DEFENDING DEMOCRACY COMES AT A PRICE; ITS DEFENDERS NEED SUPPORT

"In the long history of the world, only a few generations have been granted the role of defending freedom in its hour of maximum danger."

John F. Kennedy, Inauguration Address, January 20, 1961

"*At what point then is the approach of danger to be expected? I answer, if it ever reach us, it must spring up amongst us. It cannot come from abroad. If destruction be our lot, we must ourselves be its author and finisher*."

Abraham Lincoln, Lyceum Address, January 27, 1838

While it has become axiomatic in many quarters that democracy remains under threat, less attention is paid to those engaged on the front lines combatting that threat – the defenders – and even less attention is paid to the toll that such defense can take on the defenders and often their families. As one senior researcher on far-right extremism recently told me, "too many politicians, journalists and even researchers are stepping back from their work due to the hate, harassment and intimidation campaigns they face." As a democratic society that greatly benefits from the actions of defenders, it behooves us to consider how best to defend the defenders.

The Landscape

The threats to democracy are manifold. While the threats most likely to command our attention these days relate to elections (*see, e.g.*, Protect Democracy - Campaigns & Coalitions) and fit relatively neatly into a political paradigm (the slide into autocracy – *see, e.g.*, The Authoritarian Playbook, published by Protect Democracy), the threat landscape in fact is far broader, targeting, beyond elections,

- public health *(see* "Combatting Misinformation as a Core Function of Public Health" published in the New England Journal of Medicine and "Public Health Agencies Try to Restore Trust as They Fight Misinformation" published by the Kaiser Family Foundation);
- climate change (*see* ISD digital dispatch on mainstreaming climate scepticism);
- members of the Jewish, Muslim and AAPI communities (*see* ADL Audit 2022);
- human rights activists (*see* Joint Statement on Protecting Human Rights Defenders Online, published by the US and EU governments);
- LGBTQ activists (*see* ISD digital dispatch on anti-LGBTQ hate);
- asylum seekers (*see "*Disinformation on Migration: How Lies, Half-Truths and Mischaracterizations Spread" published by the Migration Policy Institute);
- women seeking abortions (*see* Proposed Legislation); and
- even women running for political office (*see* ISD digital dispatch on abuse targeting female politicians).

These threats manifest themselves across multiple ecosystems, starting with online harassment and disinformation/misinformation campaigns, amplified by the algorithms deployed by social media platforms and by media organizations. (Unfortunately, coming to a

(digital) screen near you, AI-driven threats are just around the corner.) Extremist, terrorist, misogynistic and hateful content remains broadly available on online platforms (*see* ISD digital dispatch on terrorist content and ISD digital dispatch on antisemitism).

As for those multiple ecosystems, we are witnessing:

- growing levels of polarization, acceptance of anti-democratic sentiments and acceptance of political violence;
- increasing levels of hate-fuelled violence (including mass shootings);
- greater prominence of domestic violent extremists and groups (*see* ISD digital dispatch on hybridized extremism);
- the continued promotion of election denial and conspiracy theories;
- the continued promotion and enactment of state-level legislation that restricts voting, that seeks to puts election outcomes into the hands of legislatures and that criminalizes election assistance;
- ongoing threats of violence against, and intimidation of, election workers (*see, e.g.*, reporting by Matt Vasilogambros in the Pennsylvania Capital-Star ("For local officials, the fight against election lies never ends" – March 2023)); and
- the decline of authoritative institutions, including news organizations, schools and universities. Academic freedom is under sustained attack, and culture wars are driving threats to school boards, the banning of books and the silencing of teachers/professors.

  As concisely summarized by Sharon Davies, CEO of the Kettering Foundation, more than 35 states have taken steps to restrict classroom discussions of the nation's history of racism; there are bills forbidding teachers from offering instruction that "promotes division" between the races, or "promotes resentment" of a particular race, or teaching that causes student discomfort due to their race. Other legislation targets teaching about sexual orientation or instruction that promotes gender fluidity. These restrictions are particularly damaging in light of disproportionately high rates of suicide/suicide attempts in the LGTBQ community.

Interestingly, some experts note that levels of participation in white nationalist, neo-Nazi and anti-government extremist groups in the United States have been falling (s*ee, e.g.*, "The Year in Hate & Extremism 2021 published by the Southern Poverty Law Center) as right-wing extremism becomes mainstream.[1] According to supplemental 2021 data released two weeks

[1] In Mainstreamed Extremism and the Future of Prevention, the Institute for Strategic Dialogue (ISD) posits that "Today extremism and terrorism are ideologically multifaceted, hyper-charged by digital platforms, and inseparably connected with the rising phenomena of disinformation, conspiracist mobilisation and weaponized hate. Far from being an issue at the fringes, extremism is increasingly characterized by a 'mainstreaming' dynamic, with mobilization taking place through political and media channels to reach wider audiences, polarizing civic discourse and undermine democratic culture and process."

Counter-extremist expert and ISD Senior Research Fellow Julia Ebner, in her new book, "Going Mainstream: How Extremists Are Taking Over," tracks how incels, anti-vaxxers, conspiracy theorists and neo-Nazi once existed on the fringes of the political spectrum. Today, accelerated by the pandemic, global conflict and rapid technological change, their ideas are becoming more

ago by the FBI, the number of hate crimes in the United States surged in 2021 and set a record of nearly 11,000 incidents. This was the largest increase in more than three decades, driven by a 28% increase in anti-Jewish attacks and a 40% increase in anti-gay attacks (*see* reporting by Masood Farivar for the Voice of America (March 2023).

Defenders of democracy can include journalists, academics, election administrators and other election workers, civil society organizations ("CSOs") and political/campaign organizations. CSOs can be focused on countering disinformation, for example, through fact-checking, digital forensics and research, public digital and media literacy campaigns, government advocacy, coalition building and mobilization of responses to disinformation campaigns. (*See* "Building Civil Society Capacity to Mitigate and Counter Disinformation" (CEPPS).) CSOs can operate in the online space (monitoring social media across platforms) or in the offline space (*e.g.,* by infiltrating hate or other extremist groups, incidentally not to be confused with infiltration by undercover agents from the FBI and other law enforcement units).

Vulnerabilities of Democracy Defenders

The challenge is that many civil society and other non-governmental defenders lack the resources to protect themselves while undertaking their work. ISD identifies four areas that highlight the vulnerability of democracy defenders:

Legal defense

Defenders are potentially vulnerable to a range of malign actors, which can be individuals, organized groups or hostile state actors. In many cases these malign actors have significant resources, or at least greater resources than the defenders they target.

Among the weapons at the disposal of malign actors are strategic lawsuits against public participation (or SLAPPs) to dissuade critics from speaking out in public. According the authors of "Getting Sued for Speaking Out," George W. Pring and Penelope Cann (who coined the acronym in 1996), SLAPPs convert a topic of public interest into a private lawsuit, substituting a legal context in place of a political framework. In the words of the Ninth Circuit, SLAPPs "'masquerade as ordinary lawsuits' but are intended to deter ordinary people 'from exercising their political or legal rights or to punish them for doing so.'" These vexatious lawsuits can have a chilling effect on defenders either because of the outcome of the lawsuit, but more often simply because of the litigation process, as defendants are forced to expend time and money to respond to these actions in court. SLAPPs can target reporters, journalists, authors, bloggers, lawyers and community activists – anyone speaking in the public space – all too often leading to self-censorship.

The good news is that a growing number of states (as of October 2022, 32 states and DC) are passing anti-SLAPP legislation, although they vary significantly in scope. (*See* Anti-SLAPP Legal Guide published by the Reporters Committee for Freedom of the Press.) Commentators have suggested that federal legislation is needed to provide protection in federal courts– one such bill was proposed in the last Congress.

---

widespread. She notes that QAnon proponents run for Congress, neo-fascists win elections in Europe and celebrity influencers spread dangerous conspiracy theories.

Cybersecurity

Digital assets and infrastructures of defenders are vulnerable to online attack. These attacks can target the organization or individual staff members. Protecting assets and infrastructure can require third-party monitoring services, antivirus protection of systems, and staff time to respond to attempted breaches of systems. Defenders also need ongoing surveillance and system fortification for their staffs and online profiles.

In February, federal officials warned attendees at the National Association of Secretaries of State and the National Association of State Election Directors conferences that foreign and domestic actors continue to pose national security threats to election systems. The FBI Cyber Division warned that national security officials remain concerned about interference from China, Iran, North Korea and, especially, Russia. "Every day, cyber threats increase." (*See* Pew Stateline Article by Matt Vasilogambros.)

Incidentally, deep fake/shallow fake technologies, exponentially augmented to the surprise even of experts by AI, compound the risks, and the legal system has not kept up with the technology to provide adequate remedies to deter or sanction those deploying these capabilities for malign purposes. As Naz Gocek notes in "Deepfakes Versus Democracy" (Rewired – August 2020), close scrutiny of the incendiary intersection of deepfakes, disinformation and democracy is timely ahead of elections. (*See generally*, Stuart A. Thompson's "Making Deepfakes Gets Cheaper and Easier Thanks to A.I." (New York Times – March 2023) and Adam Satariano and Paul Mozur's "The People on Screen are Fake. The Disinformation is Real" (New York Times – February 2023). (For a layman's description of the impact of AI, try The AI Dilemma, a podcast from Your Undivided Attention.)

Physical security

Defenders face off-line threats to facilities and personnel, which often requires CCTV equipment, alarms and physical security at office and at homes.

The Big Lie disinformation campaigns prompted armed protesters and violent harassment and threats against local and state election officials (particularly women), in turn leading of necessity to threat assessments, coordination with local law enforcement, and de-escalation and active shooter training.

Concerns have not diminished (*see, e.g.*, "Security Concerns Top of Mind as 2024 Election Approaches" – National Conference of State Legislatures (February 2023)). The Department of Justice and the FBI set up the Election Threats Task Force in 2021 and, in February, 24 Democratic US senators wrote to DHS Secretary Mayorkas, CISA Director Jen Easterly and FEMA Administrator Deanne Criswell urging DHS to prioritise funding for election security and support of election officials, framing election security as a matter of national security.

But there is, as Matt Vasilogambros reported and I have heard anecdotally, palpable distrust in federal law enforcement. Interestingly, there appears to be significant appetite among state and local law enforcement for training around the threat landscape as well as actionable information.

Mental health and wellbeing

Exposure to extremist and hate content, or online or offline harassment or threats, can take a significant toll on mental health and wellbeing of personnel. This requires offering a range of mental health and wellbeing services, including counselling, which requires both funding of programs and benefits, as well as internal staff time.

In addition to the foregoing (though beyond the scope of this note), I should note that defenders operating in a number of countries face even greater threats to personal safety, including kidnapping, imprisonment and assassination.

Applying Technology in Aid of Democracy

Attacks against election officials and elections, perhaps, are the most visible manifestation of the threat, particularly cyber and physical threats. Significant numbers of election officials have left due to over two years of harassment, burdensome frivolous records requests and lack of support from law enforcement. But elections should not obscure the scope or the depth of the balance of the challenges – there is a broad swath of the threat landscape that touches countless other areas and many of defenders in these spaces benefit from neither the attention nor the resources being deployed around elections.

I recently attended the finals for the Tech4Democracy competition (run by IE University in partnership with the State Department and Microsoft) that promotes democracy-affirming technologies – in short, digital technologies that contribute to the advancement of democracy around the globe. Funding for start-up efforts could go a long way to help deploy technology in aid of the defenders of democracy. This effort is part of a broader ecosystem that recognizes that concerted collaborative action is needed, which prompted the Danish Foreign Ministry to launch the Copenhagen Pledge. The pledge is a commitment to make digital technologies work for, and not against, democracy.

This past week, the State Department, in connection with the 2023 Summit for Democracy, published a Fact Sheet ("Private Sector Commitments to Advance Democracy") summarizing commitments received from private sector participants in four areas: advancing technology for democracy; fighting corruption; protecting civic space and human rights defenders; and advancing labor rights. (*See also* White House Fact Sheet ("Advancing Technology for Democracy").)

While the focus of the commitments, not surprisingly, is global, there are significant domestic analogues. The commitments include:

- endorsing a set of principles for companies to counter the misuse of their products and services to harm people, and specially to counter the "cyber mercenary" commercial spyware market;
- supporting digital security and safety helplines to assist those vulnerable to doxxing, harassment and account hacking, and providing security keys to individuals at high risk of cyberattacks, such as journalists, researchers and human rights defenders;
- engaging the private sector as advocates for transparency and accountability and identifying and disseminating private sector practices to combat corruption;

- supporting journalists investigating corruption, including training focused on digital safety to help them map personal risks, training on cybersecurity defense and strengthening capacity to safely investigate state abuse of public resources;
- providing training, resources and legal support to journalists and CSOs to mitigate the risk of SLAPP suits and providing legal defense and assistance to respond to threatening and commenced legal proceedings;
- convening business leaders to promote through their businesses education on the state of democracy and opportunities for engagement; convening private sector leaders on the need to protect businesses from government interference in their ability to conduct business and speak freely; and amplifying business leaders' voices on the mutually beneficial connection between a strong democracy and a strong, stable economic climate, and the risks to the private sector when civic space is weaponized by those who would undermine democratic institutions;
- providing post-quantum cryptography to artistic groups, journalists, humanitarian organizations and voices of political dissent that are the targets of DDoS and other cyberattacks as well as to operators of elections websites;
- supporting independent media, particularly in resource-poor and fragile settings; and
- convening roundtables on how best to deploy blockchain technology to support human rights, transparency and sustainability, including applications to promote government accountability, fight disinformation, reduce data manipulation and track illicit finance flows.

Concluding Thoughts

What unifies the disparate groups of defenders across the country and the globe, and across the entire ecosystem of civil society, is vulnerability they and their families face. This may seem, particularly in the United States (after the midterms), to be overstating the scope and the disruptive impact of threats. But these threats are very real, and there are very real people who face these threats on a daily basis. Some signed up to be activists, but many others signed up to be public servants, journalists, researchers, public health workers, election workers and the like, and for them simply doing their jobs became an operational hazard. Yet others who have chosen to fight back were ensnared in conspiracy theories and became, wholly unintentionally, casualties of the seemingly never-ending battles in the cultural wars blighting society.

My focus on technology is not accidental – principally because what has turbo-charged attacks that these defenders face is technology – the internet and surveillance technology. The spread and amplification of misinformation and disinformation has gone mainstream. Disinformation fuels weaponization of hate, death threats and threats of rape, coordinated misogyny and other forms of intimidation and harassment, doxxing and actual physical violence. On the receiving end, it can lead to, and is leading to, self-censorship and resignation from positions in public life (particularly among women), and more broadly a loss of trust in the ability of government institutions to protect citizens.

In a prior briefing note, I focused on interventions to reduce polarization and anti-democratic sentiment (available here), and while I am hopeful that these will, over time, reduce the efficacy among a more digitally aware population of disinformation and other malign tactics,

those promoting the threats to democracy are unlikely to pack up and go home. The defenders will need all the help they can get.

For those willing to invest in the protection of democracy, a good place to start is to consider how best to ensure that those on the front lines can continue the battle with fewer concerns about their vulnerabilities.

* * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
April 2, 2023