OSET INSTITUTE

TRUST THE VOTE PROJECT

2022 Copenhagen Democracy Summit

Special Invitational Meeting on the Future of Disinformation
Introductory/Opening Remarks

Edward "Eddie" P. Perez
Board of Directors, OSET Institute, United States

William P. Crowell
Board of Directors, OSET Institute, United States

Eddie Perez:

Thank you all for joining this evening's conversation. I am grateful to be in a room of people who have dedicated themselves to advancing and preserving democracy. Given the multi-pronged attacks it's currently suffering—pernicious corruption, rising authoritarianism, and even war—we defenders of democracy each have our role to play in this challenging time, and we must continue standing in solidarity with each other and our various projects. Some of us are leaders who can advocate for democracy culturally and politically. Others develop policy that informs legislation to protect and secure democracy. Still others, the OSET Institute among them, focus on the technology of democracy administration.

Today, we are besieged by a cyber arms-race to defend democracy from threats to election integrity, and disastrous disinformation and misinformation. I can also assure you, given my responsibilities as a Director at Twitter, where I help lead product efforts to promote healthy public discourse on civic matters, that the threats of technology-driven anti-democratic propaganda are clear and present. These digital disinformation weapons pose perhaps the most insidious, pervasive, and subversive danger to all liberal democracies.

If we are to address these threats, however, it must be emphasized that disinformation is not fundamentally a technology problem. I'll say that again: *Disinformation is not a technology problem*. Disinformation is a societal problem. It is born of geopolitical competition and perverse incentives to divide populations along invidious lines of polarized politics and identity; these dangerous and anti-democratic impulses are part of the human condition, and today's technology and AI are accelerating the harm they inflict. Treating the symptoms of the digital disinformation disease will require our most innovative technical thinking to protect media platforms. But addressing the fundamentals of this problem requires an even larger, more holistic perspective. Some of the most important work to be done lies not in machine learning, for example, but in greater sunlight and public understanding about civic processes, and greater protections for the human beings that administer democracy.

For my part, I serve on the board of the Open-Source Election Technology (or OSET) Institute because, as a former director of technology and standards for the Institute, and before that, 8 years in product management at one of the three U.S. based voting systems manufacturers, and I can assure you that developing innovative public election technology can help restore faith in democracy, by ensuring elections are verifiable, accurate, secure, and transparent. Investing in open-source election technology has to be a pathway we embrace.

For the OSET Institute, we are focused on attacks on the processes of election administration, vote counting, and result reporting; and this includes the people directly responsible for administering elections.

It has become a dangerous and frightful situation not only in the U.S; baseless challenges to election results and specious, deceitful claims about integrity are all too common worldwide. And as mis- and disinformation reaches more individuals in increasingly polarized environments, the risk of insider threats to election administration increases as well. The difficulty is that legitimate questions can arise for which election verification is essential; and the challenge is separating fact from fiction. We believe that more transparent election administration technology can advance this goal.

For our part in the conversation, we have among our team here and on video link, subject matter experts on the technological aspects including a Board member of OSET that several of you know, Mr. William P. Crowell, who has had a long and distinguished career in national intelligence and security. Bill, please add your thoughts.

William P. Crowell:

Thanks, Eddie. While Eddie Perez's statement that "*Disinformation is not a technology problem*," is basically true, it is also unquestionably true that technology provides powerful tools for the spread of disinformation to ever wider audiences.

Having served in national security and intelligence positions most of my life, I have personally witnessed the growing threats that disinformation presents to our nation's political systems and to those of our fellow democracies around the world.

In my early years as an intelligence officer, I worked on counterintelligence problems and was regularly confronted with the details of disinformation campaigns run by foreign intelligence organizations. They were often constructed in a very exacting manner to target key parts of our democratic processes and to undermine our confidence in the integrity of our election systems. While the campaigns sometimes showed a surprising understanding of how our systems were administered, they often failed because of flaws in their execution.

The disinformation campaigns also suffered from one other failing: the lack of satisfactory means of distributing the bogus information to national level audiences. The primary methods of distributing disinformation messages at the time were limited. Today that is no longer the case. Today there is the Internet.

The Internet at times seems to have been invented to make the distribution of disinformation more efficient and more effective. It also offers a vast array of ways to distribute disinformation and to amplify the resulting messages without attribution.

With the Internet as the primary means of distributing and amplifying disinformation, the emphasis by our adversaries has now shifted to developing improved messaging methodologies where whole segments of the population can be led to believe conspiracy theories, even when there is not a shred of evidence to back them up. So called "deepfakes" can now be constructed to carry convincing video and audio messages from well-known individuals in our society to audiences eager to accept them as real. Hate groups can be heralded as heroes who are just trying to preserve our "*way of life*."

Democratic institutions are in the crosshairs of these attacks.

We are seeing ever increasing targeting of both our election systems and the people who administer them. In essence, elections can be influenced, given enough knowledge of the key societal buttons to push and the resources needed to amplify the key messages of a well-constructed disinformation campaign.

During the 2018 mid-term elections in the United States, it has been reported that the Russian Internet Research Agency, an alleged social media disinformation troll factory linked to the Russian government, planned to influence our elections, as they reportedly had done during the 2016 elections. According to the Washington Post, on the eve of the election, the U.S. Cyber Command mounted an operation to deny the IRA access to the Internet, thereby shutting down their efforts to undermine trust in the integrity of our elections.

While I cannot comment on the specifics of this story, I can say that *long-term deterrence of disinformation campaigns against our democratic institutions is not easily achieved*. The cost of mounting such disinformation campaigns is very low and the impact of such attacks can be very high. There are few disincentives to the use of disinformation to spread distrust and undermine democracy. Now, with the advent of Artificial Intelligence and Machine Learning, it is not only possible to create and distribute very convincing *narratives*, but also to automate the entire disinformation plan and its execution.

Attribution to the perpetrators can be very difficult at best. And with the right planning and timing of the execution of these attacks, there is very little time available to mitigate the effects.

We are at the dawn of a new era in the *digitalization of practically everything*, but there is very little effective attention being paid to the security of information and to the means of verifying its authenticity. This is a serious problem for the preservation of our democratic institutions. We must face these dangers by creating more powerful mechanisms for determining what is real and what is not real information. Cybersecurity, AI and machine learning will become the essential tools for building these mechanisms to secure our future.

Eddie Perez:

Thanks, Bill. For our contributions to this evening's conversation, and to the cause of fighting, if not eradicating disinformation and misinformation about election administration, the OSET Institute is focused on two initiatives:

1. Delivering new public open-source election verification technology; and
2. Improving public education on election administration processes.

Nevertheless, the digital tools of disinformation are rapidly evolving and increase the appearance of legitimacy of claims, stories, and staged data and evidence—*this is a dire moment*. We must never allow normalization of such subversive actions.

On behalf of the OSET Institute, we're honored and humbled to join in this discussion and the on-going work to increase confidence in elections and their outcomes, in defense of democracy, and as a matter of any nation's sovereign right and security.