



WEATHERING THE STORMS

**Building Social Justice Resilience
Against Opposition Attacks**



WEATHERING THE STORMS (WTS) TEAM

Emily Goldfarb, RoadMap Director

Mary Ochs, Weathering the Storms Team Lead

Margi Clarke, WTS Consultant

Jen Soriano, Strategic Communications Coordinator (2012-13) and WTS Consultant

Jung Hee Choi, Strategic Communications Coordinator (2014-15)

WTS Consultants: Elizabeth Toledo of Camino PR, Lisa Russ, Nijmie Dzurinko, Charles Fulwood, Francisca Baxa, Scott Lowther, N'Tanya Lee

Digital Security Partner: Jonah Silas Sheridan, Information Ecology

See the Weathering the Storms resources page for more information and tools.
www.roadmapconsulting.org/WTS

For more information contact weather@roadmapconsulting.org

Report written by Margi Clarke, Mary Ochs, Jen Soriano and Emily Goldfarb

Report edited by Jen Soriano

© RoadMap 2015

Design by Design Action

CONTENTS

Executive Summary	2
Introduction	4
I. Storm Patterns: Types of Attacks to Watch Out For	7
ALLEGATIONS OF PARTISAN POLITICAL ACTIVITY	
PUBLIC RELATIONS ATTACKS	
INFILTRATION, SURVEILLANCE AND ENTRAPMENT	
DIGITAL INTRUSIONS	
HARASSMENT AND VIOLENCE	
INTIMIDATION LAWSUITS	
PRESSURE ON FUNDERS	
RISKS FROM DISGRUNTLED EMPLOYEES	
II. ARMOR your Organization	17
5 STEPS TO WEATHERING THE STORMS	
CALLING IN SUPPORT BEFORE, DURING OR AFTER AN ATTACK	
FUNDERS AS ALLIES	
III. Organizations That Have Weathered the Storms	21
CENTRO DE TRABAJADORES EN LA LUCHA	
9TO5, NATIONAL ASSOCIATION OF WORKING WOMEN	
WORKERS' DEFENSE PROJECT	
IV. Recommendations to Social Justice Organizations, Alliances and Funders	28
Conclusion	29
Appendices	30
WEATHERING THE STORMS PROJECT: 2012-14 HIGHLIGHTS	
WEATHERING THE STORMS TOOLKIT: TABLE OF CONTENTS	

EXECUTIVE SUMMARY



Photo Credit: Thinkstock


Social justice organizations are subject to politically motivated attacks that come in many forms and are as changeable as the weather. Drawing on years of work with social justice groups and additional research in the field, this report illustrates patterns of threats, how they can distract or weaken an organization, and the steps groups are taking to armor themselves and emerge stronger.

RoadMap is a national network of independent consultants supporting social change through organizational development, strategic communications and coaching, comprehensive assessment, webinars and training. RoadMap launched the **Weathering the Storms (WTS)** project in 2012 at the request of 12 local and national foundations. These foundations—part of the Neighborhood Funders Group's *Working Group on Labor and Community Partnerships*—shared common concerns about increased attacks on their grantees. This report outlines RoadMap's analysis based on experiences in the field and recommendations.

- » **STORM PATTERNS** cites examples of the most common threats: allegations of partisan political activity, public relations attacks, infiltration and entrapment, digital security intrusions, harassment and violence, intimidation lawsuits, pressure on funders, and risks from disgruntled employees. More than 50 percent of the groups RoadMap is supporting have experienced at least one such attack. Some attacks have succeeded in weakening, and in a few instances, closing down targeted organizations.
- » **ARMOR YOUR ORGANIZATION** shows what organizations can do to build resilience against the attacks and protect their work before, during or after an attack in this changing climate. RoadMap offers tools, training and technical assistance on how to: 1) **Assess** threats; 2) **Reduce** risks; 3) **Manage** a crisis before it happens; 4) **Organize** your communications; and 5) **Refresh** your practices.
- » **ORGANIZATIONS WEATHERING THE STORMS** feature profiles and testimonials from groups that are taking the time to invest in prevention or are proactively addressing attacks in ways that strengthen their work. We include several tips from the WTS Toolkit and share the Toolkit table of contents in the appendix.

How can WTS strengthen the social justice sector?

Political opposition is something we need to pay attention to always but we also know from experience that it heats up during election seasons. We are already seeing increased “storm activity” as we head into the 2016 election cycle, even for groups that do not primarily work on civic engagement.



RoadMap's experience of the last three years demonstrates that groups can make significant progress in just a few weeks or months of preparation against potential attacks.

We recommend working with a WTS consultant to identify and triage risks so that organizations can address the most severe risks immediately and aggressively. Following that, groups can continue to address lower-level risks over time. RoadMap offers a range of 'light-touch' technical assistance as well as deeper engagements, including training and extensive systems upgrades.

In the case of alliances, RoadMap works with a point person to disseminate WTS tools and practices among the various groups in the alliance. Such a cohort model allows groups to motivate and learn from each other and is the most impactful and cost-effective way to use RoadMap consultants to strengthen an alliance.

Over the last two years, RoadMap has supported more than 40 groups and alliances with customized WTS technical assistance, and has reached more than 300 organizations through webinars and toolkits. We are honored to work with groups across the country fighting for immigrant rights, racial justice, worker dignity, LGBTQ rights, reproductive justice, and environmental and climate justice. You are taking on our society's most pressing issues and winning unprecedented victories at the local, state and federal levels. Your work is far too important to be undermined by your opposition.

In addition to reducing risks and addressing crises cost-effectively, WTS engagements can bolster overall capacity in communications, administration, governance, and finance. RoadMap designs custom packages (starting at \$2,000 per organization) to address everything, from the core WTS checklist to the more complex engagements for multiple capacity-building goals (See appendix). Onsite trainings average \$7,500. Alliance-wide efforts can be scaled to leverage peer learning and strengthen alliance relationships. Funders interested in WTS can contribute to RoadMap's pooled fund and encourage grantees to choose from a menu of WTS options, or can set up a custom program for a specific cohort of grantees.

We offer this report to emphasize the urgency of taking care of our organizations in the face of rapid changes in the political climate, and during times of heightened scrutiny. These lessons from the field show that armoring your organization is straightforward, do-able and critical to bolstering your impact. Your work is worth protecting and RoadMap is here to help.

See the Weathering the Storms resource page for more information and tools. www.roadmapconsulting.org/WTS

INTRODUCTION



Photo Credit: Jeremy Koreski

Everyday, social justice groups are subject to politically motivated attacks. While such attacks are not new, there has been a definite change in the political climate.

If you're standing up for justice, you will face opposition. Grassroots organizers and advocates know this. Those who may lose political influence, money and cultural control are invested in undermining the organizations that expose or challenge them.

Consider this example: For over 10 years, the right had been watching **CASA de Maryland**, an organization with a long history of providing services to and advocating for the rights of immigrants. Anti-immigrant groups had not only been watching CASA closely, they had collected hundreds of their documents and had even gained access to private online discussion groups. Opponents used this material to launch an aggressive public attack on CASA, falsely

claiming that they were registering "illegals" to vote, among other baseless allegations. Working with the Alliance for Justice, John Pomeranz of Harmon, Curran, Spielberg & Eisenberg LLP, and Camino Public Relations, CASA spent two years responding to these false charges. In the end, CASA weathered the storm, exposed those who were behind the attacks, and came out more credible and effective than ever.

CASA's example is both a cautionary tale and a reminder that with preparation you can "get your house in order" and armor your organizations against opposition attacks.

Everyday, social justice groups are subject to politically motivated attacks. While such attacks are not new, there has been a definite change in the political climate leading to: increased intensity of corporate spying; the emergence of more aggressive and systematic legal challenges; more frequent government investigations based on spurious complaints; and increases in digital security attacks and incidents of personal harassment.

More than half of the groups RoadMap is supporting have experienced at least one opposition attack. Some of these attacks have been successful in weakening the targeted groups. In a few instances, attacks have resulted in the demise of organizations. All your opposition has to do to be successful is to instill fear or denial amongst your stakeholders, or doubt about your credibility in the public eye.

We at RoadMap envision a social justice sector where preparing for the worst allows organizations to operate at their best.

The good news is that there are steps you can take to build resilience against attacks and to protect your work. And RoadMap is here to help.

This report shares some of the valuable lessons RoadMap has learned through research and direct support to organizations and allies in the field. In this report you'll find a compilation of types of attacks to watch out for, a primer on how to begin armoring your organization, and a description of RoadMap's approach to supporting groups through this process. We also share success stories of organizations that have taken time to prepare themselves with RoadMap's **Weathering the Storms** support.

We at RoadMap envision a social justice sector where preparing for the worst allows organizations to operate at their best. We look forward to building this foresight and resilience together.

Weathering the Storms (WTS): Principles

The **WTS** approach is grounded in three principles that help armor and protect an organization:

- 1) **Preparing for attacks is a key part of organizational capacity**, as essential as campaign development, financial management and strategic planning.
- 2) **Preparation and response are most effective when approached holistically**, integrating communications, organizational development and legal compliance. Such integration maximizes resilience and lays strong foundations for turning attacks into opportunities to advance organizational values and goals.
- 3) **Preparing for attacks can be done through simple steps** over the course of a few weeks to several months. We know that grassroots groups are often short on time and money, so the WTS process is designed to work within each group's capacities.

There is no one season or single method of opposition attacks; they come around the clock and year after year. But it's never too late to start getting prepared. RoadMap tools and training are accessible, effective and available to you.



STORM PATTERNS

TYPES OF ATTACKS TO WATCH OUT FOR



Allegations of Partisan

Political Activity: Watch out for blizzards of allegations of voter fraud or misuse of non-profit funds for inappropriate political activity—especially if you are a c3/c4 or do civic engagement during elections with close races!



Public Relations Attacks:

Smear campaigns through online and offline media can quickly create tornados of rumors that can tear up your organization's reputation



Infiltration, Surveillance and Entrapment:

Corporate, political and law enforcement surveillance can seep into your organization and eventually cause a flood of psychological disruption and structural damage.



Digital Intrusions:

Digital surveillance can result in organizational and data theft and/or website and social media account hacking. Both can cast a dark cloud over organizational integrity.



Harassment and Violence:

It's a myth that lightning doesn't strike twice. Harassment and violence is not new and is unfortunately on the rise, ranging from prosecutors over-charging during civil disobedience arrests to death threats and arson perpetrated by opposition extremists.



Intimidation Lawsuits:

Corporations can unleash hailstorms of lawsuits on organizations, holding them accountable. These lawsuits include charges of libel, trespassing and conspiracy and are designed to put serious dents in organizational resources and confidence.



Pressure on Funders:

Opposition forces can damage your organizational home by stirring up doubt and fear with your funders. If strong enough, these winds can blow critical resources away.



Risks from Disgruntled Employees:

Like rain, disgruntled employees can become a problem if you have a hole in your roof or infrastructure. This leaves your organization vulnerable to leaks of data or resources and could be exploited by opponents looking to turn rain into a storm.



I. STORM PATTERNS

Types of Attacks to Watch Out For



Photo Credit: Thinkstock

Attacks come in many forms and are as changeable as the weather. But like the weather, there are noticeable patterns. Drawing on years of work with social justice groups and additional research in the field, RoadMap has collected information on the following types of opposition attacks, all of which are becoming more common and more aggressive: **allegations of partisan political activity, public relations attacks, infiltration, surveillance and entrapment, digital intrusions, harassment and violence, intimidation lawsuits, pressure on funders, and risks from disgruntled employees.**

Following are some definitions and examples of such attacks:



You are likely to be in the path of storms if...

- » You are winning campaigns or otherwise standing up for justice
 - » You are involved in civic engagement or electoral work, especially in elections with tight races
 - » You work in a swing state
 - » You work on hot button issues that attract right-wing backlash, such as reproductive justice, police reform and accountability, LGBTQ rights, labor, electoral reform, immigrant rights, and healthcare reform
 - » You receive federal, state or local government funding
-



Allegations of Partisan Political Activity

Such attacks involve government investigations based on allegations of activities that violate an organization's nonprofit status. Most common are allegations of voter fraud and using nonprofit funds for inappropriate partisan activity. Organizations are particularly vulnerable to this type of attack if they have a c4 status and/or do civic engagement work during elections with close races.

The attacks are usually launched by conservative business interests and/or politically motivated government officials, and are often accompanied by aggressive PR campaigns, so-called exposés and public hearings.

The **Florida New Majority Education Fund** was investigated for allegedly submitting questionable voter registrations before the 2012 elections. Florida's Secretary of State spurred the state's Department of Law Enforcement to research registration fraud, an effort that found no fraudulent activity on the part of Florida New Majority Education Fund, according to The Miami Herald.¹ But it did expose fraud by Strategic Allied Consultants, a GOP contractor that made headlines when its owner, Nathan Sproul, was caught falsifying registration forms.² Prepared with crisis response messaging, the groups were able to reassert their integrity by promptly defending their practices against these politically motivated government attacks.

The **Center for Civic Policy (CCP)** in New Mexico faced a lawsuit and several years of investigations into its alleged partisan activity. The attacks were a direct response to CCP's success at increasing voter registration and turnout. Three state legislators who lost their election rebids retaliated through a lawsuit, which was eventually dismissed. Concurrently, several state legislators also tried to pass legislation to "muzzle" a nonprofit's ability to advocate for and share facts about legislators' positions. The regional nonprofit community eventually united and defeated those attempts in the 2009 legislative session.

In recent years, the U.S. Chamber of Commerce has commissioned a number of reports that seek to undermine the legitimacy of worker centers.³ The reports claim, among other things, that worker centers are front-groups for unions. This wave of attacks has included Congressional hearings spurred by right wing political activists, lobbyists and elected officials. Despite repeated findings by the Department of Labor and the IRS that worker centers are appropriately acting as public charities and not as unions, the Chamber's accusations feed anti-union sentiments and undermine core freedoms of expression, association and redress for workers abused by their employers.



Best protective armor: Have your compliance house in order, and train staff and volunteers regularly.



Public Relations Attacks

While all attacks are designed to damage an organization's reputation, public relations (PR) attacks are uniquely focused on undermining organizational credibility in the public eye. By definition, these attacks are delivered through media channels, both online and off, and can go viral more quickly today because of social media. Some right wing organizations run active websites that purport to be muckraking journalism but actually are in the business of peddling lies, rumors or half-truths, often bankrolled

¹ <http://miamiherald.typepad.com/nakedpolitics/2012/10/florida-democratic-party-two-liberal-groups-accused-in-mysterious-complaints-of-voter-registration-f.html>

² www.colorlines.com/archives/2013/09/florida_voter_registration_fraud_investigation_comes_up_empty.html

³ www.workforcefreedom.com/media-info/new-report-us-chamber-profiles-five-leading-worker-centers

by corporate perpetrators in an effort to discredit those holding them accountable.

One such sustained PR campaign comes from the people behind the website “ROCexposed,” which targets and maligns the work of the national worker rights network, **Restaurant Opportunities Center (ROC)**, founded by immigrant restaurant workers affected by the 9/11 attacks in New York. ROCexposed regularly denounces ROC and the low-wage worker sector; more so whenever ROC achieves a victory for food service workers. Although the website’s backers are unnamed, many assume the site is associated with the National Restaurant Association, the largest food service trade association in the world.

Likewise, the website “Worker Center Watch” has launched numerous attacks to undermine the successful organizing work that ROC along with Fast Food Forward and OUR Walmart have led among workers in recent years. Those behind the site have sponsored smear campaigns on Twitter and manipulated and shared videos with insulting images of activists and workers.⁴

Campaigns using “Twitter bombing” and the flooding of Facebook pages with negative comments—as well as other uses of social media to damage reputations—have become much more common. **Progressive Leadership Alliance of Nevada (PLAN)** had its Twitter account “twitter bombed” by unknown opponents during the 2013 Nevada legislative session when PLAN and one of its Native American member organizations had been waging campaigns against corruption and expansion in the mining industry, including sweetheart tax deals, environmental destruction and serious health and safety issues. PLAN suspects that mining lobbyists were behind the twitter bomb campaign.⁵



The term “twitter bomb” refers to the posting of numerous, often pejorative, “spamming” tweets about a person or organization. The goal is to produce a flood of tweets with common hash tags so that the tags trend on Twitter. It’s a tactic that has been used for years by Internet activists as well as political parties, campaigns and commercial advertising interests. However, it has become more common as a tactic to undermine social justice work. Social justice organizations would do well to prepare for an organized online response.



Best protective armor: Monitor your opposition online and prepare your own proactive messaging.

4 www.thenation.com/blog/177376/former-walmart-exec-leads-shadowy-smear-campaign-against-black-friday-activists

5 Information provided by PLAN to RoadMap, March 2015.



Infiltration, Surveillance and Entrapment

Progressive groups have long been subject to infiltration from corporate interests, political opponents, police, or federal law enforcement. Infiltration can be on-the-ground presence with “spies” posing as supporters, or digital infiltration of data and communications. Infiltrators may document observations, attempt to secretly record organizational activities, disrupt normal processes, and seek access to public and private documents. The next section on digital intrusion explores this last piece in more depth. But first, here are examples of a range of corporate and police infiltration tactics.

CORPORATE INFILTRATION

The **Coalition of Immokalee Workers (CIW)** and other community groups which support worker organizing, immigrant rights and environmental causes have been subjected to infiltration and libelous PR attacks by their corporate targets.⁶ When CIW was fighting for wage concessions from Burger King, for example, the company hired Cara Schaffer, owner of Diplomatic Tactical Services, to infiltrate CIW’s campaign as a volunteer. Burger King confirmed that it hired Diplomatic Tactical Services “for years” and used it to obtain information about CIW’s plans.⁷

“*Spooky Business*,” a November 2013 report by Essential Information, details a range of corporate attacks, reporting that “many of the world’s largest corporations and their trade associations, including the U.S. Chamber of Commerce, Wal-Mart, Monsanto, Bank of America, Dow Chemical, Kraft, Coca-Cola, Chevron, Burger King, McDonald’s, Shell, BP, BAE, Sasol, Brown & Williamson, and E.ON have been linked to espionage or planned espionage against nonprofit organizations, activists and whistleblowers.”⁸

In an interview with Democracy Now, report author Gary Ruskin added: “Here in the United States, Congress is totally asleep. There is no investigation of this matter [corporate espionage] at all, as far as we can tell, either from Congress or from the Department of Justice. And that’s really awful. Corporate espionage against nonprofit organizations is a threat to democracy, and it’s a threat to individual privacy.”⁹

VIDEO/AUDIO ENTRAPMENT

Another type of infiltration that is on the rise is video entrapment, which involves attempts to capture potentially incriminating statements or behavior through secret video and audio recordings.

On its first venture to increase registration among eligible Latino citizens in Milwaukee and Racine, Wisconsin, **Voces de la Frontera Worker Center** was the target of an attempted entrapment. One of Voces’ voter registrars was approached at the office by two Latino men who were pressuring her to allow them to register to vote, even after they shared information that made it clear they were not eligible to vote in Wisconsin.


6 www.ciw-online.org/blog/2008/04/petition_delivery_advisory/

<http://www.ciw-online.org/blog/2014/04/chamber-commerce-hate-america/>

7 http://www.nytimes.com/2008/05/07/opinion/07schlosser.html?_r=0

8 “Spooky Business”, p. 3, Essential Information, November 2013

9 Democracy Now, Gary Ruskin interview (www.democracynow.org/blog/2013/11/25/pt_2_us_corporations_enlist_ex)



The registrar did not allow the men to register, yet accusations were made that Voces had registered ineligible voters. These charges were proven false after a Milwaukee District Attorney's investigation revealed that the two men had been sent by the anti-immigrant organization FAIR.¹⁰ The men had been secretly audio-recording the encounter in the hopes of entrapping Voces in the act of voter fraud.¹¹

“Approaching groups with hidden cameras is an increasingly common way for opponents to conduct secret taping. And, it's really easy to set up a hoax website.¹² Groups that are working on issues that are highly contested should conduct a risk assessment and readiness activities to minimize vulnerability.”

—Elizabeth Toledo, Camino PR

GOVERNMENT INFILTRATION

Infiltration of social justice groups by the U.S. government had particularly devastating impacts in the 1960s because of J. Edgar Hoover's COINTELPRO program. Although perhaps less centralized, state infiltration today has the potential to be equally devastating. Recent examples include documented instances of police infiltrators in the Occupy and #BlackLivesMatter movements. There is growing concern in the social justice movement about proliferating technologies for state surveillance which may lead to targeted arrests of community leaders and protest organizers.

Since the Bush years, the press has revealed ever more evidence of government interception of online and cell communication through legal and illegal actions, such as government subpoenas of internet service providers, intelligence agents stealing codes for cell phone chips, and police abuse of 'Stingray' technology.¹³ Such incidents have been tracked anecdotally and in some cases challenged in court. The ACLU has challenged this type of intrusion as an unconstitutional search without a warrant.¹⁴

In December 2014, local police in Bloomington, Minnesota sent undercover police to infiltrate a group that was planning a **#BlackLivesMatter** protest at the Mall of America.¹⁵ By volunteering as marshals for the action, police were able to join the text messaging alert system that the group used for the action. Police are bringing a range of charges against eleven of the protestors and claiming restitution for costs of policing the protest.

10 Voces de la Frontera notes that FAIR has been classified as an extremist hate group by the Southern Poverty Law Center (www.splcenter.org/blog/2012/08/10/how-do-we-know-fair-is-a-hate-group-let-us-count-the-ways/)

11 Information provided by VOCES to RoadMap, March 2015.

12 www.abcnews.go.com/US/planned-parenthood-asks-investigation-anti-abortion-groups-hoax/story?id=17489476#.UIBoUBjQaUY

13 www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0

14 <https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy>

15 www.defendingdissent.org/how/police-spied-on-mall-of-america-protest-organizers/



A 'stingray' mimics a cellphone tower, prompting a phone to connect to it even if no call is made. This lets a stingray operator send a signal to the phone, locate it and in some cases intercept conversations. The device sweeps up data from other people nearby, regardless of whether they are the focus of the investigation.¹⁶



Best protective armor: Assume that you may be subject to surveillance but act calmly and be cautious with sensitive personal or strategic information on email, texts and shared documents. Thoroughly screen volunteers, including security marshals for protests. Always ask media representatives to show their ID and be on the lookout for covert recording devices.



Digital Intrusions

Digital intrusions such as surveillance and data theft are on the rise as organizations become more dependent on laptops, cell phones, cloud-based services and remote work places. Intrusion may come from political opponents, police or criminal actors. Computers and servers can become infected, email identities or online accounts may be appropriated, and data lists may be corrupted or stolen. It's often difficult to know where the attack is coming from and expensive to do a thorough forensic investigation.

Nonprofit organizations can be particularly vulnerable owing to a lack of IT resources and limited knowledge of how to prevent or respond to these incidents. The risks include political vulnerabilities, exposure of employee or donor personal information, identity theft, financial theft, and fines for non-compliance with laws.

There are many possible ways your data can be negatively affected by attacks but your technology systems and how you use them can help protect against it. There are multiple steps involved in securing computers, cell phones, databases, and electronic files and they are exceedingly critical to protecting our personal privacy and our work. New this year, RoadMap and Information Ecology have added digital security protection tools and technical assistance services to the WTS Project.

In a recent incident, a national organization (that prefers anonymity) suffered a digital intrusion in which staff email credentials were appropriated and there was an attempt to steal funds from a bank account. There was a possibility that other data may also have been taken. A WTS consultant advised the organization to notify staff and vendors that data may have been stolen and the group offered identity theft protections to everyone placed at risk.

¹⁶ www.theguardian.com/world/2013/mar/28/aclu-stingray-surveillance-police-cellphones

New this year, RoadMap and Information Ecology have added digital security protection tools and technical assistance services to the WTS Project.

“The RoadMap digital security advisor was able to make recommendations for what kind of forensic data investigation we needed to do and how to communicate about the incident. He also helped design improved data security practices, and train and coach our staff to put new policies and practices in place. Having the WTS advisor on hand and able to quickly respond gave everyone confidence during the incident and improved our practices for the future. We are now doing a full technology assessment and planning for future investments to secure our systems and it has given us a jump on upgrading our IT systems in general.”

—Operations Director of a national alliance that experienced digital intrusion¹⁷



Best protective armor: Put basic Information Technology capacity in place; know what data you want to protect and where it is stored. Consider who might want to access or destroy your data and their capacity to do so and based on that knowledge, take incremental steps to implement practices that counter the most prevalent threats.



Harassment and Violence

Verbal threats, harassment and physical violence are nothing new and continue to be a growing trend in today's atmosphere of extreme bigotry against Black, Latino, Native American, Arab, Muslim, and LGBTQ communities, young women and men, and immigrants. Groups have also experienced criminal threats, arson, theft, and police harassment of organizers. Police and prosecutor misconduct is common, as is physical abuse, over-charging during arrests and attempts to collect restitution for policing costs.

Gustavo Torres of **CASA de Maryland** shares the painful harassment CASA regularly experiences: “We receive tons of hate email all the time. Anything that happens with my community—for good or for bad—I receive an email telling me how bad I am and how bad CASA is.” In May 2007, someone set fire to the doublewide trailers that house the group's Shady Grove center; though it did minimal damage, county police investigated it as a hate crime.¹⁸ Then, in May 2008, CASA staffers received a couple of death threats that rattled Torres. He had security cameras installed and called in the Anti-Defamation League to provide advice and staff training.

Most recently, in the anti-police brutality movement, organizers in Ferguson, Missouri and with the #BlackLivesMatter campaigns around the country have been subjected to threats (both online and by phone), police surveillance and infiltration, stolen computers, and other harassment. The NAACP office in Colorado Springs was bombed on January 6, 2015. **Asian Pacific Environmental Network (APEN)** has experienced phone threats stemming from its campaigns against oil giant Chevron.¹⁹ Immigrants in states like California, Georgia and Arizona have faced phone threats and vigilante attacks, and there are frequent reports of hate crimes against environmentalists, feminists and gay rights activists.

¹⁷ Information provided by client to RoadMap, February 2015.

¹⁸ www.washingtoncitypaper.com/articles/36826/montgomery-county-is-no-longer-a-haven-for-immigrants-and

¹⁹ Citation: Information provided by APEN to RoadMap, March 2015.

In the fall of 2014 and in early 2015, the San Diego and Washington, DC offices of the **Council on American-Islamic Relations (CAIR)** received various threatening letters and substances,²⁰ emails, and voice messages. In one message, the suspect allegedly used derogatory and inflammatory language, referencing the massacre at the Charlie Hebdo office in Paris and threatening a mass shooting, according to Reuters News Agency. Investigations led to the suspect's home where they found an AR-15 assault-style rifle as well as "slurs and writings of a racist nature." He was charged with hate crimes but released on bail. Hanif Mohebi, executive director of the San Diego chapter of CAIR, told Reuters that the suspect should have been denied bail and that the case exposes a double standard in the U.S. criminal justice system: "Had this been a Muslim who committed this crime, the FBI would be investigating it and they are not. We are the victims of terrorism and this case should be treated as such."²¹



Best protective armor: Practice crisis response for dangerous situations, from political threats to fire risks, to earthquakes. Create your Crisis Management Team (CMT) and have a crisis communications protocol in place with contingencies for various urgent situations.

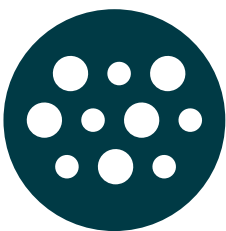


Taking time to care for our people in the difficult moments of attack

Facing violence or threats of violence can take a very personal toll. While no amount of preparation can eliminate the shock of these experiences, deliberate practice of security protocols as well as open communication can help cushion the impacts. Creating space for addressing emotions and collectively defining the extent of the threat can allow us to draw on our best instincts rather than becoming overwhelmed by fear. The WTS process can leverage crisis preparedness to make our community and workplace more caring, supportive and resilient. We have also found that outside coaching can offer needed support to individuals and groups in processing the impacts of political and personal attacks.

"Coaching can provide a safe, reflective space for leaders to work through feelings that arise in such stressful and scary situations. Then leaders can ground, focus and access inner strength and wisdom to identify support and move to next steps to powerfully address the situation."

—Belma D. González, RoadMap Coach



Intimidation Lawsuits

There are a variety of corporate lawsuits designed to intimidate and drain social justice groups and their leaders, often in retaliation for effectively holding corporations accountable. These lawsuits accuse activists of libel, trespassing and/or interference with commerce, or conspiracy; or they seek access to digital communications around organizational campaign work.

20 www.reuters.com/article/2015/01/30/cair-sandiego-arrest-idUSnPn4Nh4ST+93+PRN20150130
21 www.reuters.com/article/2015/02/04/us-usa-threat-california-idUSKBNOL804M20150204

They can even use anti-Mafia methods, called RICO or racketeering charges, where the organization or a group of organizers is accused of conspiring to interfere with a corporation through protests.

Many of these intimidation lawsuits are characterized as SLAPP suits²²—Strategic Lawsuits Against Public Participation—to reveal their intent to penalize free speech and discourage public accountability of corporations. While the courts usually dismiss these suits, legal costs and negative PR can weaken organizations in the process, by creating doubt, distraction and unnecessary expense.

Central Florida Jobs with Justice, Centro de Trabajadores Unidos (CTUL) and other low-wage worker advocacy groups—along with individual staff and board members—have been sued under trespassing²³ and racketeering charges for picketing a work place in support of worker rights. It takes a concerted and expensive legal response to quash these kinds of legal attacks. (Also see profile of CTUL on page 22.)

In some cases, intimidation lawsuits can lead to digital intrusions. For example, Jonah Silas Sheridan of Information Ecology shares this story: “In one instance, Chevron retaliated with a conspiracy suit after a financial judgment against it. In the process they filed a broad subpoena for sweeping access to 9 years of email metadata and identities of nearly 100 activists who had fought their efforts in Ecuador, in a clear attempt to map and disrupt that community. Electronic Frontier Foundation and EarthRights stepped in and that suit was dropped last year but not before some data was released. This is not infiltration or ‘hacking’, but certainly represents a threat to digital security that should not be overlooked, and is worth consideration for most organizations confronting powerful entities.”²⁴



Best protective armor: Build a legal defense fund and identify legal advisors ahead of time. Follow best practices for email and document retention and destruction. Understand the role of metadata and minimize how it can be used against you to map networks, communications and actions.



Pressure on Funders

Pressure on funders—through direct meetings, email appeals, inflammatory articles against funders and their grantees—aims to scare funders into disfavoring certain groups, and to broadly discourage new funders. Some foundation staff or trustees become nervous when questioned about their grant making, which can lead to the loss of critical financial support for some social justice organizations. Political pressure on government agencies to cut funds to disenfranchised populations is another form of pressure on funders.

²² www.civicpolicy.com/its-really-scary-to-get-sued/

²³ www.jwj.org/walmart-attempts-to-silence-protests-with-lawsuit

²⁴ www.earthrights.org/legal/long-fought-victory-anonymous-email-users-chevron-agrees-withdraw-google-and-yahoo-subpoenas

Conservative extremists targeted the Catholic Campaign for Human Development (CCHD), purporting to hold them accountable to select Catholic values. They pressured CCHD to withdraw its support from grantees, including immigrant and worker rights groups who had any form of association with marriage equality campaigns. These extremists used redbaiting and homophobia to call for the defunding of multiple social justice groups around the country.²⁵

TIDES Foundation, Open Society Institute and other progressive funders have been attacked on conservative talk shows and websites. The vehement political rhetoric of some conservative media personalities have been linked to vigilante threats.²⁶

See page 18 for advice from funders on how to work with them as allies in responding to opposition attacks.



Best protective armor: Be clear and prompt about informing allies and funders about attacks and ask for support from funders.



Risks from Disgruntled Employees

Organizations must also watch out for internal fraud, disgruntled employees, or former employees who may act against an employer. Better internal practices can prevent or detect a range of employee-related risks—from abuse of an organizational credit card, to severe cases of embezzlement; from failing to return a computer with organizational documents upon leaving a job, to taking donor lists offsite without authorization; from exaggerated labor grievances, to public complaints about the organization. Such situations can be further exploited by the opposition who may welcome “insider dirty laundry” to fortify political attacks.



Best protective armor: Strong internal administrative and personnel policies and practices can help prevent these situations and make responding smoother.

There are many, many more incidents like these occurring around the country. RoadMap’s WTS preparedness tips and response strategies are pieces of ARMOR to protect your organization from risks and threats.

²⁵ www.reformcchdnow.com/

²⁶ www.civicpolicy.com/targeting-nonprofits-the-tides-foundation-this-time-with-real-bullets/

II. ARMOR YOUR ORGANIZATION

5 Steps to Weathering the Storms

“Preparing for crisis through proactive stories and trained messengers is not only a key part of strategic communications, it is a cornerstone of the organizational development necessary to protect groups against attacks.”

- Jen Soriano, RoadMap

In a 2012 RoadMap survey, more than 50 percent of groups seeking technical support had experienced an opposition attack, and many more knew of allied groups that had experienced attacks. At the same time, most respondents reported not feeling prepared to manage an attack and were eager for guidance, especially on “how to start.” Almost two-thirds of the groups said that they wanted support on at least one element of preparedness.

The very strengths of grassroots groups—such as lean operations and open-door community engagement—can make them more vulnerable to the types of attacks described in the previous section. The good news is that common vulnerabilities can be addressed through a straightforward process. Here we offer a primer of five steps to start armoring your organization to weather the storms.

ARMOR: 5 Steps to Weathering the Storms

1. **Assess the Threats:** Prioritize your areas of need by assessing threats you may be vulnerable to based on your programs, structure, opposition research, and past experience.
2. **Reduce Risks:** Tighten up practices related to governance, archiving, digital security, finance, volunteer training, and personnel. For c3/c4 affiliated groups, strengthen administrative systems for tracking lobbying and electoral advocacy to ensure compliance with regulations and funder requirements.
3. **Manage a Crisis Before it Happens:** Create a team and clear internal protocols for crisis management. Raise awareness of staff, board and volunteers by reviewing the threats and response plan.
4. **Organize your Communications:** Prepare crisis messaging that addresses threats and affirms your core values and goals, as well as your decision-making and implementation processes for message dissemination. Identify and train messengers, including allies who can validate your organization with key audiences.
5. **Refresh your Practice:** Ensure preparedness practices are maintained with an annual ‘fire drill’ to review threat scenarios; regularly tune-up systems; and screen and orient new people as they join staff, volunteer and board positions.





Calling in Support Before, During or After an Attack

RoadMap helps organizations tackle these five steps in manageable pieces. The process usually takes several months so that organizations can incorporate this “armoring” into the work they are already doing.

Building Blocks of a Crisis Management Plan

- » Identify your Crisis Management Team (CMT)
- » Assess the situation
- » Notify staff, board, foundations and key partners
- » Develop the message platform and create a communications strategy. If the crisis has a public dimension:
 - Identify and train spokespeople
 - Conduct media monitoring and analysis
 - Practice strategic record-keeping
 - Conduct a post attack evaluation

Before an Attack:

Begin an assessment by reviewing a comprehensive checklist of administrative and communications systems and exploring threat scenarios that are most relevant to the group. Based on the assessment, RoadMap’s organizational development and communications experts will support the organization through some or all of the next four steps—from helping to strengthen systems, adapt templates and create new policies, to facilitating crisis and communications planning and supporting with “fire drills” and training. Additional time may be needed to update training or communications materials, or to develop more comprehensive communications plans. RoadMap can also conduct online or on-site training in the ARMOR capacity-building process for staff, board and volunteers.

During an Attack:

When organizations are under active attack, RoadMap serves as crisis management support, helping with internal decision-making and risk assessment, and choosing when and how to move into external communications pertaining to the attack. The goals are: to minimize impact of the attack, bolster confidence among members, allies and stakeholders, repair any policies or practices that can leave the organization vulnerable, and weaken the credibility of opponents when possible.

After an Attack:

RoadMap can help after an attack by consolidating lessons learned and facilitating scenario planning to strengthen best practices for future incidents. RoadMap also supports groups in working with their funders, who can be essential allies in confronting attacks (see box: Funders as Allies in Weathering the Storms page 18). RoadMap’s regular engagements for strategic planning, strategic communications, and internal systems upgrades may also incorporate WTS best practices.



Funders as Allies in Weathering the Storms

“Funders are becoming increasingly aware of attacks on their grantees. Although some may distance themselves to avoid controversy, others are doubling down on their commitment to grantees facing threats. These foundations want their grantees to know that they can be important allies in confronting opposition attacks. More than 12 foundations initiated and supported **Weathering the Storms** to put this commitment into action. While they want to protect their own philanthropic practices, they also see preparation for attacks and effective response to attacks as important pieces of resourcing their grantees’ work.

“We know from experience that when our grantees are feeling vulnerable or under attack, they are not sure whether or not they should reach out to their funders. It is understandable to be worried that funders will be nervous if a grantee is being publicly scrutinized for actions or behavior, however fairly or unfairly. We can appreciate you may be concerned that revealing areas of potential ‘weakness,’ risk or liability, could threaten your ongoing support.

“While we can’t speak for all funders, on behalf of our colleagues who have supported this project, we want to be good partners to our grantees. We have invested in your organizations, and that means we believe in your work and trust that you are operating with integrity and following the law. It is in our interest to ensure that your work is not interrupted by opposition attacks. For these reasons and more, we want to help make sure that your ‘house is in order’ and that you follow the advice laid out in the **Weathering the Storms** toolkit... please remember that one of the most important things you can do to work well with your funders is to reach out to us.”

—Molly Schultz Hafid, Unitarian Universalist Veatch Program at Shelter Rock

ARMOR In Place: Capacities Built Through WTS

With targeted consultant support over several months, organizations have made significant progress. The following are ARMOR capacities that RoadMap has helped organizations build through Weathering the Storms.



- » **Stronger Governance:** groups filled gaps in written policies or archiving systems and strengthened board awareness and communication protocols for crisis scenarios.
- » **Crisis Plans in Place:** groups created crisis management plans, including crisis communication plans and practices for training and refreshing staff, board and volunteers in the process.
- » **New Strategic Communications and Rapid Response Protocols:** groups integrated opposition media monitoring and crisis scenario planning into strategic communications and developed crisis messaging to reinforce core values and institutional credibility.
- » **Increased Digital Security:** groups incorporated best practices to protect sensitive data and reduce risk of criminal or political hacking incidents.
- » **Improved Electronic and Archival Document Management:** groups strengthened their systems for record-keeping and document backup, retention and destruction, in order to improve operational efficiency, reduce loss of data, and make document production efficient in case of legal attacks.
- » **Stronger Systems for Volunteer Screening and Training:** groups raised risk awareness and improved consistency in messaging among volunteers, especially those involved in civic engagement, electoral turnout or public outreach.
- » **Streamlined Human Resources and Finance Tracking Systems:** groups with affiliated c3 and c4 organizations paid special attention to this capacity to ensure compliance and improve information flow.

ARMORing your organization is straightforward, do-able and critical to maximizing your impact. And RoadMap is here to help. Your work is worth protecting!

III. ORGANIZATIONS THAT HAVE WEATHERED THE STORMS



Photo courtesy of 9to5

"Because we are building power to advance a long-term structural agenda we have to be a prepared and resilient organization. We found the assistance from RoadMap to be incredibly helpful in making sure NPA had its internal house in order. And we are jointly fundraising with RoadMap to bring this capacity to all of our affiliates."

—George Goehl, Executive Director of National People's Action

We are in a moment when progressives are gaining momentum on campaigns for worker's rights and the \$15 minimum wage, building a new racial justice movement against police and vigilante violence from New York City to Ferguson to the U.S.-Mexico border, and pushing back on corporate excess from extreme fossil fuel extraction to

predatory home foreclosures to profit-driven prison construction. Fights over voting rights, reproductive rights and public services are continuing at local, state and federal levels.

What follows are some **examples of groups that are doing this critical work, but also took the time to prepare for attacks.** The profiles we share here are just a few stories of how groups used RoadMap tools and consultant support to address vulnerabilities, "get their house in order," and ARMOR themselves against political storms.

"Our organization has experienced several attacks and is under constant scrutiny by anti-worker/anti-immigrant groups. It is essential that we run a tight ship. We found the RoadMap check list and assistance essential to making sure that our internal house is in order, so that we do not give our opponents any ammunition to further attack us."

—Christine Neumann Ortiz, Executive Director of Voces de la Frontera, Wisconsin

PROFILE:

Post-attack tune-up at Centro de Trabajadores Unidos en la Lucha



Photo Credit: CTUL

“When we learned about this project through the United Worker Congress, we jumped at the chance to learn more about the kinds of attacks going on.”

—Brian Merle Payne, CTUL

Organization: Centro de Trabajadores Unidos en la Lucha (CTUL) is a Minneapolis/Saint Paul-based organization of and for workers, committed to securing fair working conditions for present and future generations. Formed in 2005, CTUL organizes low-wage workers to develop leadership and educate one another to build worker power. In 2007, the Workers’ Center shifted from being a services group to a base-building organization.

Social Justice Impact: Over the past seven years, CTUL has pressured 31 companies—some of the biggest and most well-established employers in the area—into changing corporate policies that impact workers and gained improvements for more than 5,000 low-wage

workers, leading to an estimated \$3.9 million in additional income per year. Additionally, CTUL members have recovered more than \$1.3 million in back wages and damages, and hundreds of unjustly fired workers have been reinstated. As a result of these victories, CTUL is firmly established as a major force for worker justice in the region.

The Attacks: Not long ago, CTUL was the target of a multi-pronged attack by a large corporate opponent. CTUL’s executive director was personally sued and other staff and board members threatened with lawsuits, alleging that CTUL’s actions outside the stores represented trespassing and interfering with business functions. An injunction against these actions was imposed and restitution for loss of business income was sought. “We are not going to back down or soften our tactics,” said Brian Merle Payne, co-director of CTUL. “If we are being effective, we expect we’ll be attacked.”

Participation in Weathering the Storms: “When we learned about RoadMap’s Weathering the Storms project through the United Worker Congress, we jumped at the chance to learn more about the kinds of attacks going on. It definitely helps to know the types of tactics being used and what to watch out for. We also wanted to do all that we could to identify and address any internal vulnerabilities that we might have,” said Merle Payne.

“We learned that many things we had not paid much attention to because they seemed small or unimportant can be major liabilities. And

that our opposition will look for these kinds of things to try to discredit us or to tie up our time and money and ultimately to take us down,” admitted CTUL Co-Director Veronica Mendez.

CTUL recently gained a huge victory for sub-contracted janitors at retail stores in the Twin Cities metro area. Said Merle Payne: “We have much to celebrate but we also know this victory means we must be even more vigilant.”

Outcomes: Utilizing the WTS Checklist to identify areas of concern, CTUL used RoadMap’s consultant help to review and update its by-laws, personnel policies, volunteer screening and volunteer management systems, document security, and board governance policies.

PROFILE:

Prevention and Crisis Management Planning at 9to5 and the Family Values at Work Coalition



Photo Credit: 9to5

Organization: Founded in 1973, **9to5, National Association of Working Women's** mission is to build a movement for economic justice by engaging affected women in improving working conditions. 9to5's members and state chapters work to win family-friendly policies, such as paid sick leave, family-sustaining wages and strong wage theft protections. 9to5 works nationally, and has state chapters in California, Colorado, Georgia and Wisconsin. It's part of the national **Family Values at Work Coalition (FVAW)** and provides administrative services for the coalition. FVAW includes organizations in 21 states fighting for family-friendly policies.

Social Justice Impact: Recently, 9to5 chapters were actively engaged in large-scale voter registration and Get Out the Vote efforts in several states with close federal and gubernatorial races, including Colorado and Wisconsin. And the FVAW coalition has been at the forefront of recent victories, such as expanding coverage of the federal and state

“I also knew that 9to5 and FVAW are likely targets and that we would be foolish not to take advantage of the opportunity to minimize our risks and be prepared for opposition attacks.... Our management team found RoadMap’s Checklist and consultant assistance to be extremely valuable.”

—Linda Meric, 9to5

Family Medical Leave Acts and paid sick leave. For this work, they have come under attack from corporate interests, such as the National Restaurant Association.²⁷

The Attacks: RoadMap has worked with 9to5 and other FVAW affiliates to strengthen their organizations through Weathering the Storms. As such, they were better prepared when a coalition partner in Maine experienced a secret recording entrapment attempt by an opponent posing as a radio reporter. Groups working on elections in Colorado and Wisconsin were also able to thwart entrapment attempts.

Participation in Weathering the Storms: Linda Meric, executive director of 9to5, joined one of the Weathering the Storms webinars. “The information about the large number of attacks and the types of tactics really caught my attention,” she recalls. “I realized that opposition attacks were not only on the increase but that the tactics had become much more sinister. I also knew that 9to5 and FVAW are likely targets and that we would be foolish not to take advantage of the opportunity to minimize our risks and be prepared for opposition attacks.” Meric signed up 9to5’s entire management team for the second part of the webinar to ensure that more people in leadership understood the risks and the rationale behind investing time in crisis preparation.

9to5 has taken the WTS process seriously, using all the tools that RoadMap offers. “Our management team found RoadMap’s Checklist and consultant assistance to be extremely valuable. It helped us identify which of our policies and procedures were in really good shape, which could use some tweaking, and some that we needed to add to our organizational toolbox. We want to be sure that we have done all we can to minimize any internal vulnerabilities and to ensure that our staff, board members and volunteers are thoroughly trained to minimize risk and to be aware and ready for opposition attacks,” said Meric.

“We used and adapted RoadMap’s tools and advice to train, re-train, and document all our efforts to make sure our staff and volunteers knew the ‘dos and don’ts’ when engaging in electoral work,” said Linda Garcia-Barnard, 9to5’s national operations director.

Outcomes: 9to5 created a thoughtful Crisis Management Plan, trained all staff on the basics of the plan, and even integrated it into their new employee orientation. They have created crisis response messaging and will receive spokesperson training from a RoadMap communications specialist. These practices and policies will help 9to5 affiliates and the entire FVAW national network.

²⁷ www.familyvaluesatwork.org/wp-content/uploads/2011/10/NRA-CO-Report-and-Coversheet.pdf

PROFILE:

Crisis Communications planning at Worker Defense Project



Photo credit: Worker Defense Project

Organization: Worker Defense Project


(WDP) of Texas uses an effective mix of strategies to win protections for low wage workers, especially those in the construction sector. Through advocacy, organizing, direct services and developing grassroots leaders, WDP has become a powerful force across the state.

Social Justice Impact: WDP trains tens of thousands of workers on employment rights and educates contractors to address the interests of workers while building successful businesses. It has helped workers recover mil-

lions of dollars in back wages and helped improve safety practices in the construction sector. WDP was instrumental in winning Texas' first misclassification protection law, which imposes fines on employers caught misclassifying any workers on state contracts. It also helped win one of the nation's most progressive economic development policies, which includes living and prevailing wages, OSHA basic safety training, workers' compensation coverage, protection from misclassification for all workers, and incentivizing the hiring of "disadvantaged" (low-income/criminal record/without high school diploma) worker populations. WDP is part of a growing national movement redefining how to defend and advance worker rights.²⁸

The Attacks: Like other worker support organizations, WDP has faced a variety of threats from corporations, government officials, and business-backed groups, which accuse them of being a union-front group set up to circumvent union legal requirements, such as strict financial disclosure. Opponents charge that providing know-your-rights worker education or helping workers understand their options when abused is tantamount to practicing law without a license. WDP is also aware that the companies it has exposed for labor violations watch them closely and are ready to use any error or vulnerability to discredit the organization.

²⁸ www.nytimes.com/2013/08/11/business/the-workers-defense-project-a-union-in-spirit.html?pagewanted=all&_r=1&



Participation in Weathering the Storms: WDP attended the Weathering the Storms webinars and requested technical assistance as a way of doing internal due diligence. They wanted to ensure that internal systems stayed strong as they grew and wanted to create crisis response plans for current and future threats. WDP's senior team completed the WTS risk assessment checklist and used it to raise stakeholders' understanding of organizational strengths and weaknesses.

Outcomes: WDP established new policies and strengthened existing practices, including creating a formal document retention/email archiving protocol across all departments, updating the volunteer screening and training curriculum, and reviewing board documents, bylaws and the personnel manual for best practices.

Perhaps the most helpful part of the WTS project for WDP was the support from RoadMap's partner, **Camino Public Relations**, which worked with senior staff to create a comprehensive crisis communications plan. The communication team identified the most likely threats, outlined response plans and drafted messaging for each scenario. They then used these plans to train program and communications staff, creating a stronger set of internal protocols with more nuanced messaging, while also building confidence about how to handle any potential attacks.

"By working with the Weathering the Storms project we were able to shore up our internal procedures and develop a response to future attacks on the organization. The project gave us the tools we need to keep our organization secure as we continue to win important victories for workers in Texas."

—Emily Timm, Worker Defense Project

A LITTLE GOES A LONG WAY

From 2012-14, RoadMap learned from and supported more than 40 groups on a variety of technical assistance needs. The following examples illustrate the kinds of attacks groups experience and the ways in which a small investment of time and advice can help an organization before, during or after an attack.



RISK REDUCTION THROUGH AUDITS: CASA

“Like a lot of organizations, CASA had historically thought of the audit as something to suffer through. Our audit actually became one of our greatest weapons in proving that we had systems in place to avoid commingling of funds, appropriate tracking, etc. In the future, we would actually be even clearer with our auditors about these risks so that they focus in even more keenly on those areas that may be the source of attack. Also, at CASA, we had a somewhat segregated political reporting system and financial reporting system. What that meant was that completely different bodies in the organization were performing our financial reports and our ethics filings. We learned to centralize all of the filings.”

—Gustavo Torres, CASA, Executive Director

PREPAREDNESS IS STRATEGIC: RIGHT TO THE CITY ALLIANCE

“Understanding that one measure of our effectiveness is how much heat comes down on us from our opponents (and that what we don't know can hurt us), RoadMap's Weathering The Storms support has been immensely helpful in helping us identify potential vulnerabilities, strengthen systems and improve our preparedness. Our finance, admin and communications infrastructure keep us healthy and WTS has been an essential tune-up. The communities we are fighting for deserve nothing less than our best effort at this, and WTS is a critical tool for self-defense in the nonprofit terrain that we want our whole alliance to take up.”

—Mark Muyskens Swier, Right to the City Alliance,
Operations Director

ALLIANCE-WIDE SYSTEMS UPGRADES: PICO NATIONAL NETWORK

“Over the past few years, as PICO organizations have engaged in some of the most significant issues facing our country and led civic engagement campaigns in strategic states, we have anticipated and experienced attacks from the opposition. Preparing our organizations for these attacks and ensuring that we are in compliance as 501(c)(3) and (c)(4) organizations allowed us to focus on winning issue fights that benefit millions of families across the country.”

—Monica Sommerville, PICO, Director of Grants
Management and Compliance

BOARD GUIDANCE: CENTER FOR MEDIA JUSTICE

“At the Center for Media Justice/Media Action Grassroots Network, the board is using the WTS toolkit to guide its work this year with the goal of having all the items in place by the start of the next program year. It is so incredibly helpful to have all of the organizational requirements/best practices in one place, so we can just run down the list and check things off. It has been a strong tool for prioritization, as it showed where we're strong and exactly what we need to tackle to be more prepared. As our organization matures, this is one of the key things we need to progress to the next level.”

—Lisa Jervis, Center for Media Justice, Board
Member

IV. RECOMMENDATIONS TO SOCIAL JUSTICE ORGANIZATIONS, ALLIANCES AND FUNDERS



Photo Credit: National People's Action

- » If needed, shift organizational culture from denial or fear to proactive confidence that attacks can and must be prevented.
- » Make time to research your opposition and also to research your own organization through your opposition's eyes.
- » Follow the steps in this report and call in RoadMap support to ARMOR your organization.
- » Encourage allies and alliance affiliates to do the same.
- » Speak out and name those who use scare tactics to show that you are not intimidated.
- » Invest resources in technical assistance providers and field-building projects to keep your tools honed and to allow us to deeply support the groups that are most vulnerable.
- » Use peer-learning methods to stay up-to-date and spread Weathering the Storms practices across the movement.
- » When in doubt, get in touch with RoadMap by emailing weather@roadmapconsulting.org.

CONCLUSION

“[Climate change deniers are] many of the same people, and it’s almost an identical playbook. We try to lay out how you can just see this pattern used over and over and over again... they don’t have to win, they just have to create doubt and delay.”

—Robert Kenner, Director, *Merchants of Doubt*



Photo Credit: Josh Warren-White

Our organizations are not just fighting injustice; we are also often fighting lies. We know we are “right” in our positions but our opposition also knows that they don’t have to prove us “wrong” to be successful at undermining our work; all they have to do is stir up enough of a storm to distract, delay or conjure up clouds of doubt among those who might otherwise support us.

Unfortunately, too many of us are unprepared to weather these attacks in ways that refocus and strengthen our work while building greater confidence in our organizations. Lawsuits, digital surveillance, and PR attacks are on the rise. Forewarned is forearmed if we take these risks seriously and take the time to be prepared. Now is the time for social justice organizations

to make organizational armoring against crisis prevention part of everyday practices.

“The communities we are fighting for deserve nothing less than our best effort at this, and WTS is a critical tool for self defense in the nonprofit terrain.”

—Mark Swier,
Right to the City

There are three main takeaways from this report:

Preparing for attacks is a key part of organizational capacity, as essential as campaign development, financial management and strategic planning.

Preparation and response are most effective when approached holistically, integrating communications, organizational development and legal compliance.

Preparing for attacks can be done through simple steps over the course of several months with RoadMap Weathering the Storms support.

Mark Swier of Right to the City said it best: “The communities we are fighting for deserve nothing less than our best effort at this, and WTS is a critical tool for self defense in the nonprofit terrain.”

Together, we can strengthen organizations and alliances to build a social justice sector resilient to the coming storms!

WEATHERING THE STORMS PROJECT: 2012-14 Highlights

This summary offers an overview of the number of groups that have benefited from the Weathering the Storms project, average costs for the key components, and findings regarding key areas of need.

PARTICIPATION OVERVIEW

- » Organizations invited by one of the twelve initial funder partners: 750. Number of unique organizations: 649. Percentage of invited groups that participated in at least one component of WTS: 44.
- » Number of participants in Webinar Parts I and II in Sept 2012: 482 from 263 unique organizations.
- » Number of participants in the June 2013 Webinar: 100 from 68 unique organizations.
- » All participants were given access to a password-protected website to download the WTS Toolkit and view the recorded Webinars. As of March 2015, that site has had 1184 hits. Approximately 40 percent of the visits were in the three weeks immediately following the Sept 2012 webinars, with additional bursts in visits occurring after the June 2013 webinars and as RoadMap works with specific clients and alliances.
- » RoadMap has provided WTS Technical Assistance and training to more than 40 groups.

NEEDS ASSESSMENT SUMMARY

- » 49 individuals responded to the survey after the 2012 webinars (18 percent response rate).

- » 52 percent have experienced an opposition attack.
- » More than 60 percent indicated that they are working on an element of preparedness or would like help.
- » 63 percent of respondents had annual budgets under \$1 million.
- » 70 percent reported that they do not have (c)(4) tax status.
- » Most respondents said they do not feel confident that they are prepared to manage an opposition attack and were eager for guidance, especially on “how to start” being better prepared.

PRIORITY AREAS FOR PREPAREDNESS:

- » On organizational governance, more than 60 percent said that they are working on it or would like help.
- » In general, smaller organizations (a large majority of participants) do not have “at their service” financial or legal help that is free, immediately accessible, and able to deal with and understand issues as they may relate to opposition attacks and related crises.
- » Most groups do not have dedicated communications staff and little experience or connection to communications experts in case of attack.

WTS IS A HIGH IMPACT AND AFFORDABLE INVESTMENT IN CAPACITY BUILDING

- » Cost for delivering two rounds of the two-part webinars and producing the toolkit averaged \$178 per organization, or \$101 per person.
- » Tailored technical assistance packages ranging from 12-25 hours of phone consultation average \$2,500-6,000 for each organization. Funders or clients can contract for custom-designed packages.
- » RoadMap has provided two in-person WTS trainings: average cost \$7,500 for up to 40 participants per training, not including hard costs for participant lodging or travel.
- » Funders or clients can contract for custom-designed packages, including webinars, training, technical assistance, and peer-learning components.

WEATHERING THE STORMS

TOOLKIT: Table of Contents

For reference, the WTS toolkit includes checklists, templates and advice to armor your organization. RoadMap adds tools every year to the Toolkit.

Welcome

Introduction and Purpose
Acknowledgments
About RoadMap

Section 1: Getting and Keeping Your House in Order

- 1.1 Getting and Keeping Your House in Order: Our Top 12 Practices
- 1.2 A Guide to Getting and Keeping your House in Order
- 1.3 Working with Funder Allies
- 1.4 Best Practices for an Ethical Organization
- 1.5 Super Prepared Organization Sample Crisis Management Plan

Section 2: Crisis Communications

- Introduction
- 2.1 Crisis Communications Strategy Plan
 - 2.2 Crisis Communications Risk Assessment Tool
 - 2.3 Crisis Communications Knowledge Checklist
 - 2.4 Crisis Communications Infrastructure Checklist
 - 2.5 Sample Crisis Communications Plan: Civic Engagement Scenarios
 - 2.6 Sample Social Media Policy

Section 3: Key Organizational Policies

- Introduction
- 3.1 Elements of a Crisis Response Plan
 - 3.2 Sample Board of Directors Conflict of Interest Policy

- 3.3 Sample Whistleblower Policy
- 3.4 Sample Litigation Hold Policy
- 3.5 Sample Document Retention and Destruction Policy
- 3.6 Corporate Attacks: Limit your Risk
- 3.7 Volunteer Screening and Protocol
- 3.8 Sample Intern and Volunteer Questionnaire
- 3.9 What Should Be Included in a Volunteer Handbook? Sample Table of Contents
- 3.10 Sample Confidentiality Agreement for Volunteers

Section 4: Digital Security

Understanding Digital Security
Best Practices Checklists

Section 5: Various Memos, Tools and Documents

Understanding and Beating Back Opposition Attacks Memo
Scale of Organization Data Health Tool
C3/C4 Affiliated Organizations: Transactions Flow Chart

Section 6: Must Read Resources, Websites and Email Addresses

ACKNOWLEDGEMENTS

We thank the Weathering the Storms (WTS) consulting team and our organizational clients for sharing their experiences and paving the way for this critical work.

Our deepest appreciation goes out to all the social justice organizations that shared stories through our webinars and this report: CASA de Maryland, PICO National Network, Center for Civic Policy, Centro de Trabajadores Unidos en Lucha (CTUL), 9to5, National Association of Working Women, Workers Defense Project, Right to the City Alliance, Voces de la Frontera, Center for Media Justice, Asian Pacific Environmental Network, Progressive Leadership Alliance of Nevada, Florida New Majority Education Fund, Restaurant Opportunities Center, Coalition of Immokalee Workers, #BlackLivesMatter, Counsel on American Islamic Relations (CAIR), and Central Florida Jobs with Justice. More power to you as you continue to fight the good fight and weather the storms in your daily work.

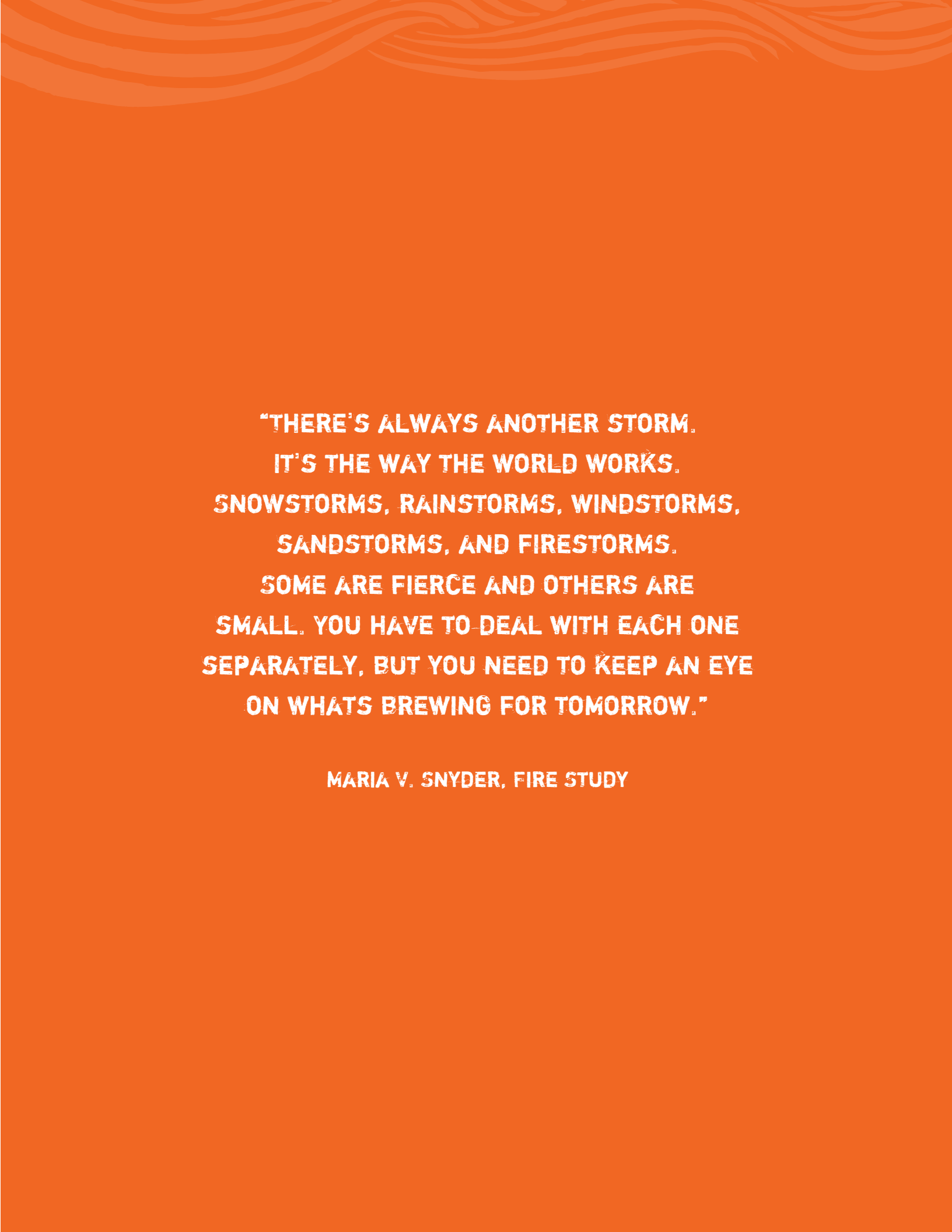
The impact of this project was brought to you in part by the expertise of our partners who applied their time, tools and services with great professionalism and care:

- » Alliance for Justice and its Bolder Advocacy Initiative
- » Camino Public Relations
- » Harmon Curran Spielberg & Eisenberg

We would especially like to thank Molly Schultz Hafid of the Unitarian Universalist Veatch Program at Shelter Rock for all of her cheerleading, fundraising and unflagging support for this project! Ever since the need for a project like WTS was identified in 2012, Molly has been our primary guide and ally. Molly successfully helped raise more than \$103,000 from peer funders for this project, contributed insight and knowledge to the creation of the webinar, toolkit, and technical assistance model, and continues to consistently remind the field that this work is critically important—and affordable, too.

And last but not least, this project would not have been possible without the generous support of these and other foundations that contributed to the Weathering the Storms pooled fund:

- | | |
|-------------------------------|---------------------------------------------------------|
| » Common Counsel Foundation | » Rosenberg Foundation |
| » The Discount Foundation | » Solidago Foundation |
| » General Services Foundation | » Surdna Foundation |
| » Hill-Snowdon Foundation | » Unbound Philanthropy |
| » The Needmor Fund | » Unitarian Universalist Veatch Program at Shelter Rock |
| » Public Welfare Foundation | |



**"THERE'S ALWAYS ANOTHER STORM.
IT'S THE WAY THE WORLD WORKS.
SNOWSTORMS, RAINSTORMS, WINDSTORMS,
SANDSTORMS, AND FIRESTORMS.
SOME ARE FIERCE AND OTHERS ARE
SMALL. YOU HAVE TO DEAL WITH EACH ONE
SEPARATELY, BUT YOU NEED TO KEEP AN EYE
ON WHAT'S BREWING FOR TOMORROW."**

MARIA V. SNYDER, FIRE STUDY



RoadMap's mission is to strengthen social justice organizations and the social justice sector through capacity building, peer learning and field-building.

Contact weather@roadmapconsulting.org to see how Weathering the Storms can help your organizations ARMOR up.

www.roadmapconsulting.org