violent, extralegal means. Editors should allow journalists who are new to a beat enough preparatory time for them to meet sources, talk to experienced colleagues, and learn practices and terminology relevant to the topic. A crime beat, in particular, demands an understanding of law enforcement procedures. (See Chapter 5 Organized Crime and Corruption, and Chapter 6 Civil Matters and Disturbances.) On crime and other high-risk assignments, you should develop a security assessment in consultation with editors. (See Chapter 2 Assessing and Responding to Risk.)

If you are a freelancer considering an assignment for a domestic or international news outlet, you should have a clear understanding of the potential risk and the news organization's ability and willingness to provide support if you encounter trouble. You should always develop a security assessment prior to a potentially dangerous assignment, enlist reliable security contacts, and establish a precise procedure for regular check-ins. (See Chapter 2 Assessing and Responding to Risk.) Freelancers should not hesitate to turn down a risky assignment. In some highly repressive countries, you may be forbidden by law from working as a journalist for an international news organization. Know the law and the implications of working for foreign news media. In a number of other countries, you may not wish to be identified in a byline or credit line. You should understand the implications of having your name appear on a story produced by a news organization based in a country seen as an adversary. Clearly convey to the assigning outlet your wishes about being identified.

Freelancers should understand the potential risk of an assignment, along with the news organization's ability to provide support. Don't hesitate to turn down a risky assignment.

All local reporters should learn what professional support is available. A number of countries have effective professional organizations that can provide guidance about laws concerning the press, along with practical advice on certain assignments. If you encounter trouble, some national organizations are also able to intervene on your behalf or publicize your case. You should also be aware that international groups such as CPJ and Reporters Without Borders can generate global attention and advocacy in case of harassment or threats. (For a listing of local and international groups, see Appendix E Journalism Organizations. The International Freedom of Expression Exchange maintains a comprehensive list of groups.)

If you are asked to work as an interpreter or fixer for an international journalist, get a clear understanding of the risk inherent in the assignment. Make sure you understand in advance whom you are seeing and where you are going. Evaluate the international journalist with whom you may work, assessing their experience, track record, and tolerance for risk. Consider the perception of appearing in a hostile area with a reporter from a country that is seen as an adversary. Understand that you can turn down an assignment, and understand what level of support the assigning journalist or news outlet can provide if you encounter trouble. Get a clear understanding of your role in an assignment. Are you being asked to interpret and provide logistics? Or are you also doing reporting? The latter has additional security implications that you

should understand.

For all types of local reporters and fixers, news outlets and their editors should clearly explain the role that the individual is expected to play and the legal and security support the organization is able to provide if a problem occurs. Editors should understand that a local journalist may turn down a risky assignment, and accept that judgment without penalty to the individual. News outlets must consider their ethical obligation in assigning a local freelance reporter to a dangerous task.

Independent bloggers, videographers, and citizen journalists have emerged as important providers of news, particularly during the Arab uprisings that began in 2011. In Libya and Syria, where authorities blocked international media access, local citizens came forward as independent journalists. Some filmed government crackdowns and posted footage online, while others disseminated breaking news through independent blogs, micro-blogs, and social media. In heavily restricted areas, their work opened a window through which the rest of the world could view the conflicts. Several of these journalists paid with their lives. In Syria, independent videographers Ferzat Jarban and Basil al-Sayed died in apparent targeted killings; in Libya, the founder of an independent website, Mohammed al-Nabbous, was shot while streaming live audio from a battle in Benghazi.

Independent bloggers and videographers should develop a network of professional and family contacts that can be mobilized in an emergency. The London-based Institute for War & Peace Reporting has helped citizen journalists organize local networks in the Balkans and the Middle East. In many nations, such networks must be created in a manner that protects the identities of their members. (See Chapter 3 Technology Security for detailed information on how to communicate securely.) Prepare a security assessment as described in Chapter 2. Independent bloggers, videographers, and other citizens taking up journalistic work in times of crisis should understand the acute dangers of working without institutional support and operating largely on one's own. Rigorous security planning, including the use of safe communication and the practice of making regular contact with colleagues and relatives, is vital.

Press Credentials

Obtain press credentials before reporting, as you may need to prove your status upon demand. Many news organizations issue credentials on request to contract employees and other freelancers. At the very least, freelancers should obtain from an assigning news outlet a letter on the organization's stationery that states their affiliation. Various journalist associations and trade groups also issue press credentials to qualified individuals who join their organizations, including the National Writers Union and the National Press Photographers Association, each based in the United States, and the International Federation of Journalists, based in Belgium. Many press associations in other nations do the same, although independent bloggers can still face difficulty in getting credentials. Independent bloggers may find that compiling a portfolio of their journalistic work can help them make a case for obtaining press credentials.

You should also research and obtain press credentials from municipal, regional, or national authorities, recognizing that officials may issue credentials on a selective basis in an attempt to influence coverage (See Chapter 6 Civil Matters and Disturbances). Press credentials from a local police department could prove useful when you're covering a local demonstration. Credentials may also be needed to take pictures or record events in public buildings such as state capitols or national assemblies.

Journalists traveling internationally should also research and inquire whether they need a journalist visa to report in a country. The answer is not always clear. In such cases, journalists should speak with other reporters and government officials to determine how best to proceed. In many instances, journalists have traveled to restrictive countries on tourist or other non-journalistic visas as a way to circumvent censorship and effectively carry out their work. Journalists should, however, weigh, potential legal consequences.

"In countries where the government might place restrictions on foreign reporters, you need to weigh those limitations against the consequences of being caught without proper accreditation," according to a fact sheet on credentialing compiled by journalist Michael Collins for the U.S.-based Society of Professional Journalists. "In the end it's a decision only you can make, but when dealing with the police, armed forces, or other officials it's almost always better to have official accreditation."

Military authorities sometimes issue their own credentials to journalists. Government military forces as well as rebel armed groups may require a journalist to obtain written authorization from a superior officer in order to clear armed checkpoints. These authorizations can range from a letter signed with a group's official seal to the business card of a commander who writes a brief note on the back. Be mindful of which credentials and authorizations you show at any given time. One group may perceive the possession of a rival's authorization as a sign of enemy collaboration.

Journalists working internationally should travel with multiple photocopies of their passport, credentials, and any accrediting letters, in addition to extra passport-size photos.

Insurance Coverage

Securing adequate health and disability insurance is among the more difficult challenges faced by many journalists. Staff journalists working domestically should thoroughly review any policies provided by their employers for conditions and restrictions. Contract journalists should attempt to negotiate for coverage with their assigning news organization. But freelance journalists may have to find and pay for coverage on their own; they should take the time to research plans that fit their specific needs. (A surprising number of journalists, from community radio reporters working in less-developed nations to war photojournalists working for major Western media, routinely work with little or no health insurance, as dozens of working journalists have told CPJ.)

Journalist associations in more affluent nations may offer access to different health and life insurance plans. The Society of Professional Journalists offers a number of insurance plans, including hospital income insurance, major medical insurance for severe and long-term injuries, accidental death or dismemberment benefits, and disability income insurance. The SPJ plans are not available in all U.S. states and are not available to journalists working outside the United States. The National Writers Union and National Press Photographers Association offer insurance plans to their respective members.

Journalists working internationally have some options. The Paris-based press freedom group Reporters Without Borders, in collaboration with the private insurer World Escapade Travel Insurance, based in Quebec, Canada, offers insurance plans at competitive rates for journalists, including freelancers, working outside their country of residence. These policies cover journalists working in hostile regions, including war zones around the world. Plan costs vary, depending on the destination. The coverage may be purchased by day for up to 365 days. Additional coverage is available to include pre-existing conditions. To become eligible for the plans, journalists must pay a fee to join Reporters Without Borders. The plans include emergency assistance protection, coverage during travel or while "embedded" with military forces (active participation as a combatant would void the coverage), and accidental death and dismemberment payments.

A number of private insurance brokers and firms also offer health, disability, and life insurance to travelers, including journalists working internationally; the costs and coverage vary depending on many factors. (See a listing of potential providers in Appendix C Insurance Providers.) Thoroughly research your options and review the policies for possible restrictions, such as exclusions for injuries resulting from acts of war or terrorism. The World Health Organization recommends that international travelers confirm that their insurance covers changes in itinerary, emergency medical evacuation, and repatriation of remains

in case of death. Keep in mind that coverage of long-term injury or disability may be the most important part of any plan. Coverage for contingencies such as emergency medical evacuation can be prohibitively expensive, and evacuation itself may not be possible in major war zones or extremely remote areas. In such cases, journalists may have no choice but to rely on locally available medical treatment.

Medical Care and Vaccinations

Keeping physically fit and maintaining a proper diet are primary preventive measures. Journalists expecting to be abroad or on remote assignment for any significant length of time should consider pre-departure visits to medical professionals, including their primary care physician, dentist, optometrist, gynecologist, or physical therapist. Any necessary dental work, in particular, should be resolved before leaving.

If you're going abroad or on remote assignment, it's important to take care of your health. Visit your primary care physician and other medical professionals in advance.

If you plan to work internationally, consult with a qualified physician or clinic that caters to international travelers to ensure you receive all recommended vaccinations in advance. As proof of vaccinations, make and carry photocopies of a signed and stamped yellow-colored International Certificate of Vaccination as approved by the World Health Organization; this certificate is available from almost all qualified clinics. Some insurers, the World Health Organization says, may require proof of immunization as a condition for emergency medical coverage or repatriation in case of emergency. Some nations may require proof of vaccination as a condition of entry; check the requirements of specific nations. Bolivia, for instance, has required visitors to have a yellow fever vaccination.

Most doctors recommend a 10-year tetanus shot for adults aged 19 to 64. For journalists traveling to areas where malaria is prevalent, doctors may also prescribe a prophylactic antimalarial medication to protect against infection. For some areas, vaccination against polio, hepatitis A and B, yellow fever, and typhoid may also be recommended. The vaccination for hepatitis B must be planned a half-year in advance because it requires three separate inoculations over a six-month period. Vaccination for yellow fever is mandatory for travel to most West African and Central African countries. Meningitis and polio vaccines are required for travel to Mecca in Saudi Arabia. The World Health Organization provides updated disease distribution maps.

Vaccinations against cholera are no longer routinely recommended for international travel, although an oral cholera vaccine may be recommended for aid workers, journalists, and others traveling to high-risk areas. An oral cholera vaccination approved for use by many nations requires two doses taken over a span of two to not more than six weeks.

Expect that some vaccinations may make you temporarily ill, but any prolonged or high fever should be reported immediately to a physician. Be aware that no vaccination is 100 percent effective. Neither are vaccinations a substitute for taking other reasonable and necessary precautions against contracting illness or disease.

Personal Precautions

Clean drinking water is essential at all times. Bottled water in sealed containers is one option in areas where tap water is known to be or suspected of being contaminated. (The International Federation of Journalists recommends drinking only bottled carbonated water in many nations; bottled still water can be contaminated.) If dirty water cannot be avoided, bringing the water to a visible, rolling boil for at least one minute is the most effective way to kill pathogens, according to the World Health Organization.

Allow the water to cool at room temperature before placing it in a refrigerator. There are other ways to sanitize water, depending on the level of suspected contaminants. Use of iodine pills or chlorine will kill most parasites. But in regions such as South Asia and much of sub-Saharan Africa, filter systems made of ceramic, membrane, or carbon may be the only way to effectively filter pathogens, including microscopic elements of human waste. Journalists should research the water purification method most appropriate for their destination.

In areas with potentially contaminated water, eat only food that is thoroughly cooked. Fruit should be peeled or washed in clean water. Avoid food from street vendors, along with products made with raw milk, water, or eggs. Avoid swallowing water when showering, use clean water to brush your teeth, and wash your hands and tableware before eating. Use of hand sanitizer is recommended. Avoid exposure to open water as well. The World Health Organization points out that coastal and inland waters, and even hotel pools and spas, may be at risk for water-borne infections. Riverbanks and muddy terrain should not be traversed without appropriate, water-resistant footwear.

In hot climates, especially during times of physical activity, adding table salt to food or drink can prevent loss of electrolytes, dehydration, and heat stroke. The World Health Organization recommends carrying an oral rehydration solution. If none is available, a substitute is to mix six teaspoons of sugar and one teaspoon of salt into one liter of safe drinking water. In malarial zones, be sure to have mosquito netting and wear long sleeves and pants.

Any cuts or abrasions should be immediately treated with an antiseptic cream or ointment. Itching or flaking between the toes should also be immediately treated with an athlete's foot or other anti-fungal treatment. (Strong, over-the-counter athlete's foot creams will also stop the spread of other fungi.) Wash daily, even if it is only with a wet cloth or towel. Talcum powder can be applied on sensitive areas of the skin. If you're allergic to bee stings or other insect bites, carry a self-injection kit or other prescribed antidotes. Carry sufficient and updated medication, contact lenses, and eyeglasses, including spares.

Know your blood type and carry a blood donor card or other medical card that clearly indicates it. Those working in hostile environments may wish to wear either a bracelet or a laminated card around their neck indicating their blood type and any allergies. Anyone allergic to drugs such as penicillin should always carry or wear a prominent card, bracelet, or other identification alerting medical personnel to the allergy. In nations with especially high rates of HIV infection, some Western embassies maintain blood banks open to embassy staff and other nationals visiting the nation. Journalists may have the option to donate blood with the understanding that the blood bank would be made available to them if necessary. Be mindful of the risks of contracting sexually transmitted diseases, including AIDS.

2. Assessing and Responding to Risk

Decisions you make in the field have direct bearing on your safety and that of others. The risks inherent in covering war, political unrest, and crime can never be eliminated, although careful planning and risk assessment can mitigate the dangers.

Be realistic about your physical and emotional limitations. It might be useful to consider in advance all the individuals who would be affected if you were, say, disabled or killed. Consider as well the emotional toll of continuing to report stressful stories one after another. At some point, one more crime victim, one more corpse, one more grieving family may be too much. A decision not to report a story should be seen as a sign of maturity, not as a source of shame or stigma.

News managers should regard the safety of field journalists as the primary consideration in making an assignment. They should not penalize a journalist for turning down an assignment based on the potential risk. News organizations should recognize their responsibilities to support all field journalists, whether they are staff members or stringers. Editors need to be frank about the specific support their organization is willing to provide, including health or life insurance or emotional counseling. Matters left unresolved before a journalist begins a story can lead to stressful complications later.

Security Assessment

Always prepare a security assessment in advance of a potentially dangerous assignment. The plan should identify contact people and the time and means of communication; describe all known hazards, including the history of problems in the reporting area; and outline contingency plans that address the perceived risks. Diverse sources should be consulted, including journalists with experience in the location or topic, diplomatic advisories, reports on press freedom and human rights, and academic research. Editors working with staffers or freelancers should have substantial input into the assessment, take the initiative in raising security questions, and receive a copy of the assessment. An independent journalist working without a relationship with a news organization must be especially rigorous in compiling a security assessment, consulting with peers, researching the risks, and arranging a contact network. An example of a security assessment form is available for review in Appendix G.

Risks should be reassessed on a frequent basis as conditions change. "Always, constantly, constantly, every minute, weigh the benefits against the risks. And as soon as you come to the point where you feel uncomfortable with that equation, get out, go, leave. It's not worth it," Terry Anderson, the former Associated Press Middle East correspondent who was held hostage in Beirut for nearly seven years, wrote in CPJ's first journalist security guide, published in March 1993. "There is no story worth getting killed for."

Risks to be identified may include:

- Battlefield hazards such as crossfire, landmines, cluster bombs, booby traps, and artillery and air strikes;
- terrorist bombings;
- abduction for ransom or political gain;
- dangers posed by crowds, including the possibility of sexual assault, theft, tear gas attack, or violence;
- traffic hazards (the leading cause of unnatural deaths worldwide);
- border crossings and other interactions with potentially hostile or undisciplined armed groups;
- physical surveillance leading to abduction or identification of sources;

- electronic surveillance and interception of information or sources;
- potential trustworthiness and loyalties of sources, drivers, fixers, witnesses, and others;
- common crime, including the types of incidents;
- natural hazards, such as hurricanes and floods;
- and health risks ranging from water-borne diseases to AIDS.

(These contingencies and more are addressed in detail in subsequent chapters of this guide.)

The risk assessment must also consider the possibility that any circumstance—from a tense political situation to a natural disaster—can escalate in severity. The assessment should include information on where to stay and where to seek refuge if necessary; where and how to get updated information inside the country; whether equipment such as a weather-band or shortwave radio is needed; whom to contact in the country, from local human rights groups to foreign embassies, for emergency information; travel plans and methods within the country; and multiple entry and exit routes.

In the assessment, outline how you intend to communicate with editors, colleagues, and loved ones outside the area of risk. A journalist should be in regular contact with an editor, colleague, family member, or other reliable person. You and the contact people should decide in advance how frequently you wish to communicate, by what means, and at what prescribed time, and whether you need to take precautions to avoid having your communications intercepted. Most important, you and the contact person must decide in advance at exactly what point a failure to check in is considered an emergency and whom to call for a comprehensive response in locating you and securing your exit or release. The response often entails systematically reaching out to colleagues and friends who can assess the situation, to authorities who can investigate, and to the diplomatic community to provide potential support and leverage.

The assessment should address the communications infrastructure in the reporting area, identifying any contingency equipment you may need. Are electricity, Internet access, and mobile and landline phone service available? Are they likely to remain so? Is a generator or a car battery with a DC adaptor needed to power one's computer? Should a satellite phone be used? Basic needs such as nourishment and medical care must be addressed as well. Are food and water readily available? Is a hospital, clinic, or physician available? Is a medical kit needed, and what should it include?

Any risk assessment should consider your desired profile. Do you want to travel in a vehicle marked "Press" or "TV," or would it be better to blend in with other civilians? Should you avoid working alone and instead team up with others? If you travel with others, choose your companions carefully. You may not wish to travel, for example, with someone who has a very different tolerance for risk.

Sources and Information

Protecting sources is a cornerstone of journalism. This is especially important when covering topics such as violent crime, national security, and armed conflict, in which sources could be put at legal or physical risk. Freelance journalists, in particular, need to know that this burden rests primarily with them. No journalist should offer a promise of confidentiality until weighing the possible consequences; if a journalist or media organization does promise confidentiality, the commitment carries an important ethical obligation.

Most news organizations have established rules for the use of confidential sources. In a number of instances, news organizations require that journalists in the field share the identity of a confidential source with their editors. Journalists in the field must know these rules before making promises to potential confidential sources. In the United States and many other nations, civil and criminal courts have the

authority to issue subpoenas demanding that either media outlets or individual journalists reveal the identities of confidential sources. The choice can then be as stark as either disclosure or fines and jail. Media organizations that have received separate subpoenas will make their own decisions on how to respond. *Time* magazine, facing the prospect of daily fines and the jailing of a reporter, decided in 2005 that it would comply with a court order to turn over a reporter's emails and notebooks concerning the leak of a CIA agent's identity, even though it disagreed with the court's position.

Media companies have the legal right to turn over to courts a journalist's notebooks if they are, according to contract or protocol, the property of the media organization. If a journalist is a freelance employee, the media organization may have less authority to demand that a journalist identify a source or turn over journalistic material to comply with a court subpoena.

In some nations, local journalists covering organized crime, national security, or armed conflict are especially vulnerable to imprisonment, torture, coercion, or attack related to the use of confidential information. In 2010, CPJ documented numerous instances throughout Africa in which government officials jailed, threatened, or harassed journalists who made use of confidential documents. In Cameroon, for example, authorities jailed four journalists who came into possession of a purported government memo that raised questions of fiscal impropriety. One of those journalists was tortured; a second died in prison. It's important to understand that your ethical responsibility could be severely tested in conflict zones by coercive actors who may resort to threats or force.

Journalists should study and use source protection methods in their communications and records. Consider when and how to contact sources, whether to call them on a landline or cell phone, whether to visit them in their office or home, and whether to use open or secure email or chat message. Consider using simple code or pseudonyms to hide a source's identity in written or electronic files. Physically secure written files, and secure electronic files through encryption and other methods described in Chapter 3 Technology Security.

In your communications, protect your sources. Consider whether to call them on a landline or cell, to use open or secure email, and to visit them at home or the office.

The identity of a source could still be vulnerable to disclosure under coercion. Thus, many journalists in conflict areas avoid writing down or even learning the full or real names of sources they do not plan to quote on the record.

Laws on privacy, libel, and slander vary within and between nations, as do statutes governing the recording of phone calls, meetings, and public events, notes the Citizen Media Law Project at Harvard University's Berkman Center for Internet & Society. In many nations, local press freedom groups can provide basic details of privacy and defamation laws, along with the practices of authorities in applying those laws. (Many of these organizations are listed in Appendix E Journalism Organizations; a comprehensive list of press freedom groups worldwide is available through the International Freedom of Expression Exchange.) Being a journalist does not give one the right to steal, burglarize, or otherwise violate common laws in order to obtain information.

Security and Arms

Most journalists and security experts recommend that you not carry firearms or other gear associated with combatants when covering armed conflict. Doing so can undermine your status as an observer and, by extension, the status of all other journalists working in the conflict area. In conflict zones such as Somalia in the early 1990s, and Iraq and Afghanistan in the 2000s, media outlets hired both armed and unarmed security personnel to protect journalists in the field. While the presence of security guards hindered

journalists' observer status, many media organizations found they had little choice but to rely on private personnel to protect staff in uncontrolled situations.

Carrying a firearm on other assignments is also strongly discouraged. In nations where law enforcement is weak, some journalists under threat have chosen to carry a weapon. In making such a choice, you should consider that carrying a firearm can have fatal consequences and undercut your status as an observer.

Sexual Violence

The sexual assault of CBS correspondent and CPJ board member Lara Logan while covering political unrest in Cairo in February 2011 has highlighted this important security issue for journalists. In a 2011 report, CPJ interviewed more than four dozen other journalists who said that they, too, had been victimized on past assignments. Most reported victims were women, although some were men. Journalists have reported assaults that range from groping to rape by multiple attackers.

Being aware of one's environment and understanding how one may be perceived in that setting are important in deterring sexual aggression. The International News Safety Institute, a consortium of news organizations and journalist groups that includes CPJ, and Judith Matloff, a veteran foreign correspondent and journalism professor, have each published checklists aimed at minimizing the risk of sexual aggression in the field. A number of their suggestions are incorporated here, along with the advice of numerous journalists and security experts consulted by CPJ.

Journalists should dress conservatively and in accord with local custom; wearing head scarves in some regions, for example, may be advisable for female journalists. Female journalists should consider wearing a wedding band, or a ring that looks like one, regardless of whether they are married. They should avoid wearing necklaces, ponytails, or anything that can be grabbed. Numerous experts advise female journalists to avoid tight-fitting T-shirts and jeans, makeup, and jewelry in order to avoid unwanted attention. Consider wearing heavy belts and boots that are hard to remove, along with loose-fitting clothing. Carrying equipment discreetly, in nondescript bags, can also avoid unwanted attention. Consider carrying pepper spray or even spray deodorant to deter aggressors.

Journalists should travel and work with colleagues or support staff for a wide range of security reasons. Local fixers, translators, and drivers can provide an important measure of protection for international journalists, particularly while traveling or on assignments involving crowds or chaotic conditions. Support staff can monitor the overall security of a situation and identify potential risks while the journalist is working. It is very important to be diligent in vetting local support staff and to seek recommendations from colleagues. Some journalists have reported instances of sexual aggression by support staff.

Experts suggest that journalists appear familiar and confident in their setting but avoid striking up conversation or making eye contact with strangers. Female journalists should be aware that gestures of familiarity, such as hugging or smiling, even with colleagues, can be misinterpreted and raise the risk of unwanted attention. Don't mingle in a predominantly male crowd, experts say; stay close to the edges and have an escape path in mind. Choose a hotel with security guards whenever possible, and avoid rooms with accessible windows or balconies. Use all locks on hotel doors, and consider using your own lock and doorknob alarm as well. The International News Safety Institute suggests journalists have a cover story prepared ("I'm waiting for my colleague to arrive," for example) if they are getting unwanted attention.

In general, try to avoid situations that raise risk, experts say. Those include staying in remote areas without a trusted companion; getting in unofficial taxis or taxis with multiple strangers; using elevators or corridors where you would be alone with strangers; eating out alone, unless you are sure of the setting; and spending long periods alone with male sources or support staff. Keeping in regular contact with your newsroom

editors and compiling and disseminating contact information for yourself and support staff is always good practice for a broad range of security reasons. Carry a mobile phone with security numbers, including your professional contacts and local emergency contacts. Be discreet in giving out any personal information.

If a journalist perceives imminent sexual assault, she or he should do or say something to change the dynamic, experts recommend. Screaming or yelling for help if people are within earshot is one option. Shouting out something unexpected such as, "Is that a police car?" could be another. Dropping, breaking, or throwing something that might startle the assailant could be a third. Urinating or soiling oneself could be a further step.

The Humanitarian Practice Network, a forum for workers and policy-makers engaged in humanitarian work, has produced a safety guide that includes some advice pertinent to journalists. The HPN, part of the U.K.-based Overseas Development Institute, suggests that individuals have some knowledge of the local language and use phrases and sentences if threatened with assault as a way to alter the situation.

Protecting and preserving one's life in the face of sexual assault is the overarching guideline, HPN and other experts say. Some security experts recommend that journalists learn self-defense skills to fight off attackers. There is a countervailing belief among some experts that fighting off an assailant could increase the risk of fatal violence. Factors to consider are the number of assailants, whether weapons are involved, and whether the setting is public or private. Some experts suggest fighting back if an assailant seeks to take an individual from the scene of an initial attack to another location.

Sexual abuse can also occur when a journalist is being detained by a government or being held captive by irregular forces. Developing a relationship with one's guards or captors may reduce the risk of all forms of assault, but journalists should be aware that abuse can occur and they may have few options. Protecting one's life is the primary goal.

News organizations can include guidelines on the risk of sexual assault in their security manuals as a way to increase attention and encourage discussion. While documentation specific to sexual assaults against journalists is limited, organizations can identify countries where the overall risk is greater, such as conflict zones where rape is used as a weapon, countries where the rule of law is weak, and settings where sexual aggression is common. Organizations can set clear policies on how to respond to sexual assaults that address the journalist's needs for medical, legal, and psychological support. Such reports should be treated as a medical urgency and as an overall security threat that affects other journalists. Managers addressing sexual assault cases must be sensitive to the journalist's wishes in terms of confidentiality, and mindful of the emotional impact of such an experience. The journalist's immediate needs include empathy, respect, and security.

Journalists who have been assaulted may consider reporting the attack as a means of obtaining proper medical support and to document the security risk for others. Some journalists told CPJ they were reluctant to report sexual abuse because they did not want to be perceived as being vulnerable while on dangerous assignments. Editorial managers should create a climate in which journalists can report assaults without fear of losing future assignments and with confidence they will receive support and assistance.

The Committee to Protect Journalists is committed to documenting instances of sexual assault. Journalists are encouraged to contact CPJ to report such cases; information about a case is made public or kept confidential at the discretion of the journalist.

Captive Situations

The kidnapping of journalists for ransom or political gain has occurred frequently over CPJ's 31-year

history. Numerous cases have been reported in nations such as Colombia, the Philippines, Russia, Iraq, Pakistan, Afghanistan, Mexico, and Somalia, according to CPJ research. In Afghanistan alone, at least 20 journalists and media workers were kidnapped by insurgent or criminal groups from 2007 through 2011, CPJ research shows. At least two of them died.

The best antidote is precaution. Travel in teams in dangerous areas, making sure that editors and perhaps a trusted local individual know your plans. Prepare a contingency plan with contact information for people and groups to call in the event you go missing. In advance discussions with editors and trusted contacts, decide the length of time at which they should interpret your being out of touch as an emergency.

If you're taken captive, one of the first things a kidnapper may do is research your name on the Internet. Everything about you online will be seen by your abductors: where you have worked, the stories you have reported, your education, your personal and professional associations, and possibly the value of your home and your family's net worth. You may want to limit the personal details or political leanings you reveal in your online profile. Be prepared to answer tough questions about your family, finances, reporting, and political associations.

Hostile environment training includes coping mechanisms and survival techniques. Among them is developing a relationship with your captors, a step that could reduce the chance guards will do you harm. Cooperate with guards but do not attempt to appease them. As best as you can, explain your role as a non-combatant observer and that your job includes telling all sides of a story. Pace yourself throughout the ordeal and, as much as possible, maintain emotional equanimity. Promises of release may not be forthcoming; threats of execution could be made.

Journalists captured as a group should act in a way that leads guards to keep them together rather than separate them. This could involve cooperating with guards' orders and persuading captors that it would be less work to keep the group together. Journalists should offer each other moral and emotional support during captivity. Maintaining cohesion could help each captive's chances of successful release.

Opportunities for escape may arise during captivity, but many veteran journalists and security experts warn that the chance of success is exceedingly slim and must be balanced against the potentially fatal consequences of failure. In 2009, in Pakistan, *New York Times* reporter David Rohde and local reporter Tahir Ludin did escape from Taliban captors who had held them for seven months. After weighing the risks, the two men concluded their captors were not seriously negotiating for their release and chose "to try to make a run for it," Rohde later wrote. Some captors, however, may have a cohesive chain of command in which you may eventually be allowed to make the case that you are a reporter who deserves to be released.

During a captive situation, editors and family members are encouraged to work together. As soon as the captive situation is confirmed, they should get in touch with government representatives in the hostage nation, along with authorities in the news organization's home country and that of each of the journalists. They should seek out advice from diplomats experienced in the theater, private security experts, and press groups such as CPJ. The International News Safety Institute has a Global Hostage Crisis Help Centre that can recommend hostage experts. The Dart Center for Journalism & Trauma can advise affected parties on how to obtain counseling for family members and others. (See Chapter 10 Stress Reactions.) Whether to meet captors' demands is a difficult question. Patience and emotions will be tested as the ordeal goes on.

Editors and relatives should make every effort to present a cohesive front, designating a person as a conduit to authorities and as a public spokesperson. Authorities may well make decisions independent of (and contrary to) the wishes of family and colleagues, but establishing a clear and consistent message to authorities and the press improves the chance of effectively influencing decision-making.

Most governments have stated policies of not paying ransom demands, although in practice a number of

governments, including those of France and Japan, have reportedly helped pay ransom in exchange for the release of captive journalists. Editors and family members may or may not be able to influence decisions on the deployment of a government rescue operation. The British government spoke to editors, but then made its own decision to order a rescue operation for a British-Irish national working for *The New York Times* in Afghanistan in 2009. The *Times* reporter, Stephen Farrell, was rescued, but an Afghan journalist who was working as Farrell's fixer, Sultan Mohammed Munadi, was killed.

Kidnappers may try to coerce a news organization into running propaganda or one-sided coverage of their viewpoint. In the 1990s, leftist guerrillas and rightist paramilitaries in Colombia often kidnapped journalists to coerce news outlets into coverage of their political grievances. In 2006, Brazil's TV Globo aired a homemade video detailing perceived deficiencies in prison conditions after a local criminal gang kidnapped a station reporter and technician. The two journalists were later freed. Editors need to recognize that acceding to kidnappers' demands could invite future attempts at coerced coverage.

In another form of coercion, captors may demand that a journalist make propagandistic statements on video. Some journalists have agreed, calculating that it may increase their chances of safe release. Others have resisted in the belief that displaying independence may give them some leverage with their captors. The decision depends entirely on the circumstances and the individuals involved.

Responding to Threats

Threats are not only a tactic designed to intimidate critical journalists; they are often followed by actual attacks. Thirty-five percent of journalists murdered in the last two decades were threatened beforehand, according to CPJ research. You must take threats seriously, paying particular heed to those that suggest physical violence.

How to respond depends in part on local circumstances. Reporting a threat to police is usually good practice in places with strong rule of law and trustworthy law enforcement. In nations where law enforcement is corrupt, reporting a threat may be futile or even counterproductive. Those factors should be weighed carefully.

Do report threats to your editors and trusted colleagues. Be sure they know details of the threat, including its nature and how and when it was delivered. Some journalists have publicized threats through their news outlets or their own blogs. And do report threats to local and international press freedom groups such as the Committee to Protect Journalists. CPJ will publicize a threat or keep it confidential at your discretion. Many journalists have told CPJ that publicizing threats helped protect them from harm.

Journalists under threat can also consider a temporary or permanent change in beat. Editors should consult closely with a journalist facing threats and expedite a change in assignment if requested for safety reasons. Some threatened journalists have found that time away from a sensitive beat allowed a hostile situation to lessen in intensity.

In severe circumstances, journalists may consider relocation either within or outside their country. Threatened journalists should consult with their loved ones to assess potential relocation, and seek help from their news organization and professional groups if relocation is deemed necessary. The Colombian investigative editor Daniel Coronell and his family, for example, relocated to the United States for two years beginning in 2005 after he faced a series of threats, including the delivery of a funeral wreath to his home. Coronell resumed his investigative work when he returned to Colombia, and although threats continued, they came at a slower pace and with lesser intensity. CPJ can provide advice to journalists under threat and, in some cases, direct support such as relocation assistance.

3. Technology Security

In the course of reporting, you use technical tools all the time—a laptop on which to write articles and do online research; mobile devices to make calls and send email; cameras for photography; and recorders for interviews. These may be combined into one device which does many tasks. These devices contain a wealth of information necessary to your reporting.

This section is about secure use of these tools. This means protecting your information: ensuring you do not lose materials crucial to a story, and keeping confidential information private. It also means ensuring that these tools work when you need them—even if someone is trying to interrupt their use.

If you are working in the field, digital files might be the most precious items you carry. Losing notes or materials like photos and videos can derail a story. Letting your contacts list or itinerary fall into the wrong hands can put you or a source at risk. Allowing your tools to be confiscated, destroyed, or interrupted can prevent you from pursuing a story at all.

Digital attacks on journalists continue to increase in both quantity and sophistication. In China, foreign correspondents have seen their personal computers infected with surveillance software that was concealed as attachments to carefully fabricated emails. Authorities in countries from Ethiopia to Colombia have accessed reporters' telephone, email, and text conversations. Government players are not the only ones who use digital surveillance and sabotage; large criminal organizations increasingly exploit high-tech opportunities. Opportunistic or "patriotic" computer criminals also target journalists working with valuable or controversial data.

In the end, good information security is rarely about fending off sophisticated attacks and Hollywood-style hackers. It's about understanding what you have to protect and the motives and capabilities of those who might want to disrupt your work, then developing consistent habits based on those assessments.

Planning for safety

What to protect

What things do you want to protect and what do you want to protect them from? The things you want to protect are assets; things that could go wrong are risks. For now, don't worry about who might attack you or how they might do it—instead, think only about assets and risks.

There are usually three risks you might think about:

1. Loss. When your hard drive dies, your phone gets smashed, or you lose your camera's data card.
2. Disclosure. Someone learns something that you would prefer to keep private.
3. Interruption. Your network connection stops working, you can't send an email, or your phone doesn't have a signal.

When considering what you want to protect, imagine what's important to you to get your job done or to an adversary who wishes to disrupt your work. This may not be obvious, so it's worth careful reflection. Even if your work is largely transparent, there are still tools you rely on and material that should remain private.

Consider whether the information that sources have given you could put them in danger if disclosed. Some things may seem innocuous in one context, but present a danger in another. Access to your Israeli contact

information when covering a story in an Arab country (or vice versa) can cause problems for all concerned. Even personal and travel-related information you've previously shared online could trip you up in another context.

Some assets are clear. You probably don't want to lose or disclose the files on your computer and mobile devices, and temporary interruptions would disrupt your work. Some assets are more ephemeral. You (and your sources) would probably prefer that your current location and location history not be disclosed. Likewise regarding a list of the people you communicate with and when, or a list of the sites you visit online while researching a story.

You also rely on technical resources to work effectively. How much would your work be disrupted by interruption to your email or to your ability to make phone calls or research on the Web, or even interruption of your network access entirely? It's worth making note of online services you rely on. Do you work on your notes, email, documents, and so on in a Web browser; how disruptive would an interruption of your access to those services be?

If you find it hard to keep track of all the tools, data, and resources you rely on, it may be useful to keep a journal of what you use over the course of a week.

Understanding the Threat

Now that you know what you might want to keep safe, it is worth putting a name or face to the ominous "they" who might want to compromise these assets.

Some threats are benign or environmental. Laptop hard drives sometimes die; without regular backup, that data is lost. Some threats come from a malicious actor—a government agent who copies your hard drive at the border, or a private detective who follows you around. It's important to consider both types of threats, but the effects are the same: the actor threatens the integrity of one of your assets.

When trying to enumerate malicious actors, it's important to consider their motivations. Who might want to disrupt your reporting or identify your source? Perhaps they wish to view non-public information you possess. Perhaps a threat isn't interested in you specifically. If a country censors the local Internet connection, that may interrupt your ability to communicate and research while you're there.

It's easy to think of an Orwellian surveillance state analyzing every digital breadcrumb. However, this is not the only threat you may face. Other actors may present much more urgent threats. You may be at greater risk from a specific part of an administration or a specific person such as a local police chief or corrupt government official. Do they have access to sophisticated surveillance equipment or are they more likely to have someone kick down your door and steal your laptop?

Also consider the possibility of attack by supporters or sympathizers of those who dislike your reporting. In many cases documented by CPJ, attacks are not directly perpetrated by governments or political parties, but by unconnected, "patriotic" troublemakers who perceive opposition or foreign media as legitimate targets.

Making a Plan

Technology security has some distinct foibles. It can be very hard to know when someone has rifled through your data. If someone steals your wallet or ransacks your hotel room, you are likely to notice. If someone makes a copy of your laptop's hard drive while you are out of your hotel room having dinner, you may never notice. The harm can be impossible to undo. Once your data has been lost, or someone has learned a secret, you can't get it back.

This is exacerbated by the fact that technology systems are complex, made up of many different parts that are always changing. Not even the smartest and most meticulous technologists can know the workings of every program on their computers, let alone how they interact with other software on the network and where those interactions could be exploited. Even if you're not an expert on bulletproof vests, you can understand basically what they do and how. Computer security is much harder to comprehend intuitively. Real-world analogies rarely paint a full picture.

This means that your emphasis should be on simplicity. A small number of easy-to-use tools, techniques, and habits are always safest. Complex systems are hard to understand; involved procedures can fall by the wayside when tasks are urgent. Sometimes, effort spent fortifying one activity is unnecessary when there's a simple weak link elsewhere.

Focus on the people who are most likely to wish to interrupt your work, the lengths they may go to do so, and how proficient and effective they are likely to be. Use that knowledge to plan how to protect your work.

Once you have thought about who might wish to disrupt your work, what they might do, and how well they might do it, you can start planning the technical measures you will use to confound their plans. The rest of these suggestions are broad guidance about information security. Detailed technical advice can become out of date quickly, especially if a new vulnerability is discovered in a piece of technology.

Protecting Communications

Communication is the bread and butter of most journalism. When you talk to someone—whether by email, text message, instant chat, telephone, or any of the many other communications services available—you may wish to keep private various details of your conversation. In general, the two most important facts about a conversation are *who* you are talking to and *what* you are saying.

The tools you use may keep track of (and potentially reveal) other details too. Use of a mobile telephone reveals your location to the telephone company and anyone the phone company chooses to reveal this to—potentially including the police or government. Using a communication tool that stores a list of contacts may reveal that list to the service provider (and anyone the provider tells). Information about past conversations (like a phone bill with call times and lengths) can reveal information about communication habits and routines and this may be enough to suspect who was talking or reveal some of what was said, especially when combined with other information.

In cases where it is very important that the identity of a source remain secret, you may have to take somewhat inconvenient steps to avoid leaving a trail that leads back to him or her.

In cases where it is very important that the identity of a source remain secret, you may have to take somewhat inconvenient steps to avoid leaving a trail that leads back to him or her.

Even when you have a good idea about your adversaries' interests and capabilities, it may be difficult to imagine how they might piece together lots of little pieces of information about your communications to reveal a larger picture. In cases where it is very important that the identity of a source remain secret, you may have to take somewhat inconvenient steps to avoid leaving a trail that leads back to him or her.

It may once have been the case that these capabilities were only available to the very sophisticated or those with deep pockets. Some capabilities are still reserved for the government or police, but many of these tools can be bought cheaply. Professional investigators have access to a powerful menu of attacks and are not always ethical in their use.

Mobile devices

Phone-tapping is one of the most familiar forms of surveillance practiced against journalists. Whenever you make a phone call, the phone company has the ability both to see whom you are calling and to listen to the content of your call. Text messages are even easier to intercept because they are small and easy to store without expensive recording equipment. CPJ has documented cases in which authorities have presented journalists with logs of text messages as an implied threat or as evidence of alleged anti-state activity.

You can mitigate some of this threat by using tools like Signal and Redphone to encrypt calls and TextSecure for text messages. It is normally prudent to assume that these tools hide only the content of conversations—not the participants, timing, your various locations, or other details.

Phones and SIM cards have unique serial numbers and both numbers are reported to the phone company whenever the phone is on. Simply moving your SIM to another phone or keeping the same phone and changing SIMs won't conceal much from a phone company since they can just compare these two serial numbers.

When you carry a mobile phone, it constantly connects to cell towers around you so that incoming calls can be routed to the right tower and reach you. This also leaves a trail of which towers you have been near, providing the phone company with a good record of where your phone has been. Removing the battery prevents this, but be aware of the trail potentially left by several people removing the batteries from their phones just before converging on a meeting. It may be more sensible to remove the battery before departure or to leave the device behind.

You can mitigate some risk by purchasing a prepaid mobile phone anonymously with cash and disposing of it after use. This is sometimes called a "burner" phone. If identification is required to purchase a phone, consider buying a second-hand phone from an existing user. The approach is not foolproof—if you carry around both a burner and a regular phone, or your burner is at your home at night and your office during the day, a careful analysis of phone-company records may reveal that the telephone is yours. Unless your contacts are also using burner phones and careful precautions, your first calls to others' existing numbers may reveal your new number. Some sophisticated analysis may be able to use call records to identify networks—groups of phones that call and message each other in the same way—and this may give you away even if everyone in the group switches burner phones at the same time.

In addition to tracking devices, mobile phones can be used as remote listening devices. Turning a phone off doesn't guarantee that it can't be used this way: for most devices, "off" is really just a very low-power mode. The only way to be sure that a phone isn't eavesdropping is to remove the battery or leave it behind.

Internet connections

If you are using the wireless connection at a public place, others on the same network may be able to snoop on your Web browsing, email, instant messages, what you type into websites, and anything else you do online. If you are at a hotel or similar location, that institution also has the opportunity to snoop on these things. If you are using a private Internet connection (and have secured your wireless network), only your Internet service provider (ISP) knows what you are doing online.

You can hide this information from snoops and ISPs by using a virtual private network (VPN). A VPN encrypts and sends all Internet data to and from your computer via a dedicated computer elsewhere on the Internet, called a VPN server. When configured correctly, a VPN will secure all of your communications from local interception. If you are employed by a media organization, your employer may well use a VPN to allow remote users access to the company's internal networks. Alternatively, some commercial services allow individuals to rent access to a VPN server on a monthly basis.

From the perspective of the rest of the Internet, you appear to be accessing the Web and other Internet services from your VPN server, not your actual location. That means it can hide your current whereabouts and bypass local censorship systems. VPNs do not encrypt every stage of your data's travels online. Because your final destination may not understand encrypted data, your information and requests emerge from the VPN server in an unencrypted state. The operators of your VPN server, and intermediaries between the operator and the sites and services you visit, still have the ability to monitor your communications. If you're defending yourself against a local adversary, such as the government, the VPN server you select should be in another jurisdiction.

An even more sophisticated alternative to a commercial VPN is the free anonymizing service Tor. Tor protects network traffic by encrypting and shuffling the data through several volunteer-run servers before it finally exits onto the wider Internet. The easiest way to use Tor is with the Tor Browser—an anonymous browser pre-configured to use Tor. You can also use Tails—a live operating system that sends all network traffic over Tor.

Many responsible websites protect you by encrypting your communications with them. You can tell whether your connection to a website is encrypted by looking at the address bar in your browser. If the address starts with "https://" rather than "http://" and there is a lock icon next to it, then your connection is encrypted. A snooper will know which site you're visiting but not which page on the site you are visiting or any information you enter. This is especially important for any website you log in to—otherwise an eavesdropper could snoop on your password and log in as you.

A browser add-on called HTTPs-everywhere helps ensure that you use a secure connection wherever possible, but some sites and services don't offer a secure connection. Whenever you browse a site that isn't protected with HTTPs, there's the possibility that an attacker might take the opportunity to inject malware into the page and infect your computer. If you are concerned about this, HTTPs-everywhere has an option to completely disable insecure HTTP—but beware that there are some sites you simply won't be able to read if you do this.

Email and instant messages

Software can encrypt your messages, scrambling them so that only the intended recipient has the ability to decode them. You can choose encryption software designed for specific uses (such as email and instant messaging) and you can adopt methods that encrypt all of your Internet traffic.

The gold standards for email encryption are GNU Privacy Guard (GPG), which is free, open-source software, and Symantec's Pretty Good Privacy (PGP). They are compatible with each other. Unfortunately, GPG/PGP have a steep learning curve and are difficult to use. If used correctly by all correspondents, they provide a high level of security for the content of your messages, but do not hide who you are or who you are talking to. Many email programs such as Outlook, Thunderbird, and Apple Mail have additional software or add-ons that support GPG/PGP; human rights and media organizations will sometimes offer instructional classes in using them.

If you are working under a repressive regime known to have access to communication providers, consider using an email provider that is based in another country without economic or political ties to your location. You may wish to encourage correspondents to use an email account on the same service when talking to you. There is little point in carefully encrypting your side of a conversation if your correspondent is reading the email insecurely.

When one email service sends a message to another service, there's an opportunity for interception. Some services use encryption when sending messages onward; others don't. If sender and recipient are on the

same service, this step is avoided. You can learn more about which services support server-to-server encryption in Google's email transparency report. You can also check a particular service at https://starttls.info. You may wish to check whether your recipient's email provider supports server-to-server encryption before emailing that person. If not, it may be valuable to consider using GPG/PGP or using a different tool to communicate.

Although server-to-server encryption can protect messages passing over the Internet, attackers may try to obtain your archive of previous messages. They might do this by installing software on your computer or that of your correspondents, or by breaking into your email provider. This makes it important to protect your own computer and the passwords of any email services you use. (See sections below on Defending Your Data and Protecting External Data.)

Instant messaging tools like Google Hangout, Skype, Facebook Messenger, Kik, WhatsApp, Viber, and so on can be as vulnerable to interception as email. Many chat programs use encryption to ensure that only the participants and the service provider can read messages or see who is communicating. Some services, such as CryptoCat, use an even safer approach in which only a chat's participants can read messages, but this is less common. Some service providers are willing to hand over chat logs when asked; others are not. Instant message services and their practices are constantly changing, so it's important to be aware of your provider's current practices. The messaging equivalent to PGP and GPG is Off-The-Record (OTR) Messaging, which can be used in combination with most instant messaging software. As with PGP/GPG, OTR requires that both sides of a conversation have the technical skill to install and learn new applications.

Tradecraft

There are many different ways to surveil and intercept electronic communication. When personal safety depends on the security of communications or the anonymity of a source, it may be sensible to dispense with them altogether.

Consider arranging codes "out of band"—that is, not via a channel suspected to be insecure. If you can meet someone in person or have a trustworthy intermediary, you can take that opportunity to arrange certain pre-agreed messages that you can then use online if needed.

Defending Your Data

Smartphones, tablets, and laptops can hold vast amounts of data and access to many valuable tools. On the other hand, losing or destroying your phone or computers may mean that you lose a large amount of important information. This also makes phones and computers attractive targets for anyone who wants access to all your work and correspondence, or for someone who wants to disrupt your work. An adversary might simply steal your device or attempt to destroy it, or they may try to infect it with malicious software that provides remote access to your files and all your communications. It is therefore important to protect information in two ways: ensure that it cannot be destroyed, and ensure that it cannot be stolen.

The simplest way to protect materials from destruction or disclosure is to keep them out of harm's way. If you are planning to travel to a riskier environment, consider leaving sensitive information behind and using a separate laptop or simple phone that carries minimal information. It may also be valuable to change passwords to email or social media accounts to something that you cannot remember, and leaving these with a trusted friend or colleague. This will mean that you cannot give up those passwords even if asked. This is not always feasible, but when appropriate, keeping materials and passwords away from a risky environment is one of the safest tools you have.

If you expect situations in which your computer may be seized or inspected—a border crossing or a checkpoint—you may wish to remove confidential information. This is not simply a matter of deleting the file or dragging it to the trash. It is often relatively simple to recover files that have been deleted via a computer's usual methods. If you want your data to be truly unrecoverable, you need to use additional software specifically designed to securely remove data. Either use your computer's "secure delete" feature, if it has one, or download in advance third-party software for this purpose.

Confidentiality and encryption

You should always encrypt your computer. Windows' BitLocker, MacOS FileVault, or the independent TrueCrypt allow you to secure your entire laptop or user account, which is much safer than just trying to protect individual files. Android and iOS devices also have encryption features that can be turned on in the settings. It is important to pick a strong passphrase for encryption. The only thing keeping your data safe is the passphrase, and someone who confiscates your device can use a computer to very quickly guess many possible passphrases.

Lock your computer's screen and use a PIN (not just a swipe pattern) on your mobile device. Although neither of these will stop a determined attacker, they protect you from casual snooping. Make sure to switch off or hibernate (not just suspend) your computer when you leave your work area or you think you may be searched, such as when crossing a border, as this will force an attacker to contend with encryption that is very difficult to attack—rather than a locked screen, which is easier.

It may be useful to keep your confidential information on a USB flash drive, which is easier to carry, hide, and protect. You should, of course, make sure to encrypt removable drives too. Compared with a laptop or even a smartphone, it is easier to carry a flash drive hidden on your person. Additionally, you may want to back up vital documents from your laptop onto a flash drive so that you have a copy if you lose control of your computer.

Even in a newsroom, be alert to people peering over your shoulder when you sign in or read your messages. If you have a particularly dedicated adversary, a hidden camera may serve the same function. Never use public computers in cybercafés or hotels for confidential conversations or to access your USB drive. And don't enter passwords into public computers.

Malware

Smartphones are a challenge to protect because of their complexity and the rich access that applications, or apps, can get to all sorts of information on the device. Many apps are funded by advertising which depend on gathering information about their users—a lot like surveillance. You can go some way toward protecting yourself by using different devices for work and for personal purposes and only installing a bare minimum of apps on your work device. Never root or jailbreak your device, bypassing the manufacturer's software restrictions, and do not enable installation of software from outside the bundled app store or marketplace.

Don't click on attachments or links sent by email, even from colleagues, without considering the possibility that the mail may be a customized fake using personal details that an attacker gleaned online.

Governments, criminals, and private actors routinely use targeted delivery of malicious software, or malware, to attack perceived enemies such as independent journalists. Taking advantage of bugs in popular software, malware remotely and invisibly installs itself on computers and can then record your keystrokes, watch your screen, or even upload local files to the attacker. It can be delivered via fake but convincing email attachments and even ordinary-looking websites. Don't click on attachments or links sent by email, even from colleagues, without considering the possibility that the mail may be a customized fake using

personal details that an attacker gleaned online. Use antivirus software on your computer, and keep it up to date; it will be able to detect all but the most sophisticated attacks. If you use Windows, both Microsoft Security Essentials and Avast provide free basic antivirus utilities. If you suspect that your computer might have been infected, most employers and independent technicians will be able to wipe the machine and reinstall your software so the malware is removed. Be sure to make a backup of any data before this process begins, and work with the expert to ensure that the data you copy is not harboring the malware.

Don't click on attachments or links sent by email, even from colleagues, without considering the possibility that the mail may be a customized fake using personal details that an attacker gleaned online.

Backups

Remote backups, in which your local files are regularly copied to a remote server, are generally a good idea. They are another way to protect your information should you lose access to your local machine. Be sure that the data being sent is encrypted along the way, and that access to the backups is controlled. (See section on Protecting External Data.) SpiderOak is a service that will automatically synchronize files securely—and keep an encrypted copy with the service provider. Crashplan is an encrypted backup tool that runs automatically on your computer and uploads backups securely. The most important thing with backups is that they happen automatically, whether you do anything or not. Life can get busy and distracting and it's best for backups to be seamless and not to require your attention, or they won't happen.

Remote Data

Not all the information you keep on your computer or smartphone is kept locally. You may store data "in the cloud" on sites such as Google Documents, on Web mail services such as Gmail or Yahoo, or on hosted social networking services such as Facebook. If you are concerned about access to private information, you should consider the security of external data, too.

Internet companies do hand over private data in response to government demands when they are required by local law or have close economic or political ties to authorities. However, access to cloud-stored data is as often obtained through deceit as through due process. Your attackers may obtain your log-in or password, or otherwise masquerade as you to obtain access. Choose your passwords and security questions carefully to prevent this. Always use an encrypted connection, provided by either the Internet service via "https" or your own software.

Don't simply protect private online data; consider what you're revealing in publicly available online venues. Social networking sites often err on the side of telling everyone everything you tell them. It's worth regularly treating yourself as the target of some investigative journalism. See how much you can dig up on your own movements by searching the Web, and how that public information might be misused by those who wish to interfere with your work.

Choosing a Strong Password

Strong password protection is by far the best general security you can give your data. But choosing an unbeatable password is harder than it sounds. Many people are shocked to discover that their ingenious choice is actually among the most popular passwords. By studying large databases of passwords, attackers can compile vast lists of possible passwords sorted from the most likely to the outright improbable. These lists include tweaks and modifications, like replacing letters with similar-looking numbers or symbols, adding numbers or punctuation to the beginning or end of words, or stringing a few words together.

Software allows attackers to rapidly test them against a password-protected device or service. Traditional password choices quickly succumb to these attacks.

Attackers can obtain your password by threatening you with harm. Consider maintaining an account that contains innocuous information, whose password you can divulge under duress. Consider using a passphrase instead of a password. One way to pick a passphrase is to think of an obscure quotation or saying which others are unlikely to associate with you. You can either use the whole phrase as your password, or abbreviate it as suggested by security expert Bruce Schneier to create a truly random-looking series of symbols. For instance:

- WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
- Wow...doestcst = Wow, does that couch smell terrible.
- Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
- uTVM,TPw55:utvm,tpwstillsecure = Until this very moment, these passwords were still secure.

This approach relies on you to pick a sufficiently obscure phrase and to abbreviate it safely. Another approach is to pick a sequence of words truly at random. You can do this easily using a pair of ordinary dice and the list of words at http://www.diceware.com. Seven or eight words picked this way will create a strong password, but the longer the password, the more likely it is to resist an automated attack. Mentally assembling these words into a humorous story or picture can make such passwords easy to remember.

If you use a lot of passwords, consider a password manager—software that will generate unique passwords and store them securely under a single passphrase. Make sure that single passphrase is a strong one. Be aware of the answers you give for the "security questions" (such as "What is your mother's maiden name?") that websites use to confirm your identity if you do forget your password. Honest answers to many security questions are publicly discoverable facts that a determined adversary can easily find. Instead, give fictional answers that, like your passphrase, no one knows but you. Do not use the same passwords or security question answers for multiple accounts on different websites or services.

Finally, understand that there is always one way that attackers can obtain your password: They can directly threaten you with physical harm. If you fear this may be a possibility, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password. One possibility is to maintain at least one account that contains largely benign information, whose password you can divulge quickly. Software like TrueCrypt offers this as a built-in feature. This approach relies on giving a convincing performance and the account's contents being convincing.

Conclusion

Security is never perfect and always involves trade-offs. Only you can determine the balance between efficiently conducting your work and protecting against attacks. When considering solutions, be honest about your capabilities and don't impose impossible security protocols on yourself. Encrypting your email, securely deleting files, and using long passwords won't help if, realistically, you won't follow those habits in the field. Think instead about fundamental steps that you will actually do. If you are more worried about technical attacks than physical seizure, for example, consider writing notes in a paper notebook instead of a Word document.

If you are facing sophisticated technical attacks, the best approach may be simple and minimal. Only you can judge the pros and cons. It's not a "cybercrime" to keep your long passwords written down on a note in a safe place. At least if somebody steals that, you'll know it's time to change them. Just don't put those passwords on a Post-it note stuck to your office wall.

4. Armed Conflict

Covering armed conflicts poses the most serious threat many journalists ever face. Being physically fit can help you avoid injury. One should also be emotionally prepared, appropriately equipped, properly trained, and adequately insured.

Security Training

Security training courses for journalists have been offered by private firms since the 1990s; traditionally, they have been staffed mainly by former British or American military personnel. Most have taught personal-awareness skills oriented toward combat risks and battlefield hazards, along with emergency first aid. Such training is highly recommended for journalists who cover armed confrontation of any kind. Knowledge and skills are imparted both in the classroom and in complex field simulations that challenge journalists to apply their skills and work together. The training benefits foreign and local journalists alike.

The Europe-based International News Safety Institute has trained pro bono hundreds of local journalists operating in hazardous areas around the world. Besides emerging with multiple sets of skills, the journalists often form bonds with one another. The training provides local journalists living and working in dangerous areas with the opportunity to meet and collaborate on neutral ground in ways that may transcend political, geographic, and other identities. Historically, security training courses have not specialized in addressing non-military contingencies, such as mitigating the risk of sexual assault while on assignment (see Chapter 2 Assessing and Responding to Risk) or lessening the hazards of covering organized crime (see Chapter 5 Organized Crime and Corruption). Since 2011, however, new and existing firms have been developing training modules covering civil scenarios and digital security.

Hostile-environment and emergency-first-aid courses are prerequisites for safe reporting in any situation involving armed engagement, including violent protests and clashes. The courses include exercises in how to react to a kidnapping scenario. Five-day courses are offered in Great Britain and the United States at a cost of US$3,000 or more. Three-day refresher courses, which are recommended periodically, cost at least US$2,000.

The Rory Peck Trust offers a Training Fund for freelancers to help cover the cost of security courses. The fund is available to "bona fide professional freelancers involved in newsgathering or current affairs for a minimum of 18 months." The Paris-based press freedom group Reporters Without Borders offers courses on safety and stress management, as well as international humanitarian law, in collaboration with the French Red Cross. The course is conducted in French and held in the French Alps.

Multilateral agencies led by the United Nations Educational, Scientific, and Cultural Organization, or UNESCO, along with unilateral government agencies such as the Swedish International Development Cooperation Agency and private groups such as the International News Safety Institute, have provided security training for journalists in less developed nations on a periodic basis.

Protective Gear

You should be fully equipped with gear appropriate to the situation. In extreme circumstances, this could involve wearing hazmat suits, carrying detectors, or ingesting oral tablets to block or act against possible biological, chemical, or nuclear agents. In combat zones, it would involve wearing body armor rated to withstand shrapnel and high-powered bullets. In cases of street clashes or violence, it could mean wearing an inconspicuous anti-stab vest.

Journalists requiring body armor should choose a vest according to the expected threat. The U.S. National Institute of Justice has developed a six-tier rating system used by most manufacturers around the world. If you are covering armed conflict, you should choose a vest rated to stop high-velocity bullets fired by military rifles. Be aware, however, that no vest is bulletproof. One may still be severely injured or die from the trauma of blunt impact, even if the body armor does stop the projectile. Consider gender-specific designs and whether you require options such as side or groin protectors.

Helmets are also recommended for journalists covering war zones. Recognize, however, that even a top-rated helmet mainly provides protection against shrapnel, and is likely to be penetrated by any direct hit from a bullet fired by an assault or sniper rifle.

Wear body armor whenever you are embedded with military forces. (Armor may not be recommended for covering criminal matters because it may cause a journalist to be mistaken for a law enforcement agent.) Body armor products are periodically updated as newer, lighter, and more reliable materials are developed. Journalists and news managers need to be mindful that different products may require different care. Ceramic plates may crack or break if they are dropped. Kevlar can deteriorate if it gets wet. Human sweat can degrade Kevlar and other products. Used body armor must be examined very carefully for signs of wear or weakening of fiber. All body armor must be properly stored and periodically inspected.

Protective gear is also available for covering civil unrest. Lightweight and relatively thin anti-stab vests can provide protection against knife attacks, rubber bullets, and other hazards. Baseball-style caps with metal plates are also available. Gas masks may also be worn, although in doing so journalists incur the risk that they could be mistaken for either riot police or demonstrators.

Embedded or Unilateral

Choosing the vantage from which to observe a conflict is among the most important choices you may make. Thoroughly research the politics, history, and behavior of all armed groups active in an area. Cohesion, discipline, morale, training, firepower, and respect for civilians, including journalists, varies widely among different military forces, and among irregular forces such as insurgents or pro-government militias. Be aware that circumstances on the ground may change at any time without warning.

The term "embed" was popularized by the U.S. military in the early 2000s for journalists who arranged to travel with specific military units during the U.S.-led invasion of Iraq. But journalists attaching themselves to military units to cover warfare goes back to the mid-19th century. Journalists who embed with any armed force are typically required to travel with the unit as ordered and avoid doing anything to reveal the unit's location or otherwise compromise its security. But you should retain the right to report events, albeit after the fact, as you see fit. CPJ has documented a number of disputes over embedding arrangements. Military authorities and representatives of armed groups, for example, have denied access to journalists whose reporting was seen as unfavorable.

> *Journalists were once able to cover conflict from different sides. Today, both governments and insurgents are attacking journalists suspected of having relationships with their foes.*

Those who report from any one side can also find themselves accused by another side of collaborating with the enemy. Decades ago, journalists were able to cover conflicts successfully from different sides in regions such as Central America. Today, both government forces and insurgents have detained or attacked journalists suspected of having relationships with their foes. In 2011, Ethiopian authorities imprisoned Swedish journalists Johan Persson and Martin Schibbye on treason charges after they were found embedded with the separatist Ogaden National Liberation Front. In Iraq and Afghanistan, U.S. military forces detained

numerous local journalists who were perceived as having had contact with insurgent forces. Some of those journalists were held for many months or years without ever being charged with a crime.

You face important trade-offs in determining whether to embed or to report unilaterally (that is, independent of military forces). Traveling with military forces provides you with exclusive access to frontline stories, but it can come at the expense of gaining other perspectives, including observing the impact of combat on civilians. Journalists traveling independently of armed forces may have a wider field of view. Fatalities are more common among journalists reporting unilaterally, but the risk of embedding with military forces should not be underestimated. Nine journalists were killed while embedded with military forces in Iraq from 2003 through 2009, while six embedded journalists died in Afghanistan from 2001 through 2011, CPJ research shows.

If you are embedded with a military force, be mindful not to stand out in a way that would suggest you are an officer or adviser. Snipers are trained to target the silhouettes of suspected officers within opposing military units. Journalists are sometimes required to wear the same uniforms as the combatants with whom they embed. Doing so does not compromise your professional obligations, but you should still wear or carry press credentials that would identify your status on closer inspection. Uniformed journalists should expect to be treated as enemy combatants by opposing forces; that includes situations in which you are separated from your military unit.

Journalists working unilaterally should also be aware of how their appearance and demeanor may look from afar. Photojournalists holding cameras or carrying gear have been mistaken for combatants, CPJ research shows. In 2003, machine gunfire from a U.S. tank killed veteran Reuters cameraman Mazen Dana as he was working outside Abu Ghraib Prison. One soldier later told investigators he thought Dana was an insurgent with a rocket-propelled grenade. If you are working unilaterally, choose clothing that does not resemble military gear and does not stand out from afar. Darker earth tones are preferable to brighter colors.

In covering armed conflict, be aware of the impact of real-time reports. What may be a compelling, fresh report to an audience far from the conflict zone may be perceived in the field as passing information to the enemy. Keep in mind that your professional role is to observe and report on the conflict, not to participate in even an inadvertent way.

Rules of War

Different rules of war apply depending on whether you are embedded or not. A credentialed, uniformed journalist legally becomes a part of the military unit with whom he or she is traveling, according to the Geneva Conventions of 1949. Embedded journalists may be fired upon legally by opposing forces as part of the unit, and the individual journalist may later be detained legally and held for the duration of hostilities as a prisoner of war.

Prisoner-of-war status can be a benefit. POWs are legally required to be imprisoned away from hostilities, and they must be fed, given medical attention, and publicly identified as prisoners (as opposed to being held incommunicado), as well as being allowed to send and receive mail. POWs may not be charged with espionage or civilian crimes, such as entering a nation without a visa.

Journalists are entitled to cover armed conflict as civilians operating independently of any armed force, according to the 1977 Additional Protocols to the Geneva Conventions. No civilian, including a journalist, may be legally targeted by any forces. But independent journalists face certain risks. Journalists captured while working unilaterally can be charged with civilian crimes such as espionage and can be subject to the potentially poor or abusive standards of civilian imprisonment.

Checkpoints

Interacting with armed groups at checkpoints is dangerous and unpredictable. Numerous civilians, including at least four journalists, were killed at U.S. military checkpoints in Iraq from 2003 through 2005. Soldiers guarding checkpoints often operate in fear of suicide bombings and other attacks.

Before traveling on local roads, consult with colleagues, military officials, and trusted local sources to determine possible checkpoint locations and their operators. Learn in advance all checkpoint procedures, such as the warning signals used by military forces and the protocol expected of approaching vehicles. Reduce speed as you approach a checkpoint, remove sunglasses, show free hands, and be respectful. Allowing soldiers or militants to search your vehicle may also be advisable. Stay focused and alert when navigating unfamiliar roads, and be aware that checkpoint signs and signals can be nonexistent or confusing. Many checkpoint casualties have stemmed from poor or misunderstood communication. Some roads should simply be avoided, particularly at night.

Checkpoints set up by irregular forces, militias, or paramilitary groups are even more dangerous and unpredictable because of poor discipline and the absence of clear lines of authority. In Libya in 2011, four *New York Times* journalists were seized at a checkpoint operated by forces allied with Muammar Qaddafi and held for six days, during which they were assaulted and mistreated. Their driver, Mohamed Shaglouf, was killed.

Journalists may encounter drunk or impaired personnel at checkpoints run by combatants, including irregular forces; they may be ordered to produce cash or other favors in exchange for being allowed to proceed. Some journalists carry small denominations of currency, packs of cigarettes, or items such as inexpensive watches in their original packaging to offer as small bribes. Be mindful not to do anything that could escalate the situation or the soldiers' demands. Engage on a level of mutual respect, without showing fear and with an overriding goal of safe exit.

Navigating checkpoints is a component of most journalist training courses (see Appendix B Security Training).

Satellite Technology in Hostile Environments

Satellite technology is a critical tool for journalists working in conflict zones where the Internet and other international connections are unreliable or have been shut down by authorities. In 2012, in the Syrian city of Homs--an opposition stronghold bombarded by government forces and effectively cut off by authorities seeking to quash news coverage--international and local journalists used satellite technology to file reports and communicate with news organizations.

American-born reporter Marie Colvin and French photographer Rémi Ochlik, who had been working with other reporters in a makeshift press center, were killed along with Syrian civilians by government shelling in February 2012. Some journalists who had worked in Homs suspected Syrian authorities targeted the building, although the city was also under heavy overall bombardment. If government forces had targeted the building, they could have relied on several forms of intelligence, including the tracking of journalists' satellite signals.

Technology experts agree that satellite phones can be tracked with ease. Detecting radio frequency emissions is "relatively simple for a trained technician," according to SaferMobile, a U.S.-based nonprofit dedicated

> *Satellite phones can be tracked with relative ease. Keep calls brief, avoid transmitting from the same location, and turn the device off when it's not in use.*

to helping human rights defenders and journalists use mobile technology more securely. The Electronic Frontier Foundation, a San Francisco-based nonprofit dedicated to Internet freedom, describes "ample" commercially available tracking devices. Satellite phones can also be tracked through their own built-in GPS devices. "GPS location data" may be "transmitted by the sat phone in the clear," noted SaferMobile.

Experts recommend strict protocols when using satellite phones in a hostile environment:

- Avoid using a satellite phone (or any radio frequency-based device) from the same location more than once.
- Avoid using a satellite phone or similar device from a location that cannot be easily evacuated in case of attack.
- Keep the maximum length of any transmission to 10 minutes. (Some experts warn that even this could be too long, as instantaneous tracking is at least possible.)
- Turn off the machine and remove its battery as soon as the transmission is over and before traveling.
- Avoid having multiple parties transmit from the same location.

Satellite transmissions, while encrypted, are not entirely secure either. In a 2012 report, for example, two German academics announced that they had broken two commonly used encryption algorithms. The U.S. nonprofit Small World News noted in its 2012 "Guide to Safely Using Satphones" that many governments are capable of defeating encryption. Use code words in highly sensitive transmissions, Small World News advises, or avoid satellite phones entirely for such communications.

If your satellite phone is confiscated, authorities or hostile actors can access critical information from its call log, phone book, and sent folder. Experts such as those at Small World advise that you routinely delete call logs and sent folders to protect your sources, and that you keep the sim card separate from the phone when not transmitting.

5. Organized Crime and Corruption

Crime and corruption are extremely dangerous beats, CPJ research shows. Thirty-five percent of journalists killed worldwide since 1992 covered these two topics. The lines between political and criminal groups are blurred in many nations, raising the risk for reporters. From Mexico to Iraq, criminal groups are operating increasingly like armed political forces, and armed political groups are operating increasingly as for-profit, criminal bands. Journalists have been attacked while reporting on collusion between crime figures and government officials, and they have been targeted while pursuing crime or corruption stories during times of both peace and war.

Local reporters pay the highest price. Nearly nine out of ten journalists killed worldwide are journalists reporting on issues in their own community, according to CPJ research. Moreover, from Mexico to the Balkans, from Russia to the Philippines, the killers get away with it in nearly nine out of 10 murder cases. Self-censorship in many nations is common because of the extreme risks.

Basic Preparedness

How to approach crime stories, including coverage of organized crime, depends almost entirely on local factors. The alarming number of journalists murdered while covering criminal activities in high-risk nations shows that there are no easy answers about what stories to cover, how to approach them safely, or whether it is safe to approach them at all.

Do as much research as possible before entering any criminal environment. One consortium of U.S.-based journalism schools and law enforcement colleges called Criminal Justice Journalists says that editors should give reporters two weeks to get up to speed before starting work on a crime beat. No doubt that's good advice. But many journalists today—especially freelance reporters—must invest their own time to prepare for work on beats such as crime. Reporters should familiarize themselves with high-crime areas, entry and exit routes, and safe, accessible places to meet sources.

In the United States, many press groups recommend that journalists meet individual law enforcement personnel in advance of working on stories. Criminal Justice Journalists suggests that reporters new to the beat request briefings from law enforcement on their operating procedures. Such advice is applicable in other nations where corruption in law enforcement is not widespread. In nations where high levels of law enforcement corruption have been documented—such as Mexico and the Philippines—you must make a different calculation. There, journalists must be watchful for law enforcement collusion with criminal actors. You need to assess each potential source's level of empathy or hostility.

Know the relevant laws concerning access to public and private property, trespassing, and invasion of privacy. (See Chapter 6 Civil Matters and Disturbances.) Be familiar with the specific conditions under which you can and cannot use video or audio recording equipment. The Reporters Committee for Freedom of the Press regularly posts updates on U.S. laws; journalists working in other nations can turn to local press organizations, many of which actively monitor and publicize laws affecting the profession. (See Appendix E Journalism Organizations for a list of many such groups. The International Freedom of Expression Exchange maintains a comprehensive listing.) Some matters remain unsettled, such as whether U.S. journalists can report inside a privately owned, publicly accessible space such as a shopping mall. Be aware that authorities in the United States and other nations may legally limit access, the ability to record, or both, at some publicly advertised events such as political rallies or speeches. You should also note that authorities may lawfully restrict access to courthouses, jails, schools, airports, military facilities, federal buildings, civic centers, and stadiums.

Crime reporters with a vehicle may wish to keep an emergency bag that includes a change of clothes,

foul-weather gear, a flashlight, and a first-aid kit. In covering any dangerous story, keep your mobile phone charged and with you. (Remember that mobile phones can be tracked by hostile subjects. See Chapter 3 Technology Security for techniques to mitigate surveillance.) At least one editor should always be aware of a crime reporter's work, sources, and progress. Freelancers should keep an editor or another trusted colleague apprised of the same.

When you approach a potentially hostile subject, you should be accompanied or observed by a colleague. To reduce the possibility of being singled out for reprisal, you should communicate to all crime sources, especially hostile subjects, that you are not working alone and that your activities are being closely monitored by a news organization or colleague. Find and cultivate, if possible, a senior law enforcement officer to whom you or others could turn in case of emergency.

Planning an Investigation

Safely covering crime and corruption requires thoughtful preparation and risk assessment. (See Chapter 2 Assessing and Responding to Risk.) Before embarking on any potentially dangerous story, thoroughly research news reports, public documents, and court records, in addition to speaking to colleagues experienced in the reporting area, and trustworthy and knowledgeable local sources.

Safety concerns are the responsibility of not only the journalist, but also the news outlet planning to publish or broadcast the reporting. Newsroom managers should consider specific security measures to protect facilities, journalists, and in some instances the families of journalists. Drawing up a written risk assessment is recommended. (See Chapter 1 Basic Preparedness and Appendix G Security Assessment Form.) When covering dangerous figures such as criminal or terrorist suspects, the assessment should be accompanied by a contingency plan in case the journalist or his or her sources become endangered.

The assessment should identify the most dangerous actors and most sensitive issues in the investigation and assess the risks that may arise. In any such investigation, the wrong question at the wrong time to the wrong source could put a journalist or his sources at risk. You may wish to begin your reporting by interviewing the sources in whom you have the most trust, gradually working toward those who may be more hostile. Be aware that your questions can give an indication as to the nature of your story. To protect yourself and your sources, limit how much you disclose about your investigation.

Begin by interviewing the sources in whom you have the most trust, gradually working toward those who may be more hostile. Limit how much you disclose about your reporting.

Toward the end of an investigation, a journalist and his or her editor may wish to draw up a separate risk assessment to help determine whether and how to approach a criminal suspect who may be a subject of the story. The assessment should include an evaluation of risk, a series of options to approach the individual, and an appraisal of the suspect's possible reactions.

The assessment should include clear protocols to establish how and when you will communicate safely with your editor and perhaps other trusted colleagues. This could be done through a variety of methods—from email to telephone calls—and it may involve simple code that would communicate whether you believe you are safe or in danger. You and your editor should also discuss in advance under what circumstances you might be compelled to suspend or call off the investigation. A contingency plan should be developed in the event that you or your sources may be in danger.

Be mindful about how you record and store information. To protect the identities of sources in your

written notebooks and electronic files, you may wish to use coding or pseudonyms that you will remember but that others will not easily decipher. This is especially important when dealing with informants who would be endangered if their identity were disclosed. Notebooks with sensitive material should always be secured; notes with innocuous material can be left accessible in case intruders search your belongings. Electronic files can be made more secure through the use of USB flash drives, strong password protection, and remote backups, among other measures. (See Chapter 3 Technology Security for a full description of securing electronic data.)

Approaching Hostile Subjects

Whether and how to approach suspected criminal actors depends on several factors. Journalists should always consider the status of law enforcement agencies. In areas where law enforcement is weak or corrupt, journalists should expect far higher levels of risk and adjust their approach accordingly.

Be mindful of how you and your news outlet may be perceived among the community of individuals being covered. Journalists should "bend over backward" to show their impartiality and willingness to give every subject the chance to tell his or her story, Drew Sullivan, editor of the Sarajevo-based Organized Crime and Corruption Reporting Project, told American Journalism Review, for an article in 2010. "Be relentless but friendly and open in your effort to talk to the people you hope to win as sources," suggests Bill Wallace of the U.S.-based Criminal Justice Journalists in the group's report "Covering Crime and Justice," developed from 2003 through 2010.

In any criminal investigation, keep in mind that the greatest risk may not be reporting on criminal groups themselves, but on the web of official corruption that protects them. In many parts of the world, extreme caution is advised. Journalists investigating official corruption or any form of collusion with criminal actors may wish to develop a cover story to tell people, especially potentially hostile sources. The cover story should be credible and broad enough to encompass the actual investigation without giving away the specific matter under investigation.

The period shortly before a story runs is often a dangerous time. Journalists should be mindful of what they say, to whom, and when. Hostile and potentially violent subjects may take pre-emptive action if they learn that they are the target of an investigation. In 2007, U.S. journalist Chauncey Bailey was shot dead three blocks from his Oakland, California, office after the proprietor of a local business tied to criminal activity learned that the journalist was investigating the establishment's finances.

One question is whether suspected criminal actors can be safely approached under any circumstances. Reporters and editors in nations where law enforcement is weak must make the realistic but ethically painful decision as to whether pursuing the story or naming alleged perpetrators is worth the risk at all. If a decision is made to approach potentially hostile subjects, editors should know in advance and the journalist should be either accompanied by or observed by a colleague. Journalists should communicate to hostile subjects that they are speaking not just to an individual but to the news organization planning to run the story.

Some subjects may be considered too dangerous to approach in person. In some cases, it is advisable to approach the subject's lawyer rather than the individual directly. The subject or the person's attorney should understand that the story is already planned and that you are seeking comment for ethical and legal reasons. In the absence of a defense attorney, you can assess whether it is practical or safe to communicate with the subject by phone, email, or other written correspondence.

But even that may be too dangerous. Communicate candidly with your editor about situations in which a subject may be too hostile to approach. Consider your safety and that of sources when considering the next

step. The public record sometimes offers a means by which a hostile subject's denial or viewpoint may be derived.

Accessing Information

Obtaining official documents is an important aspect of investigative reporting. In addition to providing the substantive benefits of citing official documents, the practice can lessen one's reliance on comments from local sources who could themselves be at risk of retribution from criminal or corrupt figures.

Reporters and editors need to be versed in the public-information laws that apply in each nation. The U.S.-based Citizen Media Law Project provides an array of suggestions and tools for accessing information from municipal, regional, and national authorities in the United States. The website Right2INFO.org compiles documents and publications on access-to-information laws worldwide. Although online access to government data remains patchy worldwide, some progress has been made. The Kenyan government, for example, launched a database of public information in 2011. In some parts of the world, including much of Africa, the right to government information is enshrined in the law, but practical procedures to obtain specific records are nonexistent or unclear. Journalists should confer with local experts and colleagues in advance of seeking information in such nations. A number of local press organizations worldwide monitor access-to-information laws and the practical procedures to obtain information. (See Appendix E Journalism Organizations for a list of many such groups. The International Freedom of Expression Exchange maintains a comprehensive listing.)

Because obtaining documents through official means is difficult in some nations, many journalists still rely on sources to access government data. A journalist must take precautions, however, to avoid revealing the identity of a source who provided sensitive documents. A reporter, for example, could visit several agencies with access to a document in question in order to enlarge the possible pool of sources and make it more difficult for authorities or other actors to identify the actual source.

Protect sources who provide sensitive documents. Visit multiple agencies with access to such records in order to enlarge the pool of possible sources.

The use of documentation may also shift risk onto the journalist. Be aware that governments and criminal actors have taken legal or extralegal action in reprisal for the disclosure of sensitive material. Nearly half of all journalists imprisoned worldwide are jailed on antistate charges that include revealing information that governments consider to be state secrets. Criminal actors, sometimes in collusion with state authorities, have used coercion in many nations to compel journalists to reveal the sources of incriminating documents.

Collaborative Efforts

Journalists are finding alternative ways to publish dangerous stories. In Central Asia and other parts of the world, many have published risky stories under pseudonyms. News outlets in Latin America have run stories with generic bylines, such as the "Justice and Peace Unit" label used by the Colombian newspaper *El Espectador*.

News organizations can also work together on dangerous topics, sharing information and publishing a story simultaneously without individual bylines. Egos, organizational rivalries, and political, ethnic, or religious identities must be set aside to pursue such collaboration. But the approach has proved effective in diffusing the risk against any individual journalist while enabling reporters to cover hazardous topics.

Journalists in Colombia began working collaboratively after a series of attacks on publishers and editors of outlets that reported critically on drug traffickers. The most notable attack was the 1986 assassination of Guillermo Cano, *El Espectador* publisher and editor-in-chief, a crime attributed to the Medellín cartel leader Pablo Escobar. As CPJ board member María Teresa Ronderos recounted in a 2010 CPJ report, *El Espectador* joined with its main competitor, *El Tiempo*, and other media outlets in the following months to investigate and publish stories about drug trafficking's many tentacles in society.

Years later, in 2004, a coalition of Colombian print outlets began working together on dangerous assignments such as infiltration by illegal paramilitary groups in the nation's lottery. This and other investigative stories were published simultaneously in 19 Colombian magazines and newspapers. The newsweekly *Semana* led another collaborative effort, the Manizales Project, designed to investigate murders and threats against journalists. While violence against Colombian journalists has not stopped, CPJ research shows, it has occurred less frequently and at a lower level.

Collaborating across borders is another way to confront organized crime. Groups such as the Washington-based International Consortium of Investigative Journalists, with members in 50 nations, have produced news-breaking reports on topics such as tobacco smuggling and black-market ocean fishing. The Belgrade-based Center for Investigative Reporting-Serbia and the Sarajevo-based Organized Crime and Corruption Reporting Project together uncovered offshore holdings of Serbian billionaire Miroslav Mišković.

Warning Signs

Journalists should be watchful for signs that they are under surveillance, notes the Sarajevo-based Organized Crime and Corruption Reporting Project. (See Chapter 9 Sustained Risks for further advice on surveillance.) Some private security firms have added surveillance detection to the hostile-environment training they offer journalists. (See Appendix B Security Training for a list of firms.) Knowing that one is under surveillance can give reporters and editors time to consider options. That includes whether or not to continue working on the story, to put other reporters on the story, to involve other news organizations, to rely on and report the matter to law enforcement authorities, and to relocate journalists and their families. Journalists should be aware of the possible reactions to stress that they and their families may face in covering organized crime and corruption. (See Chapter 10 Stress Reactions.)

6. Civil Matters and Disturbances

Civil scenarios from crime scenes to riots can generate unpredictable and dangerous conditions. Journalists need to be mindful of self-protection measures to avoid putting themselves at physical or legal risk.

Accident, Fire, and Rescue Scenes

The first responsibility of anyone among the early or "first responders"—including police, ambulance workers, and firefighters, as well as journalists—is to protect one's self by surveying the scene and being aware of potential hazards, such as oncoming traffic, downed power lines, and the leaking of combustible fuel or hazardous chemicals or gases. As in other situations, you should be close enough to observe the scene without endangering yourself or others, or interfering with security or rescue operations. Photojournalists should apply similar judgment, understanding that they must be close enough to record the events. Authorities usually establish a perimeter in order to keep onlookers, including journalists, at a distance; you may request, but cannot usually demand, a closer vantage point than other onlookers. That said, authorities should be encouraged to provide journalists with a vantage that allows them a clear view of operations. Toward that end, editors should discuss access issues with senior police and emergency officials on an ongoing basis and develop mutually agreed-upon guidelines for news coverage at emergency scenes.

Crossing police lines or disobeying police orders could lead to arrest. Being respectful in both tone and demeanor is usually the best way to proceed. Journalists covering emergency or rescue scenes should also prominently display their press credentials at all times.

Confrontations sometimes arise between authorities and journalists covering a scene. U.S. reporter Diane Bukowski was found guilty of crimes including obstructing and endangering two Michigan state troopers while covering the aftermath of a fatal crash involving a motorcyclist who was pursued by a state police vehicle. Authorities claimed Bukowski crossed a police line; Bukowski claimed she did not cross a line and was taking pictures at a distance of one of the deceased.

Crime and Terrorist Scenes

Violent crime scenes may be more complicated to cover. Self-protection is again the first rule. During a hostage standoff or other unsettled scenario, be careful not to expose yourself to risk from further disturbances. One question to ask is whether perpetrators may still be at large in the area. In the case of a terrorist attack or other action designed to attract public attention, consider the chance of follow-up attacks. CPJ has documented dozens of cases in which journalists responding to an initial blast were killed or injured when a follow-up bomb exploded. If a second attack or double bombing is possible, you may wish to remain on the periphery and interview witnesses as they leave the area.

> *Witnesses and survivors of violent events may be traumatized. Understand that the scene of a crime may not be the best or only time to ask questions.*

Clearly display credentials at crime scenes, including local government-issued credentials whenever possible. (See the section on Press Credentials in Chapter 1.) Avoid confrontations with authorities; at such times, having relationships with senior law enforcement officials is useful. (See the section on Basic Preparedness in Chapter 5.) And avoid contact with material that is potential evidence; do not remove any material from the crime scene.

Witnesses and other survivors of violent events may be agitated or traumatized. "Journalists will always

seek to approach survivors, but journalists should do it with sensitivity, including knowing when and how to back off," notes the Dart Center for Journalism & Trauma in its guide, *Tragedies and Journalists*. More than anything else, this means respecting survivors' wishes about whether they want to be interviewed or have their emotions recorded; demonstrating such respect, in fact, may well lead survivors to allow journalists greater access. Police and rescue authorities may also be traumatized. Understand that this may not be the best or only time to ask questions of either survivors or authorities.

Stories Involving Private Property

You do not have a right to trespass on private property in pursuit of a story. Journalists may enjoy some limited access to private property when covering publicly advertised political rallies or events. Learn in advance the relevant laws and regulations.

Journalists in the United States and other nations may not enter private property without the consent of the owner or resident, even if they have been accompanying police authorities responding to a situation. "Even when reporters gain access without being stopped, they can be arrested for trespass and property owners may sue them after the fact, seeking damages for trespass or invasion of privacy," the U.S.-based Reporters Committee for Freedom of the Press notes in its field guide.

In most nations, you have the right to access private property when it is open to the public at large, although your right to electronically record events, as opposed to simply taking notes, may still be limited. Political events or rallies that take place on private property, which could be deemed to include the rented space or field of a public school or other government facility, are often contentious sites between authorities and journalists. Courts frequently hold that the private owners or renters of the space (even if it is a publicly owned property like a park or school) have the right to deny journalists the use of video cameras or audio recorders, and to ask journalists to leave the premises if they refuse.

Journalists who refuse to leave may be arrested for criminal trespass in the United States and other nations. Some journalists maintain that they were not given time to leave after being ordered off the premises. In 2010, *Alaska Dispatch* editor Tony Hopfinger was detained and handcuffed by a private security guard after asking questions of a U.S. Senate candidate following a publicly advertised meeting in a public school rented by the campaign. Police arrived, removed the handcuffs, and released Hopfinger, who was not charged with a crime.

Journalists need to be prepared and use care in covering events on or near private property. Clearly displaying press credentials at all times when reporting stories on private property is recommended.

Protests and Riots

Journalists covering protests and other violent civil disturbances face legal and physical risks from all sides, often at the same time. About 100 journalists died while covering street protests and other civil disturbances from 1992 through 2011, according to CPJ research. In 2011, nearly 40 percent of work-related fatalities came during such assignments, the highest proportion CPJ had ever recorded.

Physical fitness is an important consideration in covering situations that could suddenly turn violent; journalists whose mobility is limited should weigh the risks in advance. Being mindful of one's location at all times is also essential, and this usually means finding a vantage point that allows for observation of both protesters and riot police or other authorities without ending up between them. Be aware of how such events have played out in the same locations in the past. Map out exit routes in advance, and consider working in teams when covering any potentially violent situation. Photographer and writer teams, camera operator and sound operator teams, and producer and correspondent teams allow journalists to watch out for each other.

In many nations, news organizations have hired security teams to accompany journalists. The spate of attacks against journalists during the 2011 Egyptian revolution and aftermath underscored the violent situations journalists can encounter during civil unrest. Journalists should also know the relevant laws and practices in case either law enforcement agents or protesters demand to review or confiscate video cartridges or other recording material.

Clothing should be chosen thoughtfully, including whether it would be better to stand out or blend in. Clothes should be loose-fitting and made of natural fabric, as synthetic materials can catch fire and burn much more quickly, the Brussels-based International Federation of Journalists notes. Good shoes with appropriate support and flexible, non-slip soles are also essential.

Try to keep yourself out of harm's way. One could think of a journalist as a referee on the playing field: The referee must be close enough to observe the game accurately, yet must take every precaution to avoid getting mixed up in the action. When covering protests or riots, avoid being caught between clashing groups or ending up in the middle of any crowd. "Walk along the sides of the protesters," recommends the Swiss journalist Dominik Bärlocher on the Canadian Journalism Project website J-Source. "The people who throw stones and such usually do that from the middle of the mass of protesters where they can blend back into the crowd."

In covering protests or riots, keep out of harm's way. Avoid being caught between clashing groups or ending up in the middle of any crowd.

Whether to display one's press credentials or keep them out of sight (but still handy enough to show on demand) is an important decision for writers covering civil unrest. In some circumstances, it may be better to look like any other civilian and keep your press credentials out of sight but in a closed and quickly accessible pocket, as Bärlocher suggests on J-Source. In either case, journalists should avoid wearing clothing such as a colored bandanna or a blue windbreaker, which might make them resemble a protester or law enforcement agent. In situations where being mistaken for a demonstrator could be dangerous, all journalists should clearly display their press credentials. For radio and TV reporters, and other journalists using equipment to record events, it is almost always best to display a laminated press card.

Never pick up anything thrown at a demonstration. Not only could it be a homemade explosive or combustible device, but doing so may make police presume that you are a protester.

Consider what to bring when covering a protest or similar event. Bärlocher recommends a pack with "at least a strap across the chest and…another one around the waist" to keep it "from bouncing around and hindering you, especially when running." Everything in the backpack should be expendable; items to carry include bottled water (preferably in an open side pocket), a towel, and a small first-aid kit. Be aware, however, that carrying a backpack, as demonstrators often do, could lead law enforcement agents to mistake you for a protester.

Carrying a lime, lemon, or other citrus fruit can be a good idea, according to the International Federation of Journalists. The fruit can be squeezed onto an affected area of skin to help neutralize chemical irritants. A wet towel can help protect your face from the effects of agents such as tear gas or Molotov cocktails. A gas mask, swimming goggles, or industrial eye protection can also help protect against tear gas or pepper spray. (Avoid wearing contact lenses if you think tear gas or pepper spray may be used.) Light body-armor vests designed to stop knives or rubber bullets, along with metal-lined caps, may be recommended in particularly uncontrolled situations. The International Federation of Journalists recommends that videographers and photographers carry "dud" cartridges or memory cards to hand over instead of the real ones if demanded.

Journalists should obey orders from law enforcement officers, although authorities sometimes arrest

journalists without giving orders first. At least four journalists were among hundreds arrested while covering protests related to the 2008 Republican National Convention in St. Paul, Minnesota. The journalists were arrested without warning as police attempted to corral protesters and journalists covering their actions into a fenced parking lot. Days later, police arrested dozens of journalists along with hundreds of protesters after sealing off both sides of a highway overpass.

Remain calm if you are arrested. If you choose to object to the arresting officer, you may worsen your situation. If you do speak up, make every effort to maintain a professional demeanor as you explain that you are a journalist covering news. (Whatever sympathies you may have for any actors on the ground are beside the point; what is always important is that a journalist act on the ground not like a participant but as an observer.) If the authorities decide to proceed with the arrest, comply with orders and wait for an opportunity to make your case calmly to a supervising authority.

7. Natural Disasters

Earthquakes, hurricanes, tornados, floods, tsunamis, cyclones, monsoons, volcanic eruptions, fires, avalanches, and landslides can all strike with little or no warning. Breakdowns in communication, transportation, and power should be expected. The ability to either report or disseminate information may also be impaired.

Establishing redundancies to maintain communications with colleagues is essential. Two-way radios may be necessary, for instance, if local cell phone towers are down. Newsrooms should prepare in advance for the possibility of natural disasters in their vicinity by preparing a detailed contingency plan. Journalists assigned to cover natural disasters overseas or otherwise away from their newsroom should review field safety protocols before departure.

Freelance Risks

A sudden natural disaster can create immediate opportunities for freelance journalists. But stringers must understand that they may have to navigate the risks and accept potential consequences on their own. Freelancers would be well advised to contact editors in advance to secure interest in possible stories, and to determine the level of institutional support a news organization will provide.

Freelancers should draw up a risk assessment before traveling to a scene, identifying potential hazards, detailing plans to communicate with editors and others, and charting multiple potential exit routes. (See Chapter 2 Assessing and Responding to Risk.) Freelancers should also consider what level of health, disability, and life insurance they may have, and whether their insurance policies exclude natural disasters often described in policy language as "acts of God." (See the section on Insurance Coverage in Chapter 1.)

Freelancers should draw up a risk assessment before traveling to a scene, identifying potential hazards, detailing plans to effectively communicate with editors and others, and charting multiple potential exit routes.

Newsroom Planning

Managers of newsrooms prone to hurricanes or floods should prepare and update a detailed disaster plan before each intemperate season. In areas where such events are rare, editors should update their emergency plans at the same time each year. The completed disaster plan should be printed out in hard copy (in a disaster, computers, the Internet, and electrical power could be down) and reviewed by the entire staff. All staff members should be aware of their responsibilities and the roles they will be expected to play. Everyone should retain his own hard copy of the emergency plan and know where emergency materials are stored.

The disaster plan should include the landline phone numbers, cell phone numbers, and work and personal email addresses for all newsroom employees or contractors, along with contact information for their next of kin, according to the International Center for Journalists' *Guide to Disaster and Crisis Reporting*. The plan should include a map with each individual's home address clearly marked, identifying who is certified in CPR or other emergency first aid, and who has a four-wheel-drive vehicle. In disaster-prone areas, managers should ensure that multiple staff members are trained in basic first aid. (For staff security, the plan should not be disseminated publicly or posted in a public place.)

Include contact information for government authorities as well as local emergency personnel for use in newsgathering and for newsroom safety. The contacts should include national, regional, and local emergency response and relief agencies, along with independent experts. Include instructions for operating

the newsroom in an emergency. If only a limited number of staff can reach the newsroom during the emergency, they should be able to publish or broadcast reports. Managers should prepare employees to assume such tasks as may be required.

Transportation and Equipment

Journalists of all kinds should research what equipment or other supplies may be safely stored in case of a power outage or other disruption. Generators, emergency lights, batteries, two-way radios with back-up batteries, GPS location devices, first-aid kits, and extra first-aid equipment should be part of the reserve. Packaged or canned food, bottled drinking water, cots, and blankets may also be needed in disaster-prone areas.

Press vehicles should be equipped with emergency gear, including a first-aid kit, road flares, and blankets. Managers should research where to obtain emergency rentals of vehicles, communication equipment, generators, and other gear, and include the information along with contact details in the disaster plan. They should consider having standing emergency contracts with local transportation providers, according to the International Center for Journalists. Managers should also know how to get reserve fuel during an emergency.

Large, hard-copy maps should be kept in the newsroom, marked with locations of hospitals; emergency clinics, including pediatric clinics; shelters; transportation centers; schools; and other buildings that could be used to harbor families or refugees during a crisis. Physical, topographic maps should be on hand to help identify hazards such as low-lying areas where flooding is likely.

The newsroom's digital data should be backed up and stored on at least one server located elsewhere. Important paper data should be copied and stored off-site.

Field Safety

Avoid putting yourself at risk. Doing so would only make you a burden to emergency crews and colleagues. Journalists should work in teams of at least two and preferably three people during disaster coverage; one team member should carry a small first-aid kit. Waterproof gear should be readily available and worn as needed. Carry contact information that includes your blood type and allergies, preferably on a laminated card and perhaps worn around your neck.

Reporters and editors alike should monitor road and other travel conditions and do as much as possible to keep each other informed of changing conditions. Evacuation routes should be mapped out and updated as needed. The best way into an area may not be the best way out. Multiple routes and travel contingencies must always be planned. Natural disasters can give rise to a host of other problems, from leaking toxic fumes to water-borne diseases.

Be aware of the surrounding conditions at all times. One member of the team should be watchful for any changes in conditions and be tasked with maintaining and updating exit strategies. Water lines can rise, power lines can fall, gas pipes can explode, fires can spread, and criminals can approach. Team members may also wish to carry whistles in case they become separated, as recommended by the International Federation of Journalists. Traveling with a private security entourage may be recommended when looting and other crimes are occurring during the natural disaster.

Journalists traveling to an overseas disaster or to a hazardous area at a distance from the newsroom should be equipped with a GPS device, a portable satellite phone, and a shortwave radio to monitor international broadcasts if local broadcasting is interrupted. On location, be sure you have sufficient water, food, and batteries (or other back-up sources of power for communications).

8. Health Epidemics and Mass Hazards

Outbreaks of the Ebola virus in Central Africa, the Severe Acute Respiratory Syndrome, or SARS coronavirus, in Asia, the H1N1 virus in tropical and other regions of the world, and cholera in Haiti are all examples of health epidemics that severely tested news media. Events involving bioterrorism as well as chemical and radiation emergencies pose yet another set of risks for the reporters and photojournalists covering them. As described in Chapter 7, freelancers should know that they may have to address risks and accept consequences on their own. A freelancer wishing to cover a health epidemic or mass hazard would do well to contact editors in advance to secure interest in possible stories, and to determine the level of institutional support a news organization might provide.

Basic Preparedness

Any journalist planning to cover a disease epidemic or a manmade health emergency should be in good health, have an immune system that is not compromised, and have no existing condition that could predispose him or her to illness.

Before traveling to an affected area, consult the World Health Organization's *International Travel and Health* handbook along with its region-specific publications, as well as the U.S. Centers for Disease Control and Prevention's *Emerging Infectious Diseases Journal*. The World Health Organization provides guidelines for specific diseases, explaining the science behind a disease and measures to avoid infection. In 2005, the organization released a journalists' handbook on the influenza pandemic. Health bulletins, regional updates, and travel restrictions are accessible on the international organization's website, which is available in many languages.

The World Health Organization and the U.S. Centers for Disease Control and Prevention each provide information on biological, chemical, and radioactive emergencies. These sources and others should be frequently checked for any updated information. Both sites offer podcasts, RSS feeds, and other updated information to help journalists stay on top of developments as they occur.

Consult a health care professional before departure. Receive recommended vaccinations and allow sufficient time for them to work. (See the section Medical Care and Vaccinations in Chapter 1.) Be sure your medical kit is updated with gear and medication specific to the risks you will face on an assignment. (See Appendix A Checklists.) Bring as much medication as allowed, because there may be shortages locally.

Review your medical insurance as well to see if it will cover treatment and other expenses likely to be incurred in case of illness, including the cost of emergency medical evacuation. Journalists and others might be denied permission to leave an outbreak zone if they become ill. This could expose you to further physical as well as psychological injury. Keep in mind that any serious health emergency could overwhelm local health facilities, so prepare alternative plans.

Protecting Yourself

Journalists should always prioritize their own safety. No story is worth your life, and if you were to be killed or become ill from exposure, you would become a burden instead of an asset.

Even the combination of good health and vaccination are no guarantee of avoiding a disease. Wash your hands frequently and immediately after any possible exposure, as recommended by the World Health Organization's *International Travel and Health* handbook, which is updated annually. Carry hand sanitizer in any such situation. Avoid potentially contaminated food and water. Avoid any possible contact with

bodily fluids, skin, mucous membranes, and related medical waste.

Learn how the disease in question is transmitted, and then take the appropriate precautions. The World Health Organization lists seven ways diseases can be spread: through food and water, vectors such as mosquitoes, infected animals, soil, air, and sexual contact or contact with blood and bodily fluids. Precautions include sleeping under bed nets, avoiding sexual contact, and, if possible, avoiding crowded situations and confined spaces.

Learn how specific mass hazards may be spread. Bioterrorism and other biological hazards could include anthrax, botulism, brucellosis, plague, smallpox, tularemia, and viral hemorrhagic fevers, according to the U.S. Centers for Disease Control and Prevention. Each biological agent is distinct in the way it is spread, its symptoms, prevention, and treatment. There are other chemical agents that can be of military, industrial, or natural origin. Similarly, each chemical agent will spread differently and require its own form of protection and treatment. The U.S. Centers for Disease Control and Prevention and the U.S. Department of Health and Human Services provide information on radiation emergencies, including the effects of dirty bombs, nuclear blasts, nuclear reactor accidents, and transportation accidents. Exposure to radiation can produce short- and long-term conditions, including some effects that may become apparent years later.

Learn the science of a health or mass hazard. Take precautions, adapt your behavior, and obtain protective gear. Even then, some situations may be too risky.

Learn the science of any biological, chemical, or radiation threat. "In a radiation emergency, you can think of distance, time, and shielding as protective devices," *New York Times* editors wrote in a 2011 document prepared for their reporters. "Distance means not getting too close to a spill of radioactive material or other sources of radiation. Time means that if you are in an area that your dosimeter indicates has radiation, don't stay longer than you have to. In certain circumstances, you may also gain some protection by taking shelter in a concrete or brick building."

The danger may be imperceptible. "The radioactivity meter is going up, but you don't feel a thing," Tetsuo Jimbo, Japanese journalist and founder of the website *Videonews*, told CNN in 2011 after he traveled with a Geiger counter into Japan's nuclear quarantine zone near the damaged reactor at Fukushima. "You don't smell anything, you don't feel heat, you just don't feel a thing. And that's actually the most scary part of the whole trip."

Extreme caution is required in every case. Journalists and others must realize in advance that some scenarios would be simply too dangerous to cover as long as the threat persists. Journalists should research the specific threat and the agent's possible duration, as well as all protective measures or equipment that may be needed. The list of recommended equipment is extensive in severe cases. Antidotes to counteract hazardous agents should be obtained only though qualified medical experts, as they are specific and limited in their use and carry considerable risk.

Do not hesitate to ask your employer or assigning news organization to purchase protective gear. At the same time, be aware that even the best measures and state-of-the-art equipment may be ineffective in severe situations.

9. Sustained Risks

Many of the risks described in this guide are specific to a particular assignment. But critical journalists working in repressive or hostile environments often face routine harassment and constant threat. Consider the groups most responsible for murdering journalists in recent decades worldwide. Antigovernment groups, including terrorists, are responsible for nearly one-third of all journalist murders, according to CPJ research. But government officials and government-linked groups such as paramilitaries are responsible for nearly the same proportion of journalist murders. Journalists in some nations do not know whom they can trust.

Personal Security

Being aware of your surroundings is essential when facing risk of attack or abduction. Practical safety procedures should include varying travel routes, changing routines, and keeping home and office buildings locked and alarmed. It may also involve securing vehicles in a locked garage, regularly checking vehicles for explosives, and checking mail for explosives. If you are faced with this situation, you should immediately enlist the assistance of security experts. (A number of security organizations are listed in Appendix B Security Training.) In some nations, journalists working under threat have chosen to wear body armor, travel with armed guards, and post observation cameras as well as guards outside their homes and offices. In making these decisions as well, journalists should consult with security experts.

Governments in nations from Colombia to the Balkans have official programs in which they assign armed escorts to accompany journalists under threat. In Colombia, in particular, teams of armed government bodyguards along with a driver and armored-plated vehicle have been assigned to journalists who have been attacked or threatened. As cumbersome as the arrangement may be, threatened or recovering journalists often feel it is necessary to protect themselves and deter future attacks. The hiring of private guards, if the cost is not prohibitive, may be another option.

Family Security

There may be no greater fear than believing your family members are at risk. Assessing the possible risk to your family can be guided in part by the past behavior of hostile actors. Family members of dissidents were frequently targeted in Guatemala in the late 1970s and early 1980s, as they were in Iraq in the Saddam Hussein era. Such historical background can provide insight into contemporary situations. Journalists may also wish to consult local security experts, colleagues, human rights defenders, and diplomats.

Be aware of material your family posts to social media sites. Do not share information about your family's daily schedule or vacation plans. Take care in publishing photos.

Be aware of the personal material you or your family post to Facebook or other social media sites. The people who wish to intimidate you are likely to seek out everything published online not only about you, but about your family as well. Do not share information about your family's daily schedule or vacation plans, for example. Take care in publishing photos or disclosing information not otherwise public. You may wish to have your family remove certain information from their social network pages or raise the privacy settings.

Some experts suggest you avoid sharing details about sensitive work with family members. Family members who are not informed about your investigative work, this logic goes, would not be targeted by

assailants seeking to coerce information. Nonetheless, your family members could still be targeted as a way to broadly terrorize you and deter you from pursuing a sensitive story. Special care may be advisable to ensure that your children are monitored and escorted at all times.

You may wish to consider switching assignments for a time. More drastic measures include temporary or permanent relocation of family members. Journalists may wish to contact CPJ or other international organizations that may be in a position to help.

Surveillance

Surveillance comes in many forms, from the old-fashioned tactics of shadowing journalists in the street to the electronic techniques that intercept data without leaving a trace. The former is often used by repressive regimes with limited resources, such as the African Horn nation of Eritrea. The latter is deployed with chilling efficiency in nations with well-equipped intelligence operations, such as China. Throughout much of the last decade, the Colombian intelligence service illegally intercepted emails, eavesdropped on phone conversations, and conducted surveillance against many of the nation's most prominent reporters. In Tunisia, during the regime of Zine El Abidine Ben Ali, critical journalists were placed under constant surveillance for both intimidation and information-gathering purposes.

CPJ has documented cases of physical or electronic surveillance in numerous other nations, including Afghanistan, Angola, Bangladesh, Belarus, Bosnia-Herzegovina, Bolivia, Burma, Cuba, Equatorial Guinea, Iran, Pakistan, Rwanda, Russia, Sri Lanka, Sudan, Syria, Thailand, Turkmenistan, Ukraine, Uzbekistan, Vietnam, Yemen and Zimbabwe. In the United States, a former U.S. National Security Agency analyst told MSNBC that the American spy agency electronically eavesdropped on journalists in the 2000s.

Physical surveillance of individual journalists often precedes violent attacks. Interior Ministry officials in Ukraine have acknowledged that their agents were watching journalist Georgy Gongadze shortly before he was abducted and murdered in a 2000 government plot. Colleagues of Geo TV correspondent Wali Khan Babar in Pakistan told CPJ that he was being followed in the days before he was killed in 2011. Babar was murdered by two assailants who intercepted his car and shot him four times in the head and once in the neck.

Do a broad assessment if you are concerned that your movements, communications, and reporting material are being observed or intercepted by third parties. What are you working on that might be considered sensitive? Who might take offense at your reporting? What surveillance techniques are they likely to employ? Are they more likely to have agents follow you, or are they adept at electronic surveillance? Once you've gauged the level of risk and the likely methods of surveillance, you can consider modifying your activities. That could include varying your professional and personal routines, along with your regular travel routes. In electronic communications, you may want to begin using pre-arranged codes with sources, resorting to prepaid phones not linked to your name, employing encryption programs, or using secure Web email or virtual private networks. (See Chapter 3 Technology Security.) You should also consider notifying your editors and colleagues, along with local and international press freedom groups.

Be aware of unfamiliar people or vehicles outside your home or office, especially if they appear more than once. Detecting that you are being followed can give you time to reduce risk. Enlisting a trusted person to observe your movements and those of potential followers is one method to confirm surveillance, but precise procedures are best imparted by trained experts. Some private security firms have added surveillance detection to training programs they offer journalists. (See Appendix B Security Training.)

Solidarity

Professional solidarity is important in situations in which local journalists face sustained risk. Perhaps the best step journalists can take in such environments is organizing themselves first in their newsroom, then with other journalists and news organizations within their city or region, and ultimately across their nation.

Groups such as the Philippine Center for Investigative Journalism, founded in 1989, or Colombia's Foundation for a Free Press, founded in 1996, have played valuable roles in curbing attacks on journalists and bringing journalists of all kinds together. The Philippine center has raised the profile of journalist murders and helped push authorities to bring those responsible to justice. The model has been followed by the Brazilian Association for Investigative Reporting, which was established in 2002 after the abduction and murder of national television correspondent Tim Lopes. The Brazilian group has pushed authorities to take action in anti-press attacks.

Journalists should never hesitate to contact international press freedom organizations such as the Committee to Protect Journalists and the Paris-based Reporters Without Borders, along with other human rights monitoring groups. (See Appendix E Journalism Organizations.) International groups can help raise the profile of journalists working under threat and pressure national authorities to respond.

Contingency Planning

Journalists facing sustained risk should prepare a contingency plan. The plan should include contact information for the journalist and his or her family members and editors, along with responsive government officials, foreign diplomats, and both local and international press freedom and human rights organizations.

The plan should specify the frequency and exact means by which the journalist will check in with editors and family members. The plan could include a simple code for the journalist to discreetly signal an immediate threat. Codes could also be devised to signal that the journalist wants to meet at a prearranged location, or to switch to another means of communication. In the event a journalist becomes out of touch, the plan should specify how long editors and family members should wait before taking action. The plan should include a detailed list of individuals and groups for editors and loved ones to contact or call locally, regionally and internationally.

10. Stress Reactions

Post-traumatic stress is a normal reaction to abnormal events. Stress can affect not only war correspondents, but journalists covering any tragedy involving pain or loss of life. Death penalty executions, random shootings, terrorist bombings, sexual assault, sexual abuse of children, domestic violence, suicides, and bullying are among the stories that can cause extreme stress.

Post-traumatic stress can manifest itself in many ways. The individual experiencing stress may be able to articulate no more than simply having the feeling that something is just not right, or that something more should be done. For journalists whose job is to observe and report on events, not act on them, merely watching human tragedies unfold can extract an emotional toll. Journalists who interview trauma victims, in fact, may themselves be exposed to and experience what experts call vicarious or secondary trauma. Photo and video editors may be traumatized from handling one grisly image after another. News managers on every level may be traumatized from the stress of helping to manage the risks facing their reporters and photojournalists, especially in the wake of injury or fatal loss.

Signs of Stress

Signs of stress are often subtle. A journalist may seem more anxious, irritable, withdrawn, numb, depressed, sad, or angry, and the emotions may be either sustained or fluctuating. Physical symptoms can include sleep or eating disorders, a rapid heartbeat, sweating, panic attacks, headaches, nausea, and chest pain. Strained personal and work relationships are often common. So is alcohol or drug abuse. Other signs may include an abnormally intense focus on one's work, as if one is trying, as with other compulsive behaviors, to avoid uncomfortable feelings.

How common is post-traumatic stress among journalists? More than one in eight journalists working in the United States and Europe sampled at large in a 2001 study by the German scholars Teegen and Grotwinkel showed the ongoing signs of extreme stress or post-traumatic stress disorder (PTSD). In a 2002 study led by Canadian psychiatrist Anthony Feinstein, more than one in four war correspondents showed ongoing signs of extreme stress. Studies have further shown that conflicts within the workplace, whether among journalists or between journalists and their supervisors, may compound individual reactions to trauma.

"Journalists are a resilient tribe," noted Bruce Shapiro, executive director of the Dart Center for Journalism & Trauma, in a 2010 speech in Melbourne, Australia, "but we are also vulnerable to psychological injury, no less so than firefighters, police officers, paramedics, or soldiers—and we need training, psychological support, and leadership aware of these issues."

Post-traumatic stress disorder is a diagnosis established in 1980 by clinicians working with U.S. veterans of the Vietnam War. The disorder involves a preponderance of symptoms lasting several months or longer. The disorder may also involve more intrusive symptoms, including emotional withdrawal or numbness, intense fear, anger or guilt, helplessness, hyper-vigilance to perceived threats, reduced awareness, and confusion.

PTSD can further change the way neural networks communicate with each other within the brain, and the changes "can elicit the re-enactment and reliving of past experiences," notes Matthew Friedman, executive director of the U.S. Veterans Association's National Center for Post-Traumatic Stress Disorder. If left untreated, PTSD can also exacerbate a range of medical conditions like hypertension.

The good news is that clinicians have established the phenomenon of post-traumatic growth. "We're talking about a positive change that comes about as a result of the struggle with something very difficult," University of North Carolina at Charlotte psychologist Lawrence G. Calhoun told *The Washington Post* in 2005. Post-traumatic growth involves a better sense of self, relationships with others, abilities to cope, and appreciation of life after not only recovering, but emerging enhanced from having overcome a traumatizing experience. The growth occurs from "people who have faced major life crises develop[ing] a sense that new opportunities have emerged from the struggle, opening up possibilities that were not present before," UNC Charlotte researchers wrote.

Taking Care of Yourself

Recognizing that you are traumatized may be the hardest step. Many journalists and soldiers have something in common in that the dominant culture of both groups has tended to resist recognizing the impact of trauma. "I'm still not sure that our culture is ready to accept this," Gen. George W. Casey Jr., the U.S. Army's chief of staff, told *The New York Times* in 2009. Explaining the need to cope with emotional stress can be a hard sell to a young private who mainly "wants to hang out with his buddies and drink beer," he said.

Journalists need to learn how to take care of themselves. Simply taking a break can be invaluable. So can finding the courage to tell an editor that you need a new beat. Even more important may be allowing yourself to grieve or otherwise experience your own emotions. Regular exercise helps to relieve stress, according to scientific experts. The National Institutes of Health National Center for Complementary and Alternative Medicine reports that mind-body exercises such as yoga, tai chi, qi gong, and meditation can be beneficial.

> *Learn to care for yourself. Take a break from work, tell an editor that you need a new beat. Give yourself the opportunity to grieve or experience your emotions.*

Articulating your emotions is another way to relieve stress. Journalists can only benefit from discussing their experiences with each other. The venue could be a place in the newsroom or a nearby coffee shop. Newsroom managers should help create opportunities and forums for such peer debriefing to take place. "What I really needed was time with fellow journalists, to talk through all the things that happened," said Penny Owen of *The Oklahoman* in an interview with the Dart Center after the 1995 bombing of an Oklahoma City federal building. "By the time we slowed down, everyone was so tired of the bombing that we never really got to have that big hashing-out session." Whatever the venue, the setting should be one where no one feels judged and journalists feel safe to open up in front of each other.

Speaking to a counselor is another option for journalists experiencing emotional stress. The Dart Center provides a guide for choosing a therapist. Many therapists have experience in treating post-traumatic stress, and a recommendation from a friend is often a good place to start in finding a good counselor. (Some health insurance plans will help cover costs. See Chapter 1, section on Insurance Coverage, and Appendix C Insurance Providers.) Some cultures are more resistant than others to recognize post-traumatic stress. Journalists living in nations where there is little awareness of the issue may be well advised to consult the website of the Dart Center.

Conclusion: The World Ahead

In many ways, the dangers facing journalists are unchanged over several decades. Some of the broadest, most indiscriminate attacks on the press came in 2011, during uprisings demanding democratic reforms. Government officials and ruling party militants in Egypt attacked more journalists more blatantly over a shorter span than in any time in memory. Journalists of many nationalities working for media serving audiences in every major language group were attacked or detained. The broad range of violence and restrictions underscored the invaluable role that journalists play in holding governments and others accountable.

Yet technology is rapidly altering the way news is spread. The release in 2010 and 2011 of classified American diplomatic correspondence by the document-disclosure network WikiLeaks highlighted the global revolution in the flow of information. Governments and their allies are moving aggressively to stanch this flow, CPJ research shows. About half of all journalists imprisoned around the world are incarcerated on antistate charges such as engaging in espionage and violating state secrets. And those at risk reflect the changing nature of the news business: About half of the journalists behind bars at any given time work primarily online, and about half are freelancers. Each year, those proportions grow larger.

New, online media networks are on the rise. Some are modeled on traditional news models, while others bring together journalists as a community of stringers. Journalists in the latter category often work without the institutional support, including insurance and legal backing, that many staff journalists have long enjoyed. In this changing and dangerous climate, be guided by some basic principles: Be fully informed about security issues, make your safety a primary consideration, prepare yourself thoroughly for each assignment, look out for other journalists in the field, and take care of yourself before, during, and after assignment.

Appendix A: Checklists

Personal Gear

Depending on specific needs and possible challenges, journalists should consider selecting items from the following list and also think strategically about other equipment that might be useful. Many news organizations recommend keeping a packed emergency bag at home, at the office, or in a personal or news vehicle.

On your person or among your gear:

- A blood donor card in your wallet or, if you are in a conflict area, a laminated card hanging around your neck with your blood type and any allergies clearly marked;
- cash in appropriate and possibly multiple currencies well hidden, perhaps inside specially made pouches or items with hidden compartments;
- a dummy wallet to hand over with at least one easily replaceable photograph identification card;
- a passport or travel documents, including an immunization card;
- two photocopies of every travel document stored in different locations;
- and extra passport-size photos.

In your vehicle:

- Flashlight, road flares, or emergency light;
- reflective safety vest;
- maps of the surrounding area;
- blankets;
- drinking water;
- basic tool kit;
- and inflated spare tire and jack.

In your bag:

- Sufficient prescription medications;
- antimalarial medication;
- prescription eyeglasses or contact lenses, along with spare pairs;
- contact lens solution and storage container;
- sunglasses;
- pens and notebooks;
- digital voice recorder or digital camera;
- mobile phone;
- laptop;

- AC as well as cigarette lighter chargers;
- spare batteries;
- laminated copies of contact information for newsroom staff;
- and any risk assessment plan or disaster plan.

In your pack:

- Water bottle;
- water disinfectant or, in areas where contamination with feces is possible, a water filter;
- small flashlight or headlamp;
- extra batteries;
- appropriate electrical adapters, cables, and earphones;
- dried snacks;
- rain or cold-weather gear;
- blanket;
- hat;
- gloves;
- change of clothing;
- towel and basic toiletries;
- hand sanitizer;
- wet wipes;
- sunblock;
- bug repellent;
- hand and feet warmers;
- well-stocked first-aid kit;
- athlete's foot cream;
- condoms or other contraceptives;
- tampons or sanitary napkins;
- and zip-lock bags.

Just in case:

- Pocketknife or pocket tool;
- sunblock;
- mosquito net;
- plastic bags;
- rubber bands;

- plastic zip ties;
- string or cord;
- gaffer's tape (which does not leave behind a residue like duct tape) or other strong tape;
- chamois skin;
- and dust brush for cleaning gear.
- A binocular may be advisable in some circumstances, but you should be aware that it may raise the suspicions of authorities.

First-Aid Kits

According to the World Health Organization, a first-aid kit could contain a combination of the following items. Journalists should consider the demands of each assignment and select from or add to this list as may be appropriate:

- Adhesive tape;
- antiseptic cleanser;
- bandages;
- emollient eye drops;
- insect repellent and bite treatment;
- antihistamine cream or tablets;
- nasal decongestant;
- oral rehydration salts;
- scissors and safety pins;
- simple analgesic;
- sterile dressing;
- thermometer;
- earplugs;
- antidiarrheal medication;
- broad-spectrum antibiotics;
- antifungal powder;
- and sedatives.

Individuals with appropriate training may also wish to include:

- emergency trauma bandages;
- chest seal dressings;
- burn dressings;
- alcohol or other sterilizing swabs;
- splints;
- tourniquets;
- medications;
- and other medical equipment.

Appendix B: Security Training

The firms below all offer hostile-environment courses designed in whole or in part for journalists.

AKE Ltd

www.akegroup.com

+44 (0) 143-226-7111

U.K.-based AKE was the first private firm to provide journalists with hostile-environment training. Courses are designed around practical scenarios and demonstrations to give journalists the knowledge and confidence to face dangerous situations.

Centurion Risk Assessment Services

http://www.centurionsafety.net

+44 (0) 172-686-2090

U.K.-based Centurion conducts safety training courses regularly in the United States and United Kingdom that emphasize personal safety, awareness, and emergency first aid as well as a variety of topics relevant to journalists working on dangerous assignments.

Chiron Resources

http://www.chiron-resources.com

+44 (0) 788-060-2426

U.K.-based Chiron Resources has run specialized media hostile-environment training courses and other security training courses in several countries around the world, in English, French, and Arabic.

Global Journalist Security

http://www.journalistsecurity.net

+1 202-244-0717

Founded in 2011 by this report's main author, CPJ Senior Adviser for Journalist Security Frank Smyth, Global Journalist Security's training addresses military and civilian contingencies, including sexual assault, digital security, and organized crime.

Objective Travel Safety Ltd.

http://www.objectiveteam.com

+44 (0) 178-889-9029

The U.K.-based Objective Travel Safety offers a range of security training courses every month, including courses covering emergency medical provisions, surviving natural disasters, kidnap prevention, negotiating checkpoints, booby-trap awareness, and dealing with traumatic stress.

Pilgrims Group

http://www.pilgrimsgroup.com

+44 (0) 844-788-0180

+44 (0) 148-322-8778

Pilgrims Group is a U.K.-based security training, consulting, and intelligence firm. The group provides hostile-environment training as well as body armor and security personnel. Pilgrims has also offered condensed training courses in New York and other locations.

Tor International

http://www.torinternational.com/

+44 (0) 193 287 9879

+212-452-0909

U.K.-based Tor International provides services including risk assessment and management, in addition to hostile-environment training, body armor, medical kits, communications equipment, and armored and other vehicles.

TYR-Solutions

http://www.tyr-solutions.com

+44 (0) 20-3239-5257

TYR-Solutions is a U.K.-based firm that provides security and medical training, risk and crisis management services, and communications and tracking training and support, along with portable trauma packs and communications and tracking equipment.

Appendix C: Insurance Providers

There are many different insurance providers and brokers. The list below includes only those firms or groups that help provide insurance to journalists and others on high-risk assignments. Journalists are advised to shop for the best possible rates from a host of potential providers.

Banner Financial Group

http://www.bannergroup.com

+44 (0) 199-386-2119

The U.K.-based Banner Financial Group offers individual and group insurance for people living or working abroad. Policies can cover injuries from war and terrorism and include death or bodily injury insurance.

Bellwood Prestbury

http://www.bellwoodprestbury.com

+44 (0) 124-258-4558

+44 (0) 124-258-8688

Bellwood Prestbury is a U.K-based firm providing specialized plans for individuals living or working abroad in high-risk professions or in dangerous areas. Coverage can include war or terrorism risks and kidnap and ransom insurance.

Crisis Insurance

http://www.crisis-insurance.co.uk

+44 (0) 143-226-8301

Crisis Insurance is a U.K.-based firm specializing in high-risk policies for dangerous areas or dangerous professions. Policies can be tailored to individual needs and are available for short or long terms.

Reporters Without Borders

http://en.rsf.org

+33 1 44 83 84 84

The Paris-based nonprofit Reporters without Borders offers an insurance policy tailored to the needs of journalists working abroad in possibly hostile situations. Plans can be purchased per diem or for as long as a year.

Safe Passage International

http://www.spibrokers.com

+1 303-988-9626

+1 800-777-7665

The U.S.-based Safe Passage International offers travel insurance for both corporate clients and nonprofit organizations. Under its Security First plans, the firm offers accident insurance including risks posed by war and terrorism, as well as plan covering kidnap, ransom, and extortion. Additional plans cover accidental death or dismemberment.

Appendix D: Journalism Resources and Manuals

Dart Center for Journalism & Trauma tip sheets and guides

http://dartcenter.org

New York +1 212-854-8056

Seattle +1 206-616-3223

London +44 (0) 207-242-3562

Melbourne +61 (0) 41-913-1947

Jakarta +62 217-884-2580

Cologne +49 (0) 221-278-0814

The Dart Center for Journalism and Trauma provides journalists with the necessary resources and health information to deliver quality, informed reporting on tragedy, disaster, and violence. Its website provides tip sheets, studies, and articles about trauma, journalism, and mental health. Dart has published guidebooks on reporting war and dealing with the stresses of covering tragedies.

FAIR Investigative Journalism Manual

http://www.fairreporters.org/?IJ_manuals

FAIR's manual is designed for investigative reporters who are working under difficult conditions, such as those in Africa. The manual was written based on case studies and anecdotes submitted by investigative journalists in Africa.

Frontline Protection of Human Rights Defenders Manuals

http://frontlinedefenders.org/resources

Frontline offers a Protection Manual for Human Rights Defenders that is devoted to personal security, risk analysis, and planning. The manual is also available in a condensed handbook. Frontline's Security-in-a-Box digital security manual, developed with the Tactical Technology Collective, helps ensure the safety of digital materials and correspondence as well.

ICFJ Training Manuals

http://www.icfj.org/Resources/tabid/209/Default.aspx

The International Center for Journalists offers a range of manuals covering investigative reporting, ethical decision-making, trauma, natural disasters, and a variety of special or regional topics. Many are available for free and the rest are available as low-cost digital copies.

IFJ's *Live News* Survival Guide

http://www.hnd.hr/uploads/Journalism_survival_guide2003.pdf

Published in 2003, the International Federation of Journalist's guide remains valuable. It covers working in hostile environments and war zones, civil unrest and riots, kidnapping and hostage taking, emergency medical aid, and traumatic stress.

IWPR Training Manual

http://iwpr.net/reporting-change-handbook-local-journalists-crisis-areas

The Institute for War & Peace Reporting's standard training manual contains a chapter on journalist safety.

Topics covered include personal security and situational awareness, as well as reporting from war and disaster zones. It is available in six languages on IWPR's website. The institute also publishes topical and regional guides.

Reporters without Borders *Handbook for Journalists*

http://en.rsf.org/handbook-for-journalists-january-17-04-2007,21744.html

Updated in 2010, the *Handbook for Journalists* is a comprehensive guide covering a variety of relevant safety issues, including first aid, humanitarian and public health emergencies, health precautions to take when traveling, and reporting in war zones.

SaferMobile *A Guide to Mobile Security Risk Assessment*

https://safermobile.org/resource/mobile-security-risk-assessment-guide/

SaferMobile helps journalists and others use mobile technology more securely. The guide begins with a Mobile Risk Primer that describes general security vulnerabilities associated with mobile technology and communication.

Small World News *Guide to Safely Using Satphones*

http://smallworldnews.tv/Guide/Guide_SatPhone_English.pdf

Released in March 2012, the guide examines satellite phone use in repressive nations. It offers advice on best practices, including detection avoidance and security precautions.

World Health Organization *International Travel and Health*

http://www.who.int/ith/en/index.html

The World Health Organization publishes this guide to safety while traveling abroad as well as others such as its *Guide on Safe Food for Travellers*. These cover such topics as necessary vaccinations for travel; food safety; and health risks in different regions and under different conditions, such as natural disasters. It also includes a full list of items that might be contained in a well-stocked first-aid kit.

Appendix E: Journalism Organizations

Press Freedom Groups

Adil Soz

http://www.adilsoz.kz/en/

+7 7272 911670

This Almaty-based organization provides legal support for journalists under threat and documents press freedom violations in Kazakhstan.

Andean Foundation for Media Observation & Study

http://www.fundamedios.org

+593 2 2461622

This Quito-based group, also known as Fundamedios, documents press freedom abuses in Ecuador and speaks out against official repression.

Article 19

http://www.article19.org

+ 44 (0) 20 7324-2500

Established in 1987, Article 19 fights against censorship, defends dissenting voices, and campaigns against laws and practices that silence.

Committee to Protect Journalists

http://www.cpj.org

+1 212-465-1004

The publisher of this guide, CPJ is an independent nonprofit press freedom organization that defends the rights of journalists to report the news without fear of reprisal. The organization monitors and advocates on behalf of journalists under threat and in prison around the world, documenting hundreds of press freedom violations each year and reporting on press freedom conditions in every country.

Foundation for a Free Press (Fundación para la Libertad de Prensa)

http://www.flip.org.co

+57 1-400-9677

The foundation, also known as FLIP, is a Bogotá-based organization 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 Fund for Filipino Journalists

http://www.cmfr-phil.org/flagship-programs/freedom-watch/freedom-fund-for-filipino-journalists

+63 2 894 - 1314

The FFFJ is a consortium led by the nation's Center for Media Freedom & Responsibility. Launched in 2003 in response to the murder of journalist Edgar Damalerio, the FFFJ has worked to bring the murderers of Philippine journalists to justice.

Independent Media Centre Kurdistan

http://www.imckiraq.blogspot.com

+964 0770 86 42 653

The Independent Media Centre in Kurdistan offers training for journalists and consultancy for media organizations. Courses are offered in person or online for participants throughout Iraq.

Institute for Reporters' Freedom and Safety

http://www.irfs.az

+994 12 418 0334

The institute, based in Baku, Azerbaijan, documents press freedom abuses and defends the rights of journalists to report the news.

International Federation of Journalists

www.ifj.org

Europe: +322-235-2200

Asia-Pacific: +6 129-333-0999

Africa: +22 133-867-9586

The Brussels-based IFJ is a federation of journalist trade unions in various nations, and it is the world's largest organization of journalists. IFJ promotes human rights, freedom of expression, and democracy through freedom of the press.

International Freedom of Expression Exchange

http://www.ifex.org

+1 416-515-9622

IFEX is a global consortium of press freedom groups that disseminates news about press freedom violations and organizes campaigns in support of free expression.

International Press Institute

http://www.freemedia.at

+43 1 512-9011

IPI is a Vienna-based global network of media professionals concerned with raising awareness of threats to press freedom and promoting independent journalism. The group tracks the cases of journalists targeted for their reporting and conducts assessments of press freedom in countries around the globe.

Instituto Prensa y Sociedad

http://www.ipys.org

+51 1 2474465

This Peruvian press freedom group documents press freedom violations and advocates for journalists under threat.

Journalistic Freedoms Observatory

http://www.jfoiraq.org

+964 0047 97 101 186

JFO is a Baghdad-based coalition of Iraqi media professionals providing legal support for victims of press freedom violations in Iraq and raising awareness around journalism security.

Journaliste en Danger

http://www.jed-afrique.org/en

+243 81 71 50 157

This Kinshasa-based organization defends press freedom in the Democratic Republic of Congo and other Central African nations.

Media Institute of Southern Africa

http://www.misa.org

+264 61 232975

Founded in September 1992, the Namibia-based institute promotes free, independent, and pluralistic media.

Pakistan Federal Union of Journalists

http://pfuj.pk

+92 051-287-0220-1

Established in 1950, PFUJ is among South Asia's oldest press freedom organizations. Formed for mutual protection and economic betterment, the PFUJ, according to its code, "desires and encourages its members to maintain good quality of workmanship and high standard of conduct."

Reporters Committee for Freedom of the Press

http://www.rcfp.org

+1 800-336-4243

+1 703-807-2100

RCFP is a U.S.-based organization dedicated to serving working journalists and protecting free speech and a free press within the United States. The group provides resources for journalists, academics, and government officials, along with support for freedom of information requests.

Reporters Without Borders

http://en.rsf.org

rsf@rsf.org

+33 1 44 83 84 84

Reporters Without Borders is a Paris-based press freedom organization that defends journalists threatened or imprisoned around the world. The group works on journalist safety issues and offers its own insurance, lends safety equipment, and publishes a safety handbook.

Southeast Asian Press Alliance

http://www.seapabkk.org

+66 2-2435579

The Southeast Asian Press Alliance works for press freedom in Southeast Asia. Established in Bangkok in 1998, it brings together independent journalists for advocacy and protection.

World Press Freedom Committee

http://www.wpfc.org

The WPFC is a consortium of international news organizations that defends press freedom internationally. The group conducts research on press freedom violations and censorship and insult laws, and monitors the cases of journalists jailed around the world.

Internet Freedom Communities & Groups

Electronic Frontier Foundation

http://www.eff.org

+ 1 415-436-9333

+ 1 202-797-9009

The Electronic Frontier Foundation 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.

Privacy International

https://www.privacyinternational.org/

+ 44 (0) 20 7242 2836

Privacy International defends the right to privacy across the world, and fights surveillance and other intrusions into private life by governments and corporations.

Global Voices

http://globalvoicesonline.org

Global Voices is 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.

News Safety & Support Organizations

Dart Center for Journalism & Trauma

http://dartcenter.org

New York +1 212-854-8056

London +44 (0) 20-7242-3562

Melbourne +61 (0) 41-913-1947

Jakarta +62 21-7884-2580

Cologne +49 (0) 221-278-0814

The Columbia University–based Dart Center is dedicated to informed and ethical news reporting on violence, conflict, and tragedy. It provides a range of services for working journalists and newsrooms worldwide.

Free Press Unlimited

http://www.freepressunlimited.org/en

+ 31 35-62-54-300

Free Press Unlimited supports local media professionals and works to ensure that people everywhere have access to the information they need to survive and develop.

International News Safety Institute

www.newssafety.org

+44 776-681-4274

+44 773-470-9267

INSI is a coalition of news organizations and support groups dedicated to journalist safety in dangerous environments. The group provides safety training to journalists around the world and educates policymakers, news organizations, and militaries about journalist safety. CPJ is a member of the coalition.

International Women's Media Foundation

http://iwmf.org

+1 202-496-1992

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

The Rory Peck Trust

http://www.rorypecktrust.org

+ 44 (0) 20-3219-7860

The Rory Peck Trust supports freelance newsgatherers and their families worldwide in times of need and promotes their welfare and safety through efforts such as security training.

Professional Training Organizations

Institute for War and Peace Reporting

www.iwpr.net

+44 (0) 207-831-1030

IWPR works with local journalists and media workers on the frontlines of conflict to strengthen reporting skills and increase awareness around human rights issues, promoting public discourse and debate.

International Center for Journalists

www.icfj.org

+1 202-737-3700

ICFJ promotes independent journalism around the world through education, training, and fellowships. It also publishes several handbooks on journalism skills and ethics, which are available online.

Poynter Institute

http://www.poynter.org

+1 727-821-9494

The Poynter Institute is a nonprofit educational institute that offers seminars, individual classes, and online courses about journalistic values and practices. Its NewsU online training program makes Poynter's resources available to journalists all over the world.

Tactical Technology Collective

http://www.tacticaltech.org/protect

+493 060 961816

+918 041 531129

While primarily aimed at advocates, Tactical Tech provides up-to-date advice and resources for independent journalists on information security risks and remedies.

Investigative Reporting Groups

Associação Brasiliera de Jornalismo Investigativo

http://www.abraji.org.br

+55 (11) 3159-0344

Also known as Abraji, the group focuses on professional development for journalists and in particular on sharing tips and techniques related to investigative reporting. Abraji fights for freedom of information in Brazil and offers online and in-person courses to journalists and journalism students.

Arab Reporters for Investigative Journalism

http://www.arij.net

ARIJ supports independent journalism in the Middle East by offering training and funding for investigative projects. ARIJ will pay for travel expenses, access to databases, and legal screening for investigative reports.

Bureau of Investigative Journalism

http://www.thebureauinvestigates.com

+44 (0) 796-946-6285

The U.K.-based Bureau of Investigative Journalism seeks to improve original investigative journalism by producing quality in-depth reports for other news outlets. The reports focus on national and international corruption and transparency issues.

Centro de Investigación Periodística

http://www.ciperchile.cl

+56 2 638-2629

CIPER is an independent nonprofit organization that seeks to develop investigative reporting in Chile. The group focuses on using Chilean law and professional reporting techniques to make government documents and information available to the public.

Centro Periodismo Digital

http://www.centroperiodismodigital.org

+52 3 268-8888

The Digital Journalism Training Center at the University of Guadalajara supports journalists in learning to work with new media and also promotes the training of citizen journalists. It offers courses and workshops as well as classroom instruction and online resources.

European Fund for Investigative Journalism

http://www.journalismfund.eu

+45 4082-2168

The fund supports journalists doing investigative reporting internationally or trying to cooperate with reporters in other countries. The fund is a project of the Pascal Decroos Fund for Investigative Journalism, which provides training and other grants for improving journalistic research.

Forum for African Investigative Reporters

http://www.fairreporters.org

+2711-482-8493

FAIR is a professional association for African investigative journalists working to improve the profession and its practices. FAIR provides databases, tip sheets, manuals, and grants, and seeks to support investigative journalists in Africa who face obstacles due to lack of training, low pay, and life-threatening situations.

Global Investigative Journalism Network

http://www.globalinvestigativejournalism.org

The Global Investigative Journalism Network is an organization of more than 40 nonprofit organizations worldwide, all focused on investigative or computer-assisted reporting. It organizes regional conferences to encourage best practices and support the formation of new groups seeking freedom of information. Its website also has a large directory of member organizations and other investigative reporting support networks.

International Consortium of Investigative Journalists

http://www.publicintegrity.org/investigations/icij

+1 202-446-1300

The Washington, D.C.–based Center for Public Integrity's International Consortium of Investigative Journalists is an international forum for cooperation among investigative journalists working on issues that reach beyond national boundaries. The consortium is backed by the Center for Public Integrity and focuses on international crime and corruption reporting.

Investigative News Network

http://www.investigativenewsnetwork.org

+1 213-290-3466

+1 818-582-3533

The Investigative News Network serves as a media watchdog and a support network for helping nonprofit journalism organizations. It consists of more than 50 North American nonprofit news outlets.

Investigative Reporters & Editors

http://www.ire.org

+1 573-882-2042

IRE is a nonprofit training organization for investigative journalists at the Missouri School of Journalism. It provides support for reporters and protects the rights of investigative journalists while advocating for high standards in in-depth reporting.

Organized Crime and Corruption Reporting Project

http://reportingproject.net

+387 33-56-0040

The OCCRP is a cooperative venture between several Eastern European news organizations and investigative reporting centers designed to share resources and safety tips in order to produce investigative reports about organized crime.

Philippine Center for Investigative Journalism

http://www.pcij.org

+63 2 431-9204

The Philippine Center for Investigative Journalism promotes investigative reporting in the Philippines. The center provides training for journalists both in the Philippines and elsewhere in Southeast Asia.

ProPublica

http://www.propublica.org

info@propublica.org

+1 212-514-5250

ProPublica is a U.S.-based nonprofit newsroom that produces investigative reporting about abuses of power. The group has an explicit focus on stories it sees as having moral force, and seeks to stimulate positive reforms with its reports.

Publica

http://www.apublica.org

Publica is Brazil's first nonprofit investigative journalism center and it aims to promote journalism as a public good by strengthening independent investigative reporting. The center works with other news outlets in Brazil and internationally to fund in-depth reporting projects.

SCOOP

http://www.i-scoop.org

SCOOP is a network of investigative journalists in Eastern and Southeastern Europe whose aim is to cooperate on international projects and share experiences and ideas. SCOOP works in 12 countries and its website has an extensive list of centers for investigative journalism all over the world.

Appendix F: Other Resources

International Society for Traumatic Stress Studies

www.istss.org

+1 847-480-9028

The ISTSS is dedicated to sharing information about the effects of traumatic stress and reducing its long-term consequences. The website provides research and resources, educational materials, and treatment guidelines for traumatic stress and PTSD.

National Center for Complementary and Alternative Medicine

http://nccam.nih.gov

+1 888-644-6226

The NCCAM is part of the U.S. National Institutes of Health and is dedicated to research about health practices and treatments that are not typically considered part of traditional Western medicine. The NCCAM provides information about trauma and stress and studies about potentially effective alternative treatments, as well as warnings about health risks from fraudulent treatments.

National Institute of Mental Health

www.nimh.nih.gov

+1 866-615-6464

The NIMH is part of the U.S. National Institutes of Health and conducts research and provides information about mental health conditions and services. Its website offers information about many kinds of mental health disorders, including traumatic stress.

RAINN: The Rape, Abuse, & Incest National Network

http://www.rainn.org

+1 202-544-1034

A U.S.-based organization, RAINN provides information about avoiding, surviving, and recovering from sexual assault. The National Sexual Assault Hotline is available online over the RAINN website or by telephone. In addition, the website provides a directory of international resources.

U.S. Centers for Disease Control and Prevention

http://www.cdc.gov

+1-800-232-4636 (24-hour health information hotline, Monday through Friday)

The U.S. government agency is a public source for information on common diseases, disorders, and treatments. The CDC website provides information about sickness and disease, healthy living, safety and emergency care, and disaster preparedness and response.

The World Health Organization

www.who.int/en

The World Health Organization, the public health arm of the United Nations, monitors global health conditions and follows emerging disease outbreaks around the world. It provides comprehensive guidelines for travelers regarding vaccination, sanitation, and disease prevention, as well as travel warnings and restrictions.

Appendix G: Pre-Assignment Security Assessment

The Committee to Protect Journalists developed this template from original material prepared by security experts at Human Rights Watch. This template is provided for guidance only. Note that each journalist and news organization faces unique circumstances that will require modifications of this template.

☐ **1. ASSIGNMENT DESCRIPTION**

Identify dates of travel, itinerary, and names of staff members, freelancers, and others (including locally hired consultants) who are participating in the assignment.

☐ **2. RISK ANALYSIS**

Identify potential security risks associated with carrying out the assignment.

☐ **2.1 HOSTILE SUBJECTS**

Assess the chances that you, your team, or the local contacts interacting with you on the ground will be targeted for surveillance or attack.

Identify potentially hostile actors, including government authorities, organized crime, rebel groups, and irregular forces. Identify the relative degree of cohesiveness and any prior and possibly relevant hostile actions or attacks.

☐ **2.2 LOCATION RISKS**

Identify risks associated with reporting in the location. Such risks could include outbreak of hostilities/escalation of conflict; abduction/kidnapping; interactions with hostile authorities (problems crossing borders/checkpoints, arrest, detention); physical or electronic surveillance; confiscation/misuse of sensitive information; health risks; dangers associated with various means of transportation; common crime.

☐ **2.3 SECURITY FOR LOCAL CONTACTS**

Identify risks that people working or interacting with you (local translators, drivers, sources, witnesses, etc.) may face. Assess the possible actors who could be involved, and include any such prior surveillance, actions, or attacks.

☐ **2.4 RESEARCH RISKS**

Specifically address the risks associated with conducting your work (conducting interviews, taking photographs, filming, visiting news scenes, obtaining and carrying documents and photographs that may have evidentiary value).

☐ **2.5 PROFILES**

Explain how your own profile, the profiles of other members of your team, and that of your news organization may increase or decrease the risk.

☐ **2.6 INFORMATION RELIABILITY**

Explain whether the team has access to the latest security updates for the area, what and who have been the main sources of information for the risk analysis, and the degree to which the available information may be outdated or otherwise limited.

☐ 3. PROPOSED MEASURES TO MINIMIZE RISK

Describe measures that will be taken by you, your team, headquarters, and others to minimize the risks associated with carrying out the assignment.

☐ 3.1 LODGING

Identify all hotels, guesthouses, private homes, and other types of accommodation in all locations for the duration of the trip. Explain why the proposed lodging option is considered safe. (Is security present? Is it used by international workers? Is it located in a safe area?) Indicate whether the lodging has functioning communication (phone lines, Internet access). Provide contact information for the lodging.

☐ 3.2 TRANSPORTATION ARRANGEMENTS

Describe transportation arrangements for the trip. If planning to use public transportation or taxis, indicate whether there are any risks associated with this and how they are going to be addressed. If hiring a car, explain how the driver has been or will be selected. Provide the driver's information in **Contacts** section below.

☐ 3.3 COMMUNICATION

Describe whether you or your team will use an international cell phone, local cell phones, satellite phones, land lines, and/or portable radios, and describe any problems associated with the use of each method of communication. (Such problems could include the absence or potential interruption of cell phone coverage in various locations; satellite phone coverage and any legal or security problems in using such phones; and phone surveillance.) Indicate whether the team will have regular Internet access. Identify the best means of communication should the situation on the ground require a detailed follow-up conversation with headquarters.

☐ 3.4 PROFILES

Describe whether you or your team plans to operate with a high or low profile in the country and the measures addressing the risks associated with each approach. Describe how you and your team will enter the country and present yourself at various situations (at the border, at checkpoints, during other interactions with authorities).

If there are any risks associated with the team members' individual profiles (such as nationality, ethnicity, race, gender, or sexual orientation), describe whether and how they can be addressed and whether any additional measures need to be taken to minimize the risks.

☐ 3.5 RESEARCH AND OTHER ACTIVITIES

Describe how you or your team plans to carry out its reporting in a manner safe for you and your subjects. If relevant, indicate whether specific measures are necessary to ensure anonymity of certain subjects and what method will be used to contact subjects to avoid undesirable exposure.

☐ 3.6 SECURITY OF INFORMATION

Specify measures to protect sensitive information while on assignment. Indicate whether you or your team will use electronic devices for information gathering and storage (voice recorders, cameras, computers, etc.) and measures to ensure the security of information in case the devices are confiscated or otherwise compromised, or in case of other unauthorized access to information.

If using only hand-written notes, specify what measures will be taken to protect them from unauthorized access or loss.

☐ 3.7 SECURITY OF OTHERS

Based on the risk analysis above, describe proposed measures to ensure security of people

working or otherwise interacting with your team—these include but are not limited to local consultants, interpreters, and drivers.

☐ 3.8 OTHER SECURITY MEASURES

Describe any additional security measures that may be necessary to minimize the risks associated with the mission. These may include measures to address health risks (necessary inoculations, advanced first-aid kits, etc.) and, if relevant, procedures for possible emergency evacuation from the area or country.

☐ 4. CHECK-IN PROCEDURES

Specify check-in procedures for the assignment:
Regularity and times (whether multiple locations, long travel, etc., for each location and travel segment); when indicating time, specify both the time in the area of travel and the time at location where the security check-in person is based.

Method (phone call from landline/cell/sat phone; text messaging; e-mail)
The individuals responsible for security check-in. (When designating such people, consider appropriate time zones, as well as the level of risk associated with the assignment, the volatility of the situation of the ground, and your team's experience performing check-in tasks; if appropriate, designate different team members for different parts of the assignment.)

Procedure for action in case you or your team does not check in. The usual security interval for check-ins is one hour, meaning follow-up action will be taken if after one hour from specified check-in time contact with the team has not been established. Indicate whether a certain segment of the assignment (e.g., border or checkpoint crossing) would require a shorter interval. In addition, specify:

- If an associate is responsible for receiving check-ins, at what point he or she should notify the supervisor;
- If and when the news organization should attempt to reach emergency contacts on the ground;
- What further action the news organization should or should not take (which may include notifying relatives, notifying other media, or contacting the embassy).

☐ 5. CONTACTS

Provide contact information (mobile and landline phone numbers, email addresses) for the following:

- Staff traveling on the assignment
- Staff conducting check-ins
- Supervisors and other back-up contacts in headquarters
- Non-staff participants (consultants, interpreters, drivers)

☐ 6. EMERGENCY CONTACTS

Contacts in-country: (a) indicate a designated in-country security contact (a trusted colleague, for example) who will be kept regularly informed of your plans, movements, and locations; (b) provide a list of additional contacts in the country who would be able to assist the news organization in case of a security incident, loss of contact with the team, or other emergency situation (these may include contacts in relevant embassies, U.N. or humanitarian staff, local NGOs, friendly local officials, and law enforcement authorities).

Other emergency contacts: If available, provide other contacts who would be able to assist the news organization in case of a security incident, loss of contact with the team, or other emergency situation.

Acknowledgments

CPJ wishes to thank the following journalists and experts for their valuable contributions to this guide: Mustafa Haji Abdinur, Molly Bingham, Umar Cheema, Carolyn Cole, Bill Gentile, Eric S. Johnson, Sebastian Junger, Rebecca MacKinnon, Judith Matloff, Fabio Pompetti, David Rohde, David Schlesinger, and Javier Valdez Cárdenas. CPJ also gratefully acknowledges the vital research done by the International News Safety Institute, the Dart Center for Journalism & Trauma, Human Rights Watch, and numerous local and international journalism organizations. The Associated Press, Agence France-Presse, and Reuters provided photo services.

The publication of this guide was made possible by grants from the Adessium Foundation, the Omidyar Network, and the RealNetworks Foundation.

Editorial Director: Bill Sweeney
Senior Editor: Elana Beiser
Deputy Editors: Kamal Singh Masuta, Shazdeh Omari
Designer: John Emerson
Chief Researcher: Casey Nitsch
Researcher: Faye Steinhauser
Copy Editor: Camille Rankin
Video Producer: Dana Chivvis

About the Authors

Frank Smyth, the main author of this guide, is CPJ's senior adviser for journalist security. Smyth is a veteran journalist who has specialized in armed conflict, organized crime, and human rights. He has reported from nations worldwide, including El Salvador, Guatemala, Colombia, Eritrea, Ethiopia, Rwanda, Sudan, Jordan, as well as Iraq, where he was imprisoned for 18 days in 1991. Through the 1990s, Smyth investigated arms trafficking for Human Rights Watch. He has reported for CBS News, and written for *The Nation*, *The Village Voice*, *The New Republic*, *The Washington Post*, *The New York Times*, *The Wall Street Journal*, *The International Herald Tribune*, *World Policy Journal*, and *Foreign Affairs*. Smyth has testified on press freedom matters before the Organization of American States, the International Commission of Jurists, and the U.S. Congress. Smyth is the founder and executive director of Global Journalist Security, a firm that provides consulting and training services to journalists and others. He blogs regularly on journalist security issues for CPJ.

Tom Lowenthal, CPJ's staff technologist in San Francisco, is responsible for the latest work on the Technology Security chapter of the guide. Tom has a special interest in operational security and grassroots surveillance self-defense. A strong believer in individual privacy and personal freedom, Lowenthal has worked as project coordinator at the Tor Project and as a technologist on Mozilla's privacy and public policy team. He is also a freelance journalist, and has written for Ars Technica on security and tech policy. He earned his bachelor's in political theory, with minors in computer science and technology policy, from Princeton University. The fingerprint of his GPG public key is 1ADE 9951 1A97 95FA 3557 53DC 51E7 1B75 4A09 B187.

Danny O'Brien, who wrote the first edition of the Technology Security chapter, served as CPJ's Internet advocacy coordinator from 2010 to 2013. O'Brien is international director of the Electronic Frontier Foundation and has been at the forefront of the fight for digital rights worldwide. He was an original staff member for *Wired UK* magazine and co-founded the Open Rights Group, a British digital rights organization. He has also worked as a journalist, covering technology and culture for *New Scientist*, *The Sunday Times of London*, and *The Irish Times*.