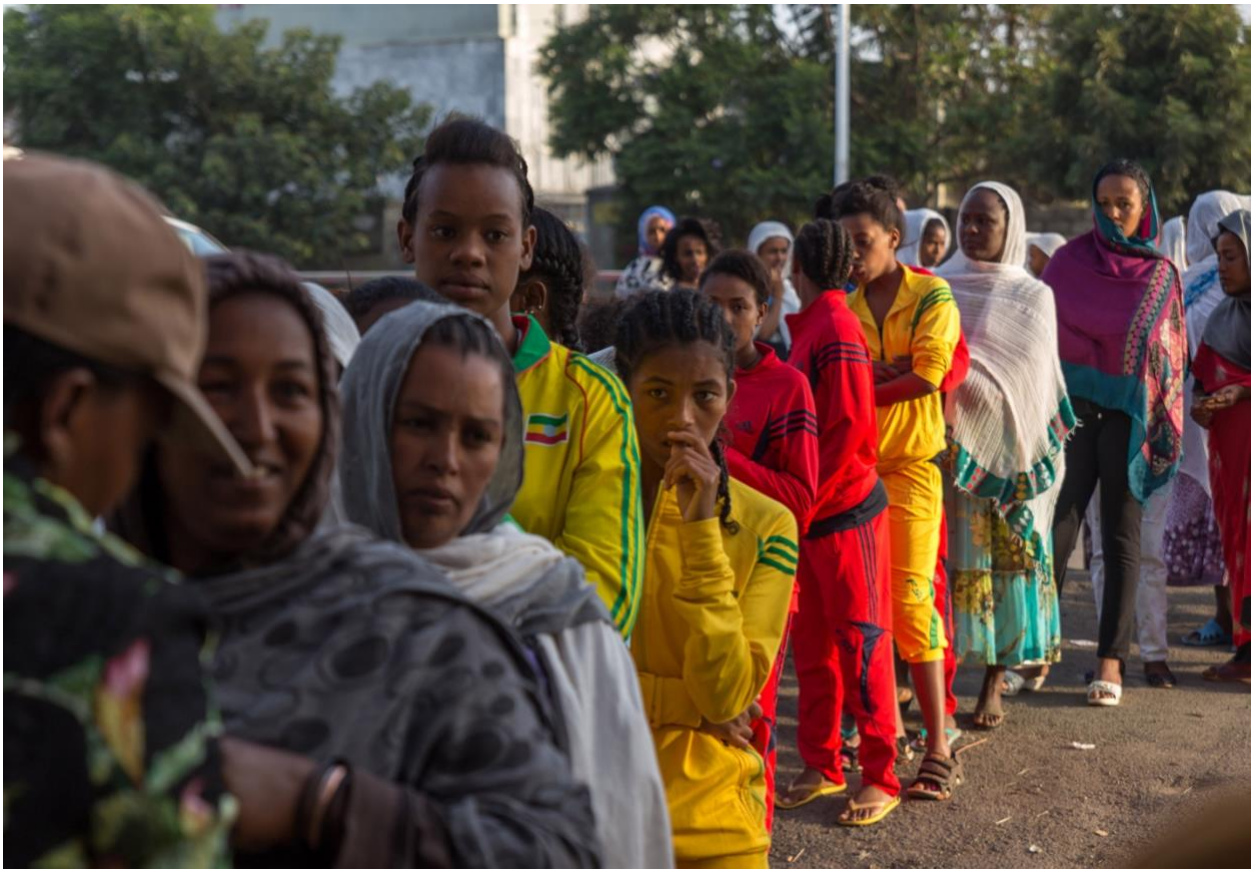
Committee to Protect Journalists

Ethiopia elections 2021: Journalist safety kit

Ethiopia is scheduled to hold general elections later this year amid heightened tensions across the country. Military conflict broke out in the Tigray region in November 2020, and is ongoing; over the past year, several other regions have witnessed significant levels of violence and fatalities as a result of protests and inter-ethnic clashes, according to media reports.



Voters line up to cast their votes in Ethiopia's general election on May 24, 2015, in Addis Ababa, the capital. Ethiopians will vote in general elections later in 2021. (AP/Mulugeata Ayene)

At least seven journalists were behind bars in Ethiopia as of December 1, 2020, according to CPJ research, and authorities are clamping down on critical media outlets, as documented by CPJ and media reports. The statutory regulator, the Ethiopia Media Authority, withdrew the credentials of *New York Times* correspondent Simon Marks in March and later expelled him from the country, alleging unbalanced coverage. The regulator has sent warnings to media outlets and agencies, including The Associated Press, for their reporting on the Tigray conflict, according to media reports.

Journalists and media workers covering the elections anywhere in Ethiopia should be aware of a number of risks, including--but not limited to--communication blackouts; getting caught up in violent protests, inter-ethnic clashes, and/or military operations; physical harassment and

intimidation; online trolling and bullying; and government restrictions on movement, including curfews.

CPJ Emergencies has compiled this safety kit for journalists covering the elections. The kit contains information for editors, reporters, and photojournalists on how to prepare for the general election cycle, and how to mitigate physical and digital risk.

Contents

Contacts & resources

Journalists requiring assistance in Ethiopia can contact CPJ's Emergencies program via electionsafety@cpj.org or CPJ's Africa program at cpjafrica@cpj.org.

CPJ's resource center has additional information and tools for pre-assignment preparation and post-incident assistance.

Physical safety: General safety advice

- Research historic and current incidents of civil unrest/violent clashes in the area. If particularly severe, as recently witnessed in the Oromo Special Zone in Amhara state, consider the potential risks versus the editorial gain.
- Consider if your ethnicity, the ethnicity of those you are working with, or the affiliation of your media house may increase the chances of being targeted by locals or the authorities in the region you're working in.
- If driving to the location, find out if there has been any recent violence or security incidents along the way. For instance, the A2 highway passes through the Ataye area of Amhara, which is a known flashpoint for unrest. If the risk is high, consider flying instead, if feasible.
- Journalists flying should be prepared for increased scrutiny at airports, even for domestic trips, and always carry their accreditation documents and permits with them. In September 2020, a group of journalists were barred from flying to Mekelle from Addis Ababa, to cover an election that was deemed illegal by the federal government.
- Communication blackouts have been described as a 'go to tool' of the authorities, and present a clear operational hazard on the ground as well as serious challenges to reporting, journalists tell CPJ. Consider how you will communicate and keep abreast of developments under such circumstances.
- Ethiopia restricts the importation of satellite phones, with Ethiopian law criminalizing the use of unapproved telecommunications equipment, and they could *potentially* be monitored by the authorities. Journalists must obtain prior approval for their equipment during the accreditation process, though permission to bring in the satellite phones might be difficult to obtain.
- Minor and side roads in Ethiopia can be challenging and treacherous in places, especially in the wet and in mountainous areas. If you need to drive on such roads, use a robust vehicle with good ground clearance and a competent driver.
- Parts of Ethiopia are located more than 2,500 meters (8,200 feet) above sea level. If visiting such an area allow yourself sufficient time to acclimatize, keep hydrated, and avoid rushing around.
- If arranging overnight accommodation, note that a number of hotels have been targeted by hand grenades and bombs in the past, including the Grand Hotel Resort (Bahir Dar); the Sokiele Hotel (Nekemte); and the Florida International hotel (Gondar). Research any security at the hotel, who it is owned by, and the potential risk of being targeted (e.g. a Tigrayan-owned hotel in Amhara may be at an increased risk).

- Find out who is likely to be at the event, and assess the likelihood of violence based upon any upcoming announcements or local/regional issues that could trigger unrest. **Be aware that violence can occur, escalate, and spread with little warning throughout Ethiopia.**
- Ensure that you have obtained the correct accreditation or press identification:
    - Foreign nationals should consult the relevant Ethiopian embassy/consulate regarding both visas and Ethiopian Media Authority permits, including for any equipment you plan to take with you.
    - The National Election Board of Ethiopia will issue additional accreditation for both local and international journalists.
    - Media workers may require additional documentation from regional and federal authorities to access certain parts of the country.
    - Be aware that the accreditation process for foreign journalists can take a long time -- some journalists who spoke to CPJ in mid-May said they had been waiting for weeks for their approvals to travel to Ethiopia.

Physical safety: Reporting from political rallies & crowd events

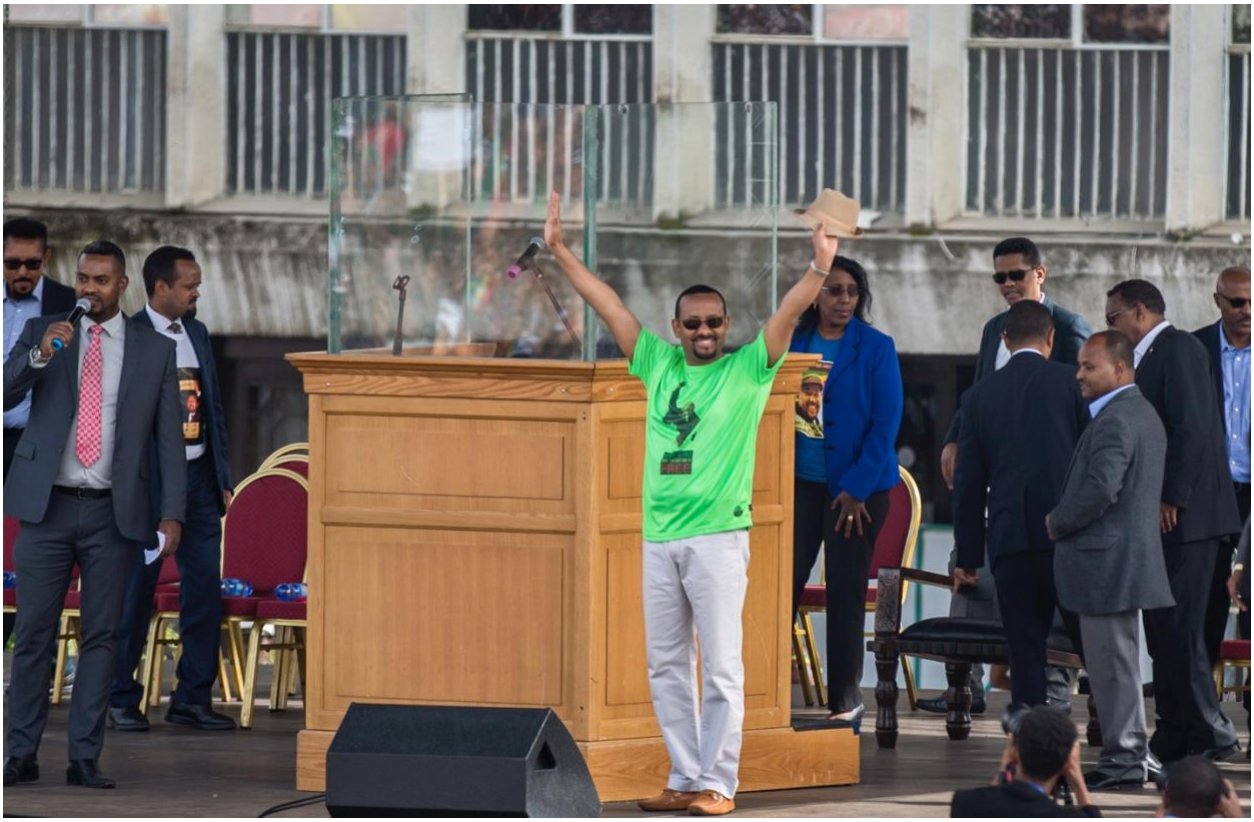
Media workers should be aware of the danger of getting caught up in and affected by unrest and/or violence when attending political rallies, crowd events, or election-related protests -- especially in woredas (districts) and zones where inter-ethnic tensions exist and where armed groups and militias are known to operate.

To help minimize the risks, media workers should consider the following safety advice:

On the ground

- Ethiopia's main rainy season, the Kirimet, typically begins in June. Take wet weather gear with you and protection for equipment if working in the open.
- If reporting at an outdoor event, consider the time of day and exposure to the sun. Note that you may be waiting for some time before an event starts. Keep hydrated, wear a sun hat, and apply sunscreen if necessary.
- Consider taking a variety of personal protective equipment (PPE) if any violence is anticipated. For more information, see **CPJ's PPE guide (English only)**.
- If the crowd or police might be or become hostile toward the media, avoid clothing with media company branding and remove media logos from equipment/vehicles if necessary.
- Wear sturdy footwear with hard soles, laces, and some kind of ankle support. Avoid wearing sandals or slip-on shoes.
- Working with a colleague is sensible, so consider going with another reporter or photographer if possible, noting that election events may finish late into the evening. After dark the risk level increases.
- **Display your press accreditation if safe to do so.** Avoid using a lanyard around your neck. Instead clip it to a belt or in a transparent velcro pouch around your bicep.
- Try to gauge the mood of the crowd. If possible, call other journalists already at the event to assess the atmosphere. If the crowd is hostile, mentally prepare for verbal abuse. Do not react to the abuse and avoid engaging with the crowd.

- Identify the closest point/location of medical assistance.
- If the task was difficult/challenging, do not bottle up your emotions. Tell your superiors and colleagues. It is important to discuss and speak about any challenging experiences and recognize that everyone learns from each other.



Ethiopian Prime Minister Abiy Ahmed waves to the crowd at a rally in his support in the capital, Addis Ababa, Ethiopia, on June 23, 2018. (AP/Mulugeta Ayene)

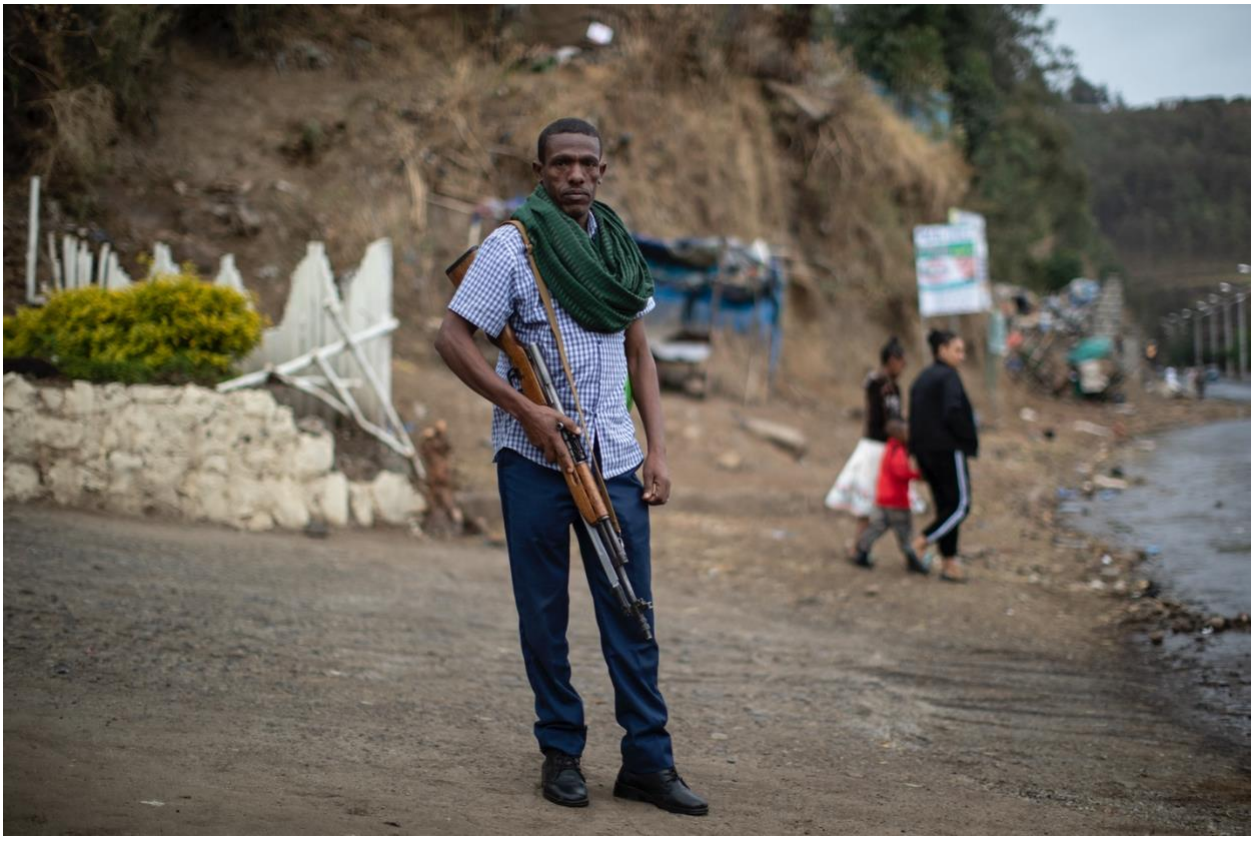
Positioning & situational awareness

- Remain alert to speeding vehicles or motorbikes approaching the location, which could be used to target the crowd and/or political candidates from. Note that a hand grenade was thrown at an Abiy Ahmed political rally in 2018.
- Regularly assess your position in relation to political candidates and the crowd at public events, noting the danger of potential stampedes. Try to keep to the periphery of the crowd and continually assess all available escape routes. If the crowd starts jostling or becoming unruly, fall back to a safe location and continue to monitor escape routes.
- Avoid getting caught in the crowd if political candidates--who could be targeted by hostile individuals--move among the audience. If you intend on asking a candidate a question, do so from a safe distance, if feasible.
- Regularly monitor the crowd for individuals who may present a threat. Pay attention to how people are behaving and if/how they are communicating with others. Trust your instincts, and maintain a safe distance behind or to the side of any suspicious individuals.
- Pay attention to vehicles parked close by and any individuals in or around them for signs of suspicious activity.

- Remain alert to the threat of pickpockets while working in or close to a crowd, especially in areas where petty crime is known to be a problem.
- Have an escape strategy in case circumstances turn hostile. Try to plan this in advance of arrival, if feasible. Report from a secure location such as a press holding area (if there is one), taking into account the distance from all available exit routes.
- If working with others, identify an emergency rendezvous point. Regularly assess the safety of all routes leading to this point.
- Park your vehicle facing the direction of escape in an accessible and secure location, or ensure you have an alternative guaranteed mode of transport.
- Avoid hanging around and/or questioning people if the crowd becomes hostile.

Physical safety: Working in areas of civil unrest & remote locations

Violent clashes, civil unrest, and military operations have occurred across Ethiopia since Prime Minister Abiy Ahmed came to power in 2018, with hate speech and disinformation helping reignite historic distrust and flame tensions between ethnic and political groups. Other typical triggers of localized or regional unrest include land disputes, grazing rights, student protests, and religious conflict.



An Amhara militia member poses for a photograph in Gondar, in the Amhara region of Ethiopia, on May 2, 2021. (AP/Ben Curtis)

Understanding what is driving the unrest and the dynamics at play is essential in helping identify and mitigate the myriad of risks on the ground. Is it a sporadic flare-up due to disputed regional borders (as recently witnessed in Somali and Afar); religiously motivated attack (as recently

witnessed in Oromia); or simmering inter-ethnic tension (as recently witnessed in Dire Dawa and Harar)?

Media workers should be aware that any location can witness a sudden outbreak of violent unrest, be it in a large city or a remote woreda, and often with little or no warning.

Advance planning

- Always ask about the feasibility of accessing an area affected by unrest, noting that security forces or local militias may block access during periods of tensions and conflict.
- Research the various security forces and militia groups who operate in the area. Find out what uniforms they wear, their likely attitude toward the media, and typical tactics used on the ground. Such forces may include:
  - Ethiopian National Defence Force (ENDF)
  - Regional/state police forces
  - Separatist militias (e.g. Oromo Liberation Army)
  - Foreign military (e.g. Eritrean)
  - State special police (e.g. Somali Regional State Special Police)
- Consider your profile, ethnicity, gender, and previous work—and that of intermediaries you may be working with (e.g. drivers, translators). Do such factors increase the chances of being monitored and/or targeted by local people, the security forces, or militia groups?
- Try to establish trusted contacts on the ground who can provide advice/assistance during your assignment. If working in a particularly dangerous area, consider the need for extra support or working alongside the authorities (**if considered safe to do so**).
- If a foreign national working in a remote location such as the northern Afar region, research the risk of kidnaping and/or targeted killings, as per incidents witnessed in 2007, 2012, and 2017.
- Individuals should not be expected to work alone in remote locations and areas experiencing unrest. Journalists should work with somebody who speaks the local language in the region in order to help avoid communication issues on the ground.
- If violent unrest is expected, the use of protective safety goggles, helmets, tear gas respirators, and protective body vests should be considered, depending on the range of threats. For more information, see **CPJ's PPE guide (English only).**
- Ensure a colleague, friend, or family member knows where you are heading to and when to expect you back. It is recommended to set up a check-in schedule along with an action plan if a check-in doesn't happen at a designated time, **taking into account that communications blackouts can happen with little or no warning.**
- Research the layout of the location, and identify key flashpoints/landmarks that unrest may center around (e.g. a town square, a monument, or a particular building).
- Assess the routes in/out of the location for dead ends or choke points. Be fluid with your plans and prepared to adapt your itinerary accordingly.
- Have a legal representative who you can contact in case of detention, noting that journalists and translators can be arrested without charge, as documented by CPJ.
- Maintain a flexible itinerary, noting that a number of journalists have been stopped in recent months at Bole international airport and prevented from flying, according to media reports and to sources CPJ spoke to who asked to remain anonymous for security reasons.

- Identify all local medical facilities. If working in Tigray, note that approximately 70% of health facilities have been vandalized, according to Médecins Sans Frontières (MSF).

Transportation & equipment

- Plan all journeys according to local movement restrictions, which may be prohibited during certain hours (as seen in Karat, in Konso Zone in the Southern Nations, Nationalities and Peoples regional state). Note that journalist Dawit Kebede Araya was shot and killed in Mekelle in January 2021, as documented by CPJ. Though the motive for his killing remains unclear, local officials suggested he had broken the curfew.
- Know the terrain you will be covering, which can vary from muddy tracks to scorching desert to rocky piste to mountain passes. Always use an appropriate vehicle and competent driver, with equipment and provisions in case you get stuck or break down.
- Plan alternative routes where feasible, noting the risk of road closures and roadblocks during civil unrest (***see checkpoints section below***).
- Work out the approximate journey duration and an expected arrival time. Do not rely on apps to determine driving time/distance. Source reliable local information instead.
- If a check-in procedure is deemed necessary, communicate any change of itinerary to your management team or trusted contact in good time.
- If arriving at an airport or bus station, it is advisable to use a trusted driver from the area to meet you on arrival and during the assignment.
- Wherever possible use a vehicle that blends in at the location (e.g. an expensive SUV is likely to attract more attention, particularly in less well-off and rural areas).
- Take a comprehensive first aid/trauma kit with you, especially when in remote locations.
- Always park in a well-lit and busy area, facing the direction of escape. Conduct a visual inspection of the vehicle exterior before departing, and more frequently if/when driving on challenging roads.
- Routinely check your rear view and side mirrors. If you suspect you are being followed, trust your instincts and drive to a place of safety as soon as possible.
- Avoid travelling at night unless absolutely necessary, and plan your journey to arrive at your destination during daylight hours.
- Limit the number of valuables you take. Do not leave any equipment in vehicles, which are likely to be broken into. After dark, the criminal risk increases.
- Ensure that vehicle doors are locked and windows are kept up when driving in slow traffic, and while at junctions/traffic lights, noting the risk of petty crime and robbery.
- If travelling by public bus/coach, be aware that petty crime can be a risk and vehicles can be targeted by bandits.

Location safety & awareness

- Identify key buildings and/or landmarks that could be a flashpoint for violence, which may include mosques, churches, or government buildings.
- Minimize time on the ground as much as possible. Get what you need and move on.
- It is sensible to maintain a low profile throughout the assignment, avoiding any overt displays of wealth or attracting undue attention.
- Avoid working in quiet, poorly lit and/or remote locations, especially after dark, when the risk level increases.

- If working in the same location for a period of time, try to vary your daily routine as much as possible. Behave purposefully and with confidence. Try and avoid being distracted on the go (e.g. using your phone).
- When out and about, pay constant attention for individuals who could be monitoring you. If meeting in a public place, such as a restaurant or hotel, avoid sitting near windows where you can be more easily monitored. Remain alert to vehicles pulling up, who is coming in/out of the building, and individuals hanging around outside. Identify who might be able to assist you if necessary. Pay attention to individuals taking photos or following you, whether on foot or in a vehicle.
- Where possible it is recommended to stay at overnight accommodation with some form of security. Always identify all available escape routes from the property, and try to avoid staying in rooms at the front of the building.

Checkpoints

Checkpoints operated by the military, police forces, and local militias can be a common sight along Ethiopian highways and roads, especially in areas of civil unrest and military operations.

Be aware that NGO vehicles and employees have recently been targeted at checkpoints and roadblocks, including workers for MSF in Tigray and Irish aid agency GOAL in Benishangul-Gumuz. In addition, CNN recently reported that Eritrean troops manning a checkpoint had blocked its news crew from accessing parts of Tigray, despite receiving permission from the Ethiopian military.

General safety

- Identify known legitimate checkpoints along your route in advance.
- Try and find out the location of any unofficial checkpoints by contacting trusted contacts such as local journalists. Plan your route to avoid them (if feasible).
- Avoid driving in areas where unofficial checkpoints are known to be a problem, especially after dark when the prevalence of checkpoints and level of risk increases.

Best practices

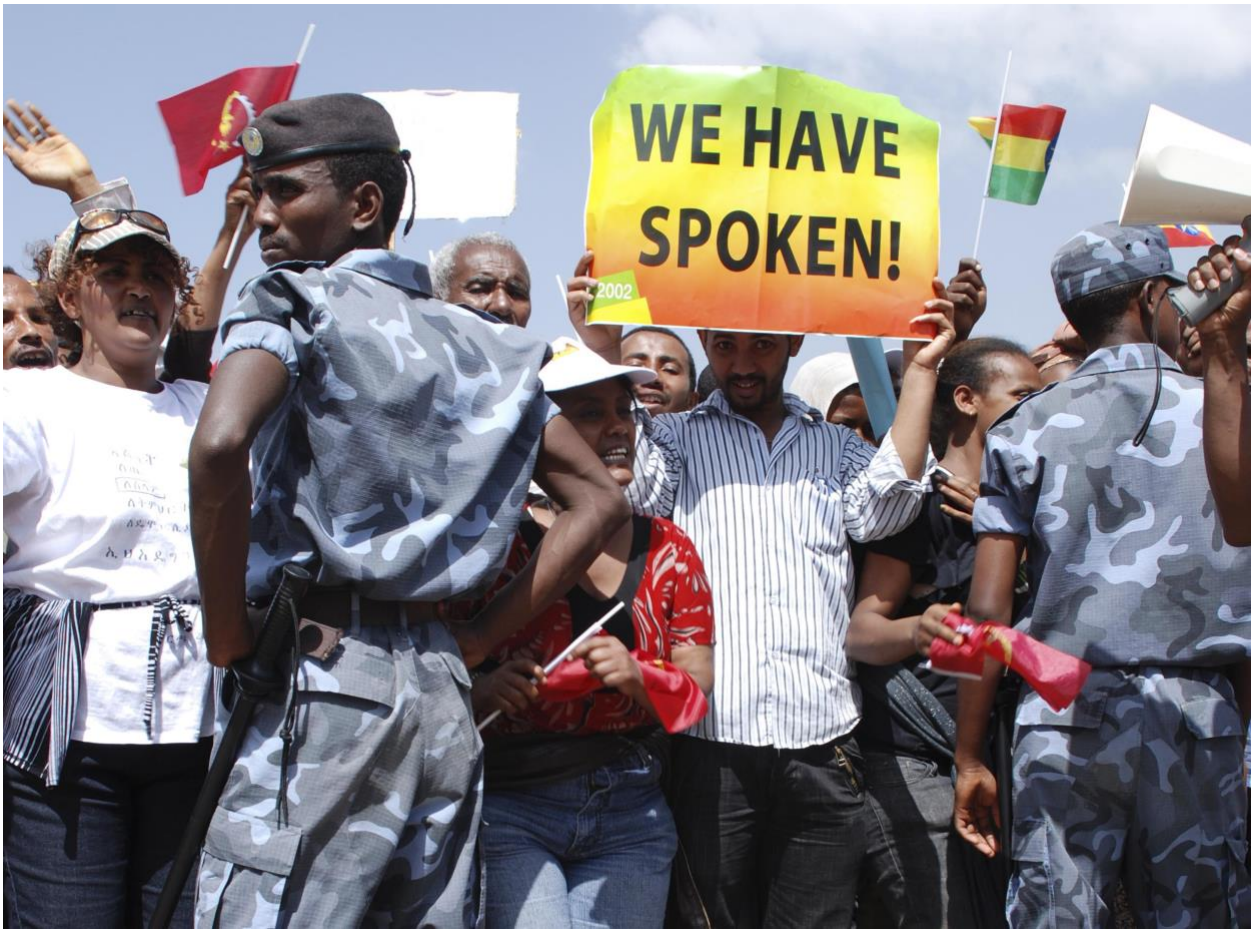
- Slow down, indicate if pulling over, dim headlights (if at night), and park up where directed to do so.
- Keep your hands visible at all times, and turn on the interior light (if dark).
- Keep windows closed until asked to open them.
- Do not use any devices such as mobile phones.
- Keep equipment out of sight such as laptops and cameras. If asked, mention that you have them in the vehicle.
- Have all travel and vehicle documents to hand (e.g. passport, driving license, vehicle insurance policy).
- If wearing sunglasses and/or a hat, take them off.
- Stay calm, maintain eye contact, a confident posture, and engage in a positive manner. Comply with instructions, and always be polite and courteous.

You should avoid

- Accelerating, swerving, or trying to turn off the road.

- Shouting or become hostile to an individual.
- Turning your back on an individual if they are still talking to you.
- Using confrontational body language (e.g. pointing or folded arms).

Physical safety: Reporting from election-related protests



Tens of thousands of ruling party supporters rally on May 25, 2010, in Addis Ababa, Ethiopia, to celebrate victory in the national election. (AP/Anita Powell)

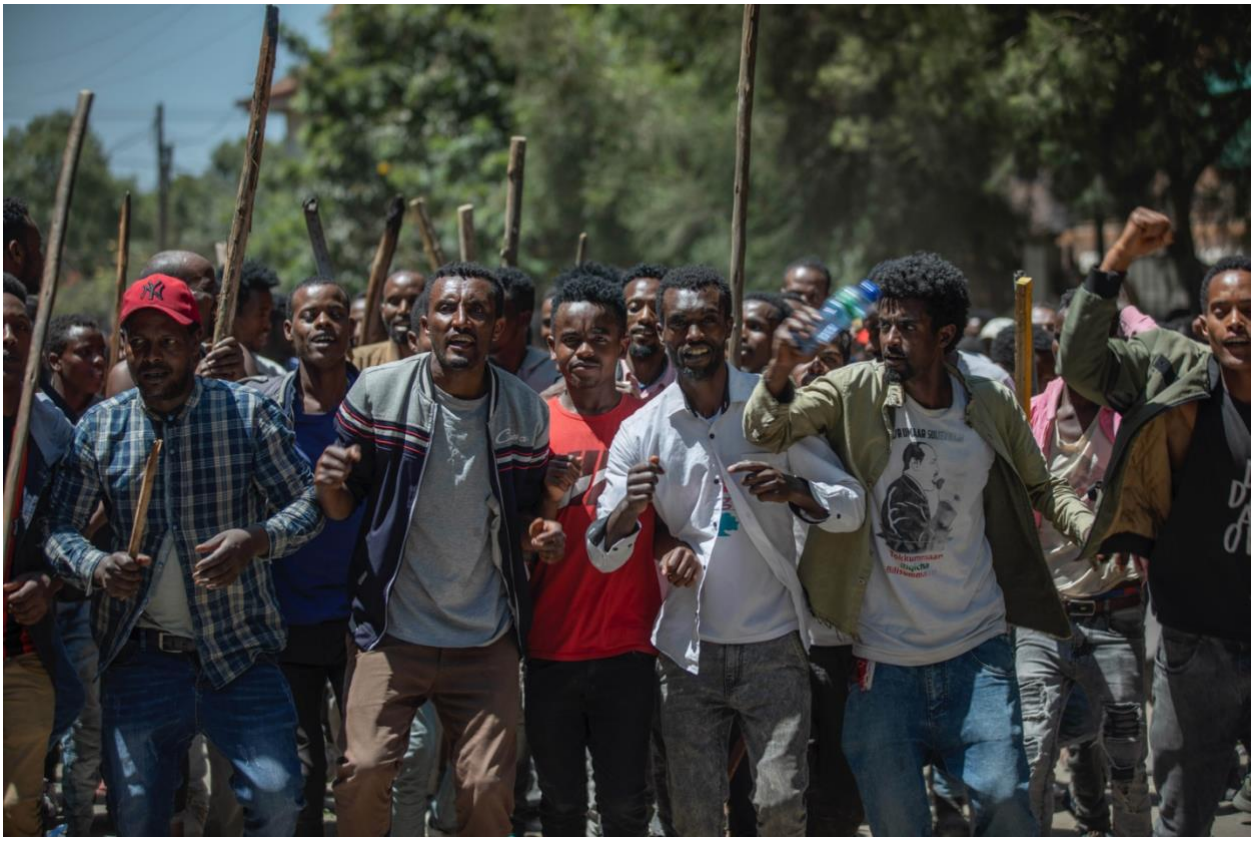
Crowd demonstrations can occur during any election cycle and can quickly turn deadly, as previously witnessed in Ethiopia in 2006. Media workers covering such protests can be exposed to a range of dangers if violence breaks out between protesters, counter-protesters, and the security forces, who are known to use live ammunition and tear gas to disperse crowds. In conflict zones such as Tigray, the risk of light weapons being used cannot be ruled out.

To help minimize the risk, media workers should consider the following safety advice:

Planning

- Identify the material you require for your report. Lingering at a protest gathering material that will not be used increases the risk of harm.
- If violence is anticipated, the use of protective safety goggles/glasses, helmets, tear gas respirators, and protective body vests should be considered, depending on the range of threats. For more information see **CPJ's PPE guide (English only).**

- Research the layout of the location in advance by studying a map of the immediate area. Identify all potential safe exit routes in case you need to escape, which streets/roads are dead ends in order to avoid going down them, as well as an emergency rendezvous point if you are working with others.
- Individuals should not be expected to work alone at protest locations. Try to work with a colleague and set up a regular check-in procedure with your base, family, or friends. Working after dark is riskier and should be avoided if possible. For more information, please see **CPJ's advice for journalists reporting alone.**



A group of supporters perform and shout slogans at the house of opposition leader Jawar Mohammed to show their support, in Addis Ababa, Ethiopia, on October 24, 2019. (AP/Mulugeta Ayene)

Clothing & equipment

- Avoid wearing military style patterns, loose clothing, political slogans, media branding, and flammable materials (e.g. nylon).
- Wear sturdy footwear with hard soles, laces, and some kind of ankle support.
- Fix long hair into a bun or a low braid that can be tucked into clothing. This will prevent individuals from pulling you from behind. Avoid wearing chains, lanyards, or jewelry around your neck for the same reason.
- Take a medical kit if you know how to use it, and ensure you have a full battery on your mobile phone. If this is not feasible, try and take a portable power bank and a charger with you.
- Only carry the minimum amount of equipment with you as necessary, which will help keep you agile and won't weigh you down if you need to move quickly.
- Limit the number of valuables you take. Do not leave any equipment in vehicles, which may be broken into. After dark, the criminal risk increases.

Positioning & situational awareness

- Consider your position and maintain situational awareness at all times. If feasible find an elevated vantage point that might offer greater safety.
- Try to maintain a safe working distance from buildings as well as vehicles, noting the dangers associated with looting, vandalism, and arson (e.g. falling debris, smashed glass, and fire).
- If working close to a crowd, keep to the periphery and avoid being sucked into the middle, where it is hard to escape. All journalists should be conscious of not outstaying their welcome in a protest crowd, which can turn hostile quickly.
- Continuously observe and read the mood and demeanor of the authorities in relation to the crowd dynamic. Police can become more aggressive if the crowd is agitated (or vice versa). Visual cues such as the appearance of police dressed in riot gear or throwing of projectiles are potential indicators that aggression can be expected. Pull back to a safe location, or plan a quick extraction when such 'red flags' are evident.
- Photojournalists generally have to be in the thick of the action so are more at risk. Consider having someone watch your back, remember to look up from their viewfinder every few seconds to assess your position, and avoid wearing the camera strap around your neck to prevent strangulation or being pulled to the ground. Photojournalists often do not have the luxury of being able to work at a distance, so it is important to minimize the time spent in the crowd. Get your shots and get out.
- Identify the closest point of medical assistance.

Dealing with tear gas

The use of tear gas can result in sneezing, coughing, spitting, crying, and the production of mucus that obstructs breathing. In some cases, individuals may vomit, and breathing may become labored. Such symptoms could potentially increase media workers' level of exposure to coronavirus infection via airborne virus droplets. Individuals who suffer from respiratory issues like asthma, who are listed in the COVID-19 vulnerable category, should therefore avoid covering crowd events and protests if tear gas is likely to be deployed.

In addition, evidence suggests that tear gas can actually increase an individual's susceptibility to pathogens such as coronavirus, as highlighted by NPR.

For further guidance about dealing with exposure to and the effects of tear gas, please refer to CPJ's civil disorder advisory.

Physical harassment and assault

When working on the ground, media workers should consider the risk of physical assault from both protesters and the security forces, as highlighted in the case of Reuters photographer Tiksa Negeri. When dealing with aggression, consider the following the safety advice:

- Assess the mood of protesters toward journalists before entering a crowd, and remain vigilant for potential assailants. If the crowd is hostile, retreat to a safe location as soon as possible.
- Read body language to identify an aggressor/s, and use your own body language to pacify a situation.

- Maintain eye contact with an aggressor, use open hand gestures, and keep talking in a calming manner.
- Keep an extended arm's length from the threat. Back away and break away firmly without aggression if held. If cornered and in danger, shout.
- If aggression increases, keep a hand free to protect your head and move with short deliberate steps to avoid falling. If in a team, stick together and link arms.
- While there are times when documenting aggression is crucial journalistic work, be aware of the situation and your own safety. Taking pictures of aggressive individuals can escalate a situation.
- If you are accosted, hand over what the assailant wants. No equipment or money is worth your life.

Physical safety: Reporting in a hostile community

During the election cycle, media workers may be required to work in areas or among communities that are hostile to the media or outsiders. This can happen if a community wants to hide illicit activities (e.g. arms or human migrant trafficking). Such communities can therefore view journalists as a threat that could potentially expose them. Others may believe that the media does not fairly represent them or portrays them in a negative light.

To help reduce the risks

- Be aware that certain communities in Ethiopia have their own local laws and/or their own militias (e.g. parts of the Omo Valley, remote parts of the Afar and Somali regions). If working in such a location you should thoroughly research the local laws, customs, and rules to prevent any issues on location.
- Always secure permission to access such communities in advance, noting that turning up without an invitation or someone vouching for you can cause problems. Try and ascertain what the likely reaction to the media will be by researching the community and their views in advance. Adopt a low profile if necessary.
- Note the dangers associated with disinformation being spread in the community, which could lead to hostility and/or mob attack, as witnessed with the fatal attack on researchers in West Gojjam Zone in Amhara in 2018.
- It is sensible to hire a local facilitator, community leader, or person of repute in the community who can accompany you and help coordinate your activities. Identify a local power broker who can help in case of an emergency.
- If there is endemic abuse of alcohol or drugs in the community, or a high crime rate, be aware that the unpredictability factor increases.
- If a community is particularly high risk, consider wearing a covert protective body vest.
- Ideally work in a team or with backup. Depending on the risk level, the backup can wait in a nearby safe location (e.g. a petrol station) to react if necessary.
- Think about the geography of the area and plan accordingly. Consider the need for security if the risk is high. A local hired 'backwatcher' to protect you/your equipment can be attuned to a developing threat while you are concentrating on work.
    - Park your vehicle in the direction of escape, ideally with the driver in the vehicle ready to go.

  - If you have to work remotely from your transportation, know how to get back to it. Identify landmarks and share this information with colleagues.
  - Know where to go in case of a medical emergency, and work out an exit strategy.
- Always ask for consent before filming/photographing an individual. Be respectful to the individuals and their beliefs/concerns at all times.
- Avoid working in a hostile community at night, when the risk level increases dramatically.
- When you have the content you need, get out and do not linger any longer than necessary. It is helpful to have a pre-agreed cut off time and to depart at that time. If a team member is uncomfortable, do not waste time having a discussion. Just leave.
- Wear clothing that is appropriate and respectful, without media company branding. Remove media logos from equipment/vehicles if necessary.
- Limit the amount of valuables/cash that you take. Will thieves target you and/or your equipment? If accosted, hand over what they want. No equipment is worth your life.
- Take a medical kit if you know how to use it.
- Before broadcast/publication consider that you may need to return to this location. Will your coverage affect your welcome if you return?

Physical safety: COVID-19 considerations

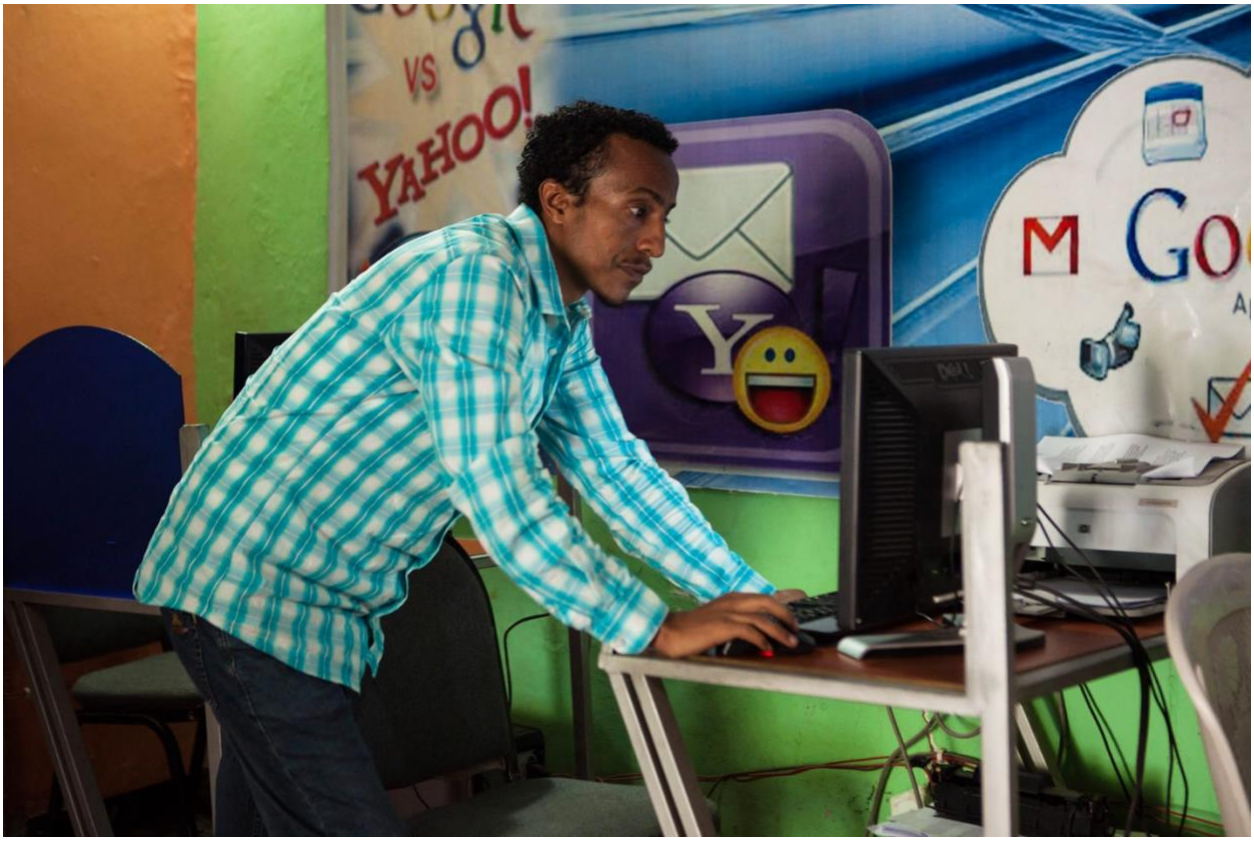
Large crowds are commonplace at election events and/or related protests, where maintaining physical distancing measures will be challenging. Members of the public may not wear face coverings/face masks, and media workers could be confined to a particular area in close proximity to other journalists. Such confinement could potentially expose them to virus droplets, as well as verbal or physical attacks from hostile members of the public, who could cough or sneeze over them.

Be aware that people shouting or chanting can result in the spread of virus droplets, therefore increasing media workers' level of exposure to coronavirus infection.

- Be aware that COVID-19 restrictions and/or curfews could potentially be used as an excuse to limit access/movement in locations the authorities don't want you to visit.
- Always research what COVID-19 restrictions are in place where you will be reporting from. Restrictions are likely to vary at a local and regional level, and may change with little or no notice. The Ethiopian Ministry of Health provides updates on the status of COVID-19 in the country through its website and social media channels. In addition, The Africa Centres for Disease Control and Prevention, an African Union institution, provides information on travel restrictions and requirements, including to Ethiopia, while information published by the state-owned Ethiopian Airlines might be useful to travelers, even if they are using other airlines.
- If travelling internationally to cover the Ethiopian elections you may be required to provide evidence of a recent COVID-19 test, and/or need to quarantine on arrival. Always check the latest requirements in advance.
- Wearing a good quality face mask is essential at any crowded event or protest (i.e. N95 / FFP2 standard or higher). Note that the implementation of strict measures regarding wearing face masks is likely to vary at a local level.

- Ensure you wash your hands regularly, properly, and thoroughly as often as feasible throughout the assignment. Ensure hands are dried in the appropriate way. Use alcohol-based hand sanitizer regularly if you can't wash your hands, but try not to make this a substitute for a regular hand washing routine.
- All equipment should be thoroughly cleaned post-assignment.
- All clothing and shoes should be removed before re-entering your home and washed/cleaned with hot water and detergent where possible.

For further detailed COVID-19 reporting guidance, please see CPJ's COVID-19 safety advisory (Amharic version)



Kaleb Alemayehu, the owner of an internet cafe in Adama, southeast of the capital Addis Ababa, checks a computer on April 4, 2018. (AFP/Solan Kolli)

Digital safety: General best practices

- Your online accounts hold a lot of information about you, your family, and your sources. Ensure that you secure your accounts by using long passwords of 15 characters or more and by turning on two-factor authentication (2FA). Regularly backup and delete content from your accounts. This will limit the data available to others should they gain access to your accounts. Learn more about securing accounts in the CPJ Digital Safety Kit (Amharic version).
- It's important to secure your devices to protect the data that is held on them. Lock your devices with a password or PIN. Ensure that you regularly update your operating system,

your apps, and your browsers. This will help better protect against malware and spyware. Backup your devices regularly to protect against losing content or data. Read more about device security in the CPJ Digital Safety Kit.

- Understanding which tools to use to communicate securely with others can be key to protecting you and your sources. Where possible, use end-to-end encrypted messaging apps, such as Signal or WhatsApp. All content, including calls, audio messages, documents, and photos, are encrypted in transmission and on the server. The CPJ Digital Safety Kit has more information on how to communicate securely with others.
- Be aware that any SMS or phone call via your cell phone company or landline is insecure and may be being monitored.
- Ensure that the websites you are visiting are encrypted by looking for https and a padlock icon at the start of every URL (https://cpj.org), ensuring that the traffic between you and the site is encrypted. Ensure that the website is authentic and not a spoof by also checking the spelling of the site.
- Spyware has been used to target Ethiopian journalists and dissidents, according to research by Citizen Lab. To better protect against it, journalists should update their devices, apps, and browsers on a regular basis. Read the section on phishing below for more details on how to protect against spyware.

Digital safety: Preparing your devices for political rallies

Taking steps to secure your devices and your data before covering a rally can reduce the possibility of others accessing information about you and your sources.

Best practices

- Ensure you have a full battery on your cell phone and take a portable power bank with you.
- Prepare your devices. Know what data is on your phone and your laptop and how that could put you or others at risk. Backup and remove information that you would not want accessed by others if your devices are stolen, confiscated, or broken.
- Secure your devices with a pinlock or password. Be aware that this may not stop authorities from being able to unlock it.
- Log out of and remove any apps from your phone that you will not use at the event
- Where possible use end-to-end encrypted messaging services, such as Signal or WhatsApp, to communicate with others. Be aware that phone conversations and SMS can be intercepted by law enforcement.
- Know what content is in your messaging apps and set up a process for regularly backing up and deleting content.
- Manage the contacts in your phones and messaging apps. Remove details of people you feel could put you or them at risk. Be aware that contacts are stored in apps and in the cloud, as well as on the SIM card.
- Set up your devices to remote wipe. If you are concerned you won't have time to remote wipe your devices if arrested or detained you should speak with a trusted contact about wiping them for you. A device will only wipe if it is connected to the internet or mobile data. Consider whether wiping your device will make you look more suspicious.
- If your devices leave your line of sight and are then returned to you at a later date they may have been infected with spyware. If possible, you should buy new devices. If this is not

possible, you should carry out a factory reset of your phone but be aware that it may not remove the spyware.
- If you are concerned about taking your personal phone to cover the event consider buying a cheap second phone and taking that instead.
- Encrypt your devices. See CPJ's guide on encrypting devices.
- Secure your accounts with two-factor authentication and long, unique passwords of 15 characters or more. Put passcodes on your devices instead of using biometrics. See CPJ's guide on securing accounts.
- Backup content from the event regularly when on the ground. This will prevent you from losing content if your devices are taken or broken.
- Be aware that live tweeting or live streaming your exact location at the event could put you at greater physical risk.
- Be vigilant for people who may wish to take, break, or steal your devices.

Digital safety: Preparing for a communication blackout

Communication blackouts in Ethiopia are common, especially during times of political unrest, as documented by CPJ. There was a nationwide shutdown in June 2020, and regional blackouts are common. Tigray has had an internet disruption since the outbreak of the armed conflict in November 2020, CPJ has documented. Communication blackouts can last from a few hours to months and may involve complete or partial blackouts. Working during a communications blackout can be complicated, but there are steps that journalists can take to prepare.

General digital security advice

- Secure your devices and limit the amount of information available on them to better protect you and your sources should you be detained while reporting during a shutdown.
- Use end-to-end encrypted messaging apps to contact others. End-to-end encryption means that content sent via the app, including calls, is encrypted and cannot be intercepted in transit. Examples include Signal or WhatsApp, companies that do not have access to the content of messages and therefore cannot be subpoenaed by governments. If you are unable to use these services because they are blocked then be aware that SMS and phone calls that go through a telecommunications company can be intercepted.

Preparing for a communication blackout

- Predict when an internet or communications shutdown will occur. This will likely include times of civil unrest, protests, and during election periods. Some regions of the country may be more prone to internet restrictions than others. Although the Ethiopian government has in the past imposed nationwide shutdowns, some recent regional disruptions were in Tigray and in western Oromia, according to reports.
- Speak with your newsroom and colleagues about planning for a complete shutdown. Create a plan detailing where and when to safely meet in person, and how you will document and transmit information to editors without using the internet. Consider sharing

landline contact details, but be aware that landline calls are insecure and should not be used for sensitive conversations. Plan how you will support colleagues who may be living and working in a region or area that is likely to be affected by a shutdown.

- Print out any documents or content from online sites that you might need in advance of a shutdown.
- Provide staff with USB drives or CDs for data storage during the shutdown.
- Identify people or services that may have access to the internet during an internet shutdown, for example embassy workers or banks. Contact them in advance to see if they will be able to access the internet for you.

Choose the right tools

Online tools and services are vulnerable to security breaches. Journalists are advised to stay up to date with the latest digital safety information especially when it comes to communication tools, such as messaging apps. The following advice is current as of May 2021.

- Download and set up VPN services to help you access blocked sites during a partial shutdown. Internet service providers frequently block VPNs, so it is recommended to have a number of options available. VPN use is not illegal in Ethiopia, however journalists should be aware that local authorities may interpret the law differently and use it to restrict VPN use. A VPN will not help you during a complete internet shutdown.
- Have more than one way to contact others. Downloading and setting up a variety of communications apps will mean that you can change between services should one become blocked. Be aware of the security vulnerabilities that may exist with different apps. For example, some services may require you to turn on encryption rather than it being the default. During an internet shutdown you may be forced to communicate via more insecure means, such as SMS, so be mindful of how you share sensitive data.
- Learn how you can share data using Bluetooth, WiFi Direct, and Near Field Communication (NFC). These methods allow you to pair your phone with another to transmit information, and do not need access to the internet. They can normally be found in the settings section of your phone. Practice using them before a shutdown occurs and understand their limitations when it comes to sharing files.
- Download and set up peer-to-peer messaging tools, such as Briar or Bridgefy. Briar is an end-to-end encrypted messaging app that works via internet, WiFi Direct, and Bluetooth. Bridgefy has fewer security features than Briar, but will work over longer distances.
- An international SIM card with roaming or a satellite phone can give you access to the internet. These options are expensive and journalists will require prior approval from authorities to import and use satellite phones in Ethiopia. Be aware of the security risks of using these services, especially with regard to location tracking. Foreign journalists using their cell phones in Ethiopia should be aware that their device will likely be connecting to the state-owned Ethio Telecom (ETC), meaning that the government will be able to track their location.

During a communications blackout

- Reporting during a shutdown may make you more vulnerable to being detained, depending on the circumstances. Ensure that your devices do not have any sensitive information on them that could put you or others at risk.

- Even if it is difficult to report in real time, you may still be able to document what is happening. Use USBs or CDs, encrypted if possible, to store data and hand it to colleagues and editors. Be aware that if information on these devices is not encrypted it could be accessed by the authorities if you are detained.
- Share files between devices using Bluetooth, WiFi Direct, or NFC (usually found under device settings). Be aware that transmitting data this way is not secure, and anything you use should be turned off immediately after use to avoid your device linking up with unknown devices nearby.
- Use peer-to-peer communication apps, such as Briar and Bridgefy. Be aware of the security risks of each one.
- Try to avoid using insecure communications methods, such as SMS or phone calls, for sensitive information during a shutdown. These communications methods can be intercepted or accessed by the Ethiopian government via the state-owned telecommunications provider.
- Android phone users can use F-Droid to download apps without needing a connection to the internet. Another option for Android is to use an APK file to install an app. These app files can be shared between devices without connecting to an app store, but are not subject to app store vetting, so only accept files from people you trust.
- Document the shutdown by taking screenshots of blocked sites. You can share this information at a later date with digital rights organizations in your country or internationally. Be aware that doing so may put you at risk.

After a communications blackout

- Speak with your newsroom or colleagues about what worked and what didn't when it came to preparing for a shutdown.
- Review your devices, backup and remove content to an external drive or to the cloud. Where possible, encrypt your data to keep it more secure.

Digital safety: Protecting against phishing

Phishing campaigns are likely to increase during an election period. Ethiopian dissidents, journalists, and media outlets have previously been targeted by sophisticated phishing attacks which led to commercial spyware being installed on their devices, according to Citizen Lab and Privacy International. Journalists covering the campaign should be extra cautious when dealing with documents and links sent via email and messages. Best practice advice is laid out below.

General best practices

- Always download software from the website of the service instead of downloading files or clicking on links sent to you via messages or email.
- Be wary of messages that urge you to do something quickly or appear to be offering you something that appears too good to be true, especially if they involve clicking on a link or downloading an attachment.
- Check the details of the sender's account and the message content carefully to see if it is legitimate. Small variations in spelling, grammar, layout, or tone may indicate the account has been spoofed or hacked.
- Verify the message with the sender using an alternative method, like a phone call, if anything about it is suspicious or unexpected.

- Think carefully before clicking on links even if the message appears to be from someone you know. Hover your cursor over links to see if the URL looks legitimate.
- Preview any attachments you receive by email; if you do not download the document, any malware will be contained. If in doubt, call the sender and ask them to copy the content into the email, or take screenshots of the document in preview instead of downloading it.
- Be cautious of links or documents sent via group chat. Chats with large numbers of people in them may be infiltrated by the authorities or others looking to target participants.
- Use the desktop version of apps to review messages and links if possible. A bigger screen helps you verify what you have received, and you're less likely to multitask.
- Upload suspicious links and documents to Virus Total, a service that will scan them for possible malware, though only those that are known.
- Enable automatic updates and keep all software on your devices up to date. This will fix known vulnerabilities that malware relies on to compromise your security.
- Stay particularly alert to phishing attempts during elections and periods of unrest or if colleagues or local civil society groups report being targeted.

Digital safety: Online abuse and misinformation campaigns

Journalists are likely to face an increased level of online harassment, including targeted attacks and misinformation campaigns directed against them, during election periods, especially if their reporting is construed as being too negative or too favorable of the government, as documented by CPJ. Both supporters and critics of the ruling party are very active online. Media workers reporting on Tigray should be aware that they are likely to face online abuse and accusations of spreading misinformation. Attacks are also likely to come from the Ethiopian diaspora who have set up and run orchestrated Twitter campaigns critical of the current government, according to a report by the nonprofit digital rights network Code for Africa. There are a number of steps that journalists can take to better protect themselves and their accounts.

To minimize the risk

- Secure your accounts with 2FA, long passwords of 15 characters or more, and a password manager, as described in the general best practice section. Don't reuse passwords.
- Search for your name using various search engines and remove data that you do not want available in the public domain.
- Review your social media accounts and remove or limit access to any personal data that can be used to verify your identity or locate you. Remove any contact details, such as personal phone numbers, that you do not want made public.
- Look through your accounts and remove any photos or images that could be manipulated and used as a way to discredit you.
- Monitor your accounts for signs of increased trolling activity or for indications that a digital threat could become a physical threat. See below for more details on what makes a greater threat. Be aware that certain stories are likely to attract higher levels of harassment.
- Speak with family and friends about online harassment. Online abusers often obtain information about journalists via the social media accounts of their relatives and social

circle. Ask family and friends to remove from or limit access to photos of you on their social media sites.

- If you can, speak with your editor about having a plan in place should you need to leave your home as a result of an online threat. If you are a freelance journalist, speak with colleagues about online abuse and setting up a support network to help you should you need it.

During an attack

- Try to ascertain who is behind the attack and their motives. This can help you gauge the risk of a physical threat.
- Look at your messages to see whether there is a high risk of a physical attack. The risk is deemed to be higher if data, such as your home address or phone number, is being circulated online. If you do not feel able to review your messages you should ask a colleague or trusted friend to do it for you.
- Document any comments or images that are of concern, including screenshots of the trolling and the time, the date, and the social media handle of the troll. This information may be useful at a later date if you wish to report the abuse to a social media company, your editor, organizations that defend freedom of expression, or, in some cases, the authorities.
- Inform your family, employees, and friends that you are being harassed online.
- Adversaries will often contact family members and friends as part of the harassment cycle.
- Blocking, muting, and restricting who can reply to your messages may be helpful steps to take, although this restricts your ability to interact with others online and may mean that you miss potentially threatening messages.
- Consider making most of your social media accounts private until the harassment has died down.
- Work with your newsroom to decide if and how you should respond to online harassment. It is not feasible or useful to respond to each message. However, during a misinformation campaign it may be helpful to have a message of support from your newsroom pinned at the top of your and their social media feed.
- Online harassment can be an isolating experience. Ensure that you have a support network to assist you. In a best-case scenario, this will include your employer. For more information about how to protect your mental health in the event of an online attack, consult CPJ's safety note.

Editor's safety checklist

Editors may require media workers to cover election-related events at short notice, and should always consider the increased level of risk when reporting from an event that could turn hostile, a remote location, or an area affected by inter-ethnic clashes or conflict. This checklist includes key questions and steps to consider to help reduce risk for staff.

Important: ***The following considerations should also be extended to local intermediaries, such as fixers, guides, translators etc.***

Staff considerations

- Are selected staff experienced enough for the assignment?
- Do any selected staff fall into the COVID-19 vulnerable categories or have family members/dependents who rely upon them? If so, have they been vaccinated with the required number of doses?
- Does the profile, ethnicity, or identity of any staff member make them a potential target? Does the political affiliation of the media house pose a potential risk to the journalists?
- Are selected staff fit enough and/or have any health issues that could affect them?
- Does the specific role of any selected staff put them at more risk? For example, photojournalists who work closer to the action.

Equipment & transport

- Have you identified how you will communicate with the team and how they will remove themselves from a situation if necessary? **Note the potential complications and impact of any communications blackout on the ground.**
- Have staff backed up and secured their devices, including their personal cell phones?
- Have you spoken with staff about secure communications methods and ensured they have downloaded the relevant messaging apps on their devices?
- Have staff researched the security of the route they will be taking, any recent security incidents or violence along the way, and the likelihood of checkpoints?
- If violence is anticipated, have you made available the relevant PPE such as safety helmets? Do staff know how to use such PPE?
- Are selected staff driving themselves, and is their vehicle roadworthy, appropriate, and sufficiently robust for the terrain and road conditions?
- Have you discussed the risk of COVID-19 exposure with selected staff, and provided them with good quality face masks and alcohol-based hand sanitizer?

General considerations

- Is the level of risk to selected staff acceptable relative to the editorial gain?
- Have selected staff been issued with the appropriate accreditation, press passes, or a letter indicating they work for your organization?
- Have you recorded and securely saved the emergency contact details of all staff going on the assignment?
- Have you set up a check-in procedure (if deemed necessary)?
- Is the team correctly insured and have you put in place appropriate medical cover?
- Have you identified all local medical facilities in case of injury and made team members aware of the details? (Note that approximately 70% of medical facilities in Tigray are said to have been vandalized, according to MSF.)
- Have you considered and discussed the possibility of trauma-related stress that could result from the assignment?

For more information about risk assessment and planning, see the CPJ Resource Center.