Multi-Stakeholder Insights

A Compendium on Countering Election Interference

Microsoft

alliance for securing democracy
G|M|F

Canada

Introductory Letter

Governments, civil society and industry recognize the importance of a secure, stable and accessible cyber and digital information space, especially in today's challenging and unpredictable environment.

In November 2018, the French Government launched the Paris Call for Trust and Security in Cyberspace (Paris Call), recognizing that "cyberspace now plays a crucial role in every aspect of our lives" and that "it is the shared responsibility of a wide variety of actors from all sectors to improve trust, security and stability in cyberspace."

The Paris Call is the largest multi-stakeholder cybersecurity voluntary agreement, supported by over 1100 entities internationally, including over 75 governments and hundreds of industry and civil society organizations. It relies on a set of nine principles to secure cyberspace, and provide guidance on discussion and action related to cyber threats including those related to election interference.

As co-champions of Principle 3: Defend Electoral Processes under the Paris Call, the Alliance for Securing Democracy (ASD), the Government of Canada, and Microsoft are working together to strengthen our collective capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

Trust in the electoral process and in the legitimacy of electoral outcomes is fundamental for democracy. Securing democratic institutions from interference requires the smart use of technology, and new models of partnership and cooperation given the ways that the challenge of interference in our democratic institutions crosses all sectors of society. At a time when trust in our institutions is being challenged on so many fronts, bringing a broad range of stakeholders together to increase our resilience in the face of these evolving threats will help ensure citizens can continue to have confidence in how their representatives are chosen.

Throughout 2020, the co-champions brought the global community together through the organization of multi-stakeholder workshops, each one addressing a critical topic related to preventing interference in electoral processes. During these workshops, key observations, ideas and effective practices were collected from a diverse group of experts, practitioners and stakeholders. Based on what we heard and learned in these discussions, we have developed a compendium of good practice that offers election management bodies, governments and other democratic stakeholders a useful resource to support their efforts to safeguard elections and democracy.

The insights and ideas heard in these discussions and reported in this compendium reflect the diverse perspectives and expertise of a truly multi-stakeholder group, not necessarily the views of individual participants or the co-champions. Yet, it is for this very reason that this multi-stakeholder approach to electoral security is so crucial. Indeed, as election processes vary greatly across jurisdictions – along with threats and vulnerabilities – this compendium recognizes that there is no "one-size fits all" approach to protecting democracy. However, by working together as we have done here, we will continue to build global expertise and understanding of ways to counter interference that are effective and appropriate in different situations.

As cyberspace becomes an increasingly important venue for the exercise of democracy and one of the greatest conduits for threats to it, we stand committed to protecting elections from foreign interference and offer this compendium of good practice to those who are working to do the same. Our collective efforts to maintain trust in our democratic institutions will help ensure citizens remain engaged and informed – which in the end is democracy's best defence.

Brad Smith,
President,
Microsoft

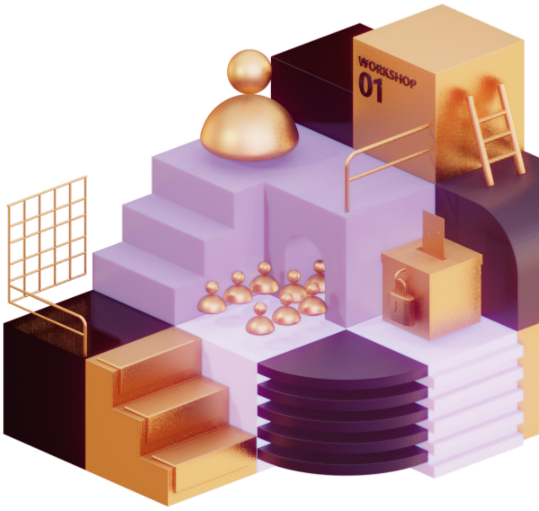
Karen P. Donfried

Dr. Karen Donfried,
President
The German Marshall Fund of the United States

The Honourable Dominic LeBlanc, P.C., Q.C., M.P.
President of the Queen's Privy Council for Canada and Minister of Intergovernmental Affairs

Contents

Workshop 1: Improving Multi-Stakeholder Information Sharing



Bringing communities together to tackle threats and identify practical solutions can help to build resilience against hybrid threats. In many places, intelligence services and electoral authorities are not familiar or in regular contact with each other. Lack of resilience is a bureaucratic vulnerability, however ongoing efforts to break down silos, within and between both the public and private sectors, can help to alleviate it. The challenge of information sharing becomes even more significant between the public and private sectors.

When it comes to determining vulnerabilities, consider the ecosystem holistically– every part of the electoral cycle is potentially vulnerable to interference and in need of protection. It is also important to recognize that interference comes from both state and non-state actors. Interference is not necessarily a singular event; rather, it can be the cumulative effects of individual acts that in the aggregate add up to an impactful act of interference, which can include cyber interference and disinformation. Disinformation in the election environment is often a good indicator that wider hybrid threats are at play. As democracies suffer the impact of this aggregate effect, it is important to develop a shared language to discuss threats, threat actors, and responses – something that is currently lacking. Lastly, it is important to recognize that just as responses continue to improve, threats constantly evolve.

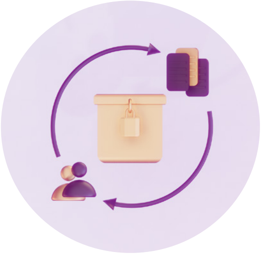
Effective Practice:

Build Multi-stakeholder Relationships

First, it is important to identify points of contact across government, civil society, and the private sector early, and manage the size of this group. Once these points of contact are identified, keep lines of communication as simple and direct as possible and create clear expectations about information sharing, including threat trends and tactics, techniques, and protocols. To ensure continued communication during the election period, venues and platforms should be provided for multi-stakeholder cooperation in advance of and during election events. Additionally, these relationships can be enhanced by conducting joint scenario planning and rapid response exercises to develop an understanding of how people and organizations will respond. For additional perspectives, cooperating with like-minded countries is valuable as the problems of each individual state are not unique- there are advances that everyone can make together by sharing lessons learned and exploring opportunities for joint action.

Intra-government Coordination

Building inter-agency cooperation early and seeking support from the top (e.g. cabinet level) help ensure constant communication. Some examples of important connections to make include: Electoral management bodies (EMBs) and national security technology experts; intelligence officers and communication specialists; central agencies at the intersection of the public service and political actors; and outreach specialists who engage vulnerable groups. For the election period, it is valuable to create a non-partisan expert group that is tasked with collecting and assessing reports of election interference and notifying the public when interference has occurred. This encourages public servants to come forward with information without a threat of politicization. Lastly, it is critical to be inclusive and comprehensive by engaging with all political parties, including the smaller and lesser known parties, to ensure all involved know what steps to take and whom to contact in the event of an incident. Moreover, it is valuable to consider shared resources for smaller agencies and localities such as "Cyber Navigator" programs, which help election authorities to defend against cyber breaches and detect and recover from cyber-attacks. These create a single point of contact to the private sector and allow for greater specialization.



Develop Methods for Communication

Across all efforts, communication should be in simple language and in a manner that provides citizens with tools for increasing their resilience against interference. Additionally, consider the audience and identify opportunities to educate and communicate. At every opportunity, improve and publicize methodology on what constitutes interference and influence, not only in the information space but also in the tech field. First, build relationships and communicate with the media early but be aware that media can also be a vector for interference if it is manipulated. Next, classify reports at the lowest level possible to maximize their reach. When events do occur, consider the power of attribution. Actions by government, private sector, and civil society organizations will have different political impacts, and each should be as transparent as possible in their standards and methodology.

Consider that when an entity is the victim of interference, it places those affected at the center of conversations. As victims they have the power to release private sector and government actors from obligations that would otherwise prevent information-sharing; use lines of communication and communities built through communication to use these situations effectively and with impact. Users should be notified not only when there has been a successful breach, but also when there is an attempted compromise successfully thwarted.

Finally, create a repository of good practices that all countries can draw on so that this information does not depend solely on individual relationships. This is especially important for smaller states, which may have fewer internal resources to draw on or more limited experience from which to learn.

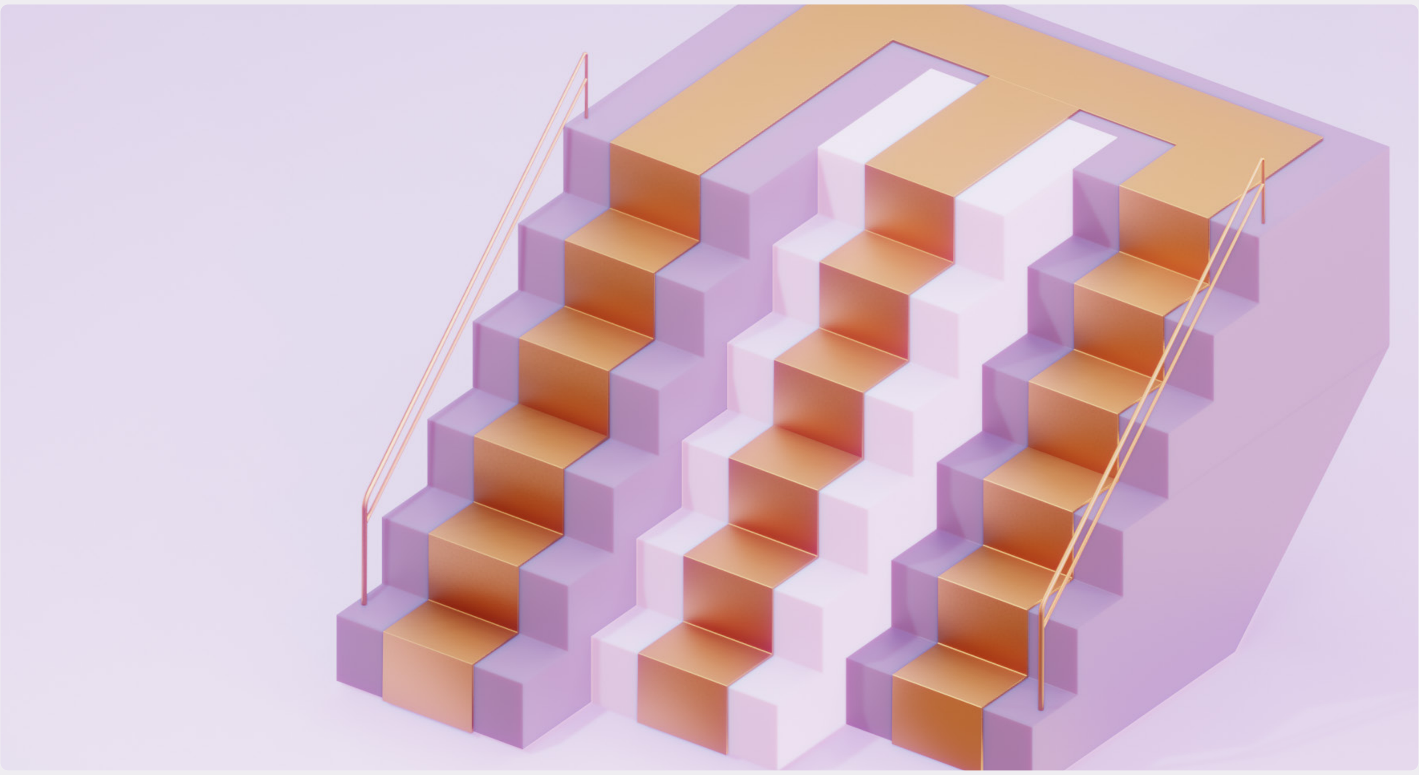
Public-Private Coordination on Policy Changes

It is important to give the private sector enough time to absorb changes to rules, and to be aware that sometimes big companies will have an easier time adapting than smaller businesses.

Workshop 1

Three Ways to Enhance Cooperation in Order to Safeguard Democratic Processes

During 2019 and 2020, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) ran a project focused on countering electoral interference in our participating states. This involved seminars, conferences and practical exercises with participants from our participating state governments, private sector companies and academia. The work centred on finding practical ways to counter electoral interference and the three good practices listed below are a distillation of our experience from this project. They take a multi-stakeholder approach to countering electoral interference by establishing situational awareness, enhancing understanding and enabling an effective response to malign activity.



The Hybrid CoE safeguarding democratic processes project will continue in 2021.

Further work, including the full version of this paper, will be published on www.hybridcoe.fi in the coming months.

1.
Developing a government fusion cell ahead of elections helps establish situational awareness.

The fusion cell should primarily be focused on monitoring the information environment ahead of and during elections. The team can consist of computer emergency response team (CERT) members, strategic communicators, open-source intelligence analysts, the intelligence community, the foreign ministry and the government authority in charge of holding the election. One should think laterally about team composition, beyond traditional security ministries, and consider including practitioners who can offer a broad variety of views.

2.
Joint exercising enhances understanding.

Exercises where a variety of actors, such as social media companies, media outlets and academia are present have proven valuable opportunities to identify key concerns and risks, and practice joint response, ahead of the election itself. Exercises are an opportunity to familiarize oneself with the way other organizations, such as social media platforms, work. They also provide an excellent forum to engage with various stakeholders, ask questions, and build trust.

3.
Early engagement across different stakeholder groups ensures effective response.

Many countries are part of multilateral cooperation mechanisms aimed at countering the threat of election interference. Often these mechanisms have links to the private sector and may serve as useful routes to build connections with social media platforms. Contacting peer states that have recently held elections can enable an exchange of valuable experience and good practice, for example on new trends or tactics that will be useful to be aware of when preparing for elections. Members of academia might be able to brief government practitioners on their view of risks related to an upcoming election. The important outcome is that relationships and mutual trust are built well ahead of elections. Trying to build relationships in a crisis can be ineffective and puts a timely response to malign activity at risk

Lina Rosenstedt –
Project Co-ordinator,
The European Centre of Excellence for Countering Hybrid Threats

Workshop 1

A Case Study from Finland

Finland: Cooperation Group on Election Security Preparedness

To be able to maintain the stability of the electoral system in the changing operating environment, ongoing cooperation between the authorities and a better understanding of election interference is required.

Therefore, the Ministry of Justice Finland (MoJ) has appointed a cooperation group on election security preparedness (2.3.2020 - 30.6.2023). The cooperation group is based on the Ministry of Justice's training project, which operated from 2018-2019 and focused on raising awareness of election interference. The training project concluded, for example, that a permanent cooperation group would support a more long-term perspective and faster responses in the changing information environment, also between the elections. The cooperation group is also linked with the national Democracy Programme 2025, which includes measures to strengthen democracy and participation.

The tasks of the cooperation group on election security preparedness include

- to follow the international debate and developments related to election interference and election security between national elections, in particular by participating in the work of the European cooperation network on elections,
- to improve the exchange of information about changes occurring in information influence activities, hybrid threats, cyber security, and society, which may affect the conduct of elections or the public confidence in elections,
- to provide expertise and coordinate cooperation with other key stakeholders in elections,
- to support the Ministry of Justice and other election authorities in improving election security.

Heini Huotarinen
Ministerial Adviser, Ministry of Justice

Johanna Kaunisvaara
Project Manager, Ministry of Justice

Workshop 1

A Look at the 2020 U.S. Election - What Went Well: Improved Cross-Sector Communication about and Public Exposure of Foreign Interference

In the months leading up to the U.S. 2020 election, government, media, and private sector actors took proactive steps to communicate with the American people about the developing threat of foreign interference.

In 2020, government actors regularly communicated with the public about malign actors and activity.
Officials from the Office of the Director of National Intelligence (ODNI), FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and others provided regular public updates highlighting threat actors, exposing influence efforts and activities, flagging potential avenues for interference, and updating the public on the steps that federal agencies were taking to secure the election.[1]

In the wake of an Iranian campaign to impersonate a far-right group and intimidate voters, U.S. officials provided rapid attribution for the operation, publicly identifying the Iranian effort within 27 hours of the incident—the fastest disclosure of attribution by U.S. officials to date—quickly informing citizens.[2] Officials also reassured the public that the Intelligence Community "caught this activity immediately," and "acted swiftly in response to the threat," and the FBI and CISA followed up days later with a cybersecurity advisory revealing how Iranian actors had accessed voter information and providing guidance on mitigating the threat.[3]

In the months before the election, the U.S. Treasury also sanctioned Ukrainian lawmaker Andrii Derkach, who it described as a "Russian agent," for attempting to interfere in the election by spreading false information and narratives about then-candidate Joe Biden.[4] Derkach's efforts were previously exposed by National Counterintelligence and Security Center (NCSC) Director William Evanina.[5] These actions sparked bipartisan calls for domestic actors not to weaponize Derkach's narratives, which may have deterred or weakened attempts by U.S. lawmakers and political actors to seize on the Kremlin-backed operation to influence the election.[6]

Private sector actors also provided regular, public reports on foreign interference throughout the election cycle. Technology companies like Microsoft, Google, and Cloudflare monitored for hacking attempts targeting political campaigns and other key stakeholders, often publicly flagging attempted hacks and probing attempts and providing attribution[7] when possible. Facebook and Twitter also took steps to remove inauthentic accounts and networks from their platforms ahead of the election, with Facebook providing short explanations, along with sample content and tentative attribution to foreign actors.

From the Alliance for Securing Democracy's assessment of the 2020 U.S. election: Brandt, J. and Hanlon, B. (2021, March 30). *Defending 2020: What Worked, What Didn't, and What's Next.*[8]

[1] Frequently Asked Questions. Internet Crime Complaint Center (IC3) (n.d.). Federal Bureau of Investigation, United States of America Department of Justice. **https://www.ic3.gov/**

[2] U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election. Nakashima, E. (2020, November 3). The Washington Post. **https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html**
U.S. government concludes Iran was behind threatening emails sent to Democrats. Nakashima, E. et al. (2020, October 22). The Washington Post. **https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/**

[3] DNI John Ratcliffe's Remarks at Press Conference on Election Security. Ratcliffe, J. (October 22, 2020). Office of the Director of National Intelligence. **https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security**.

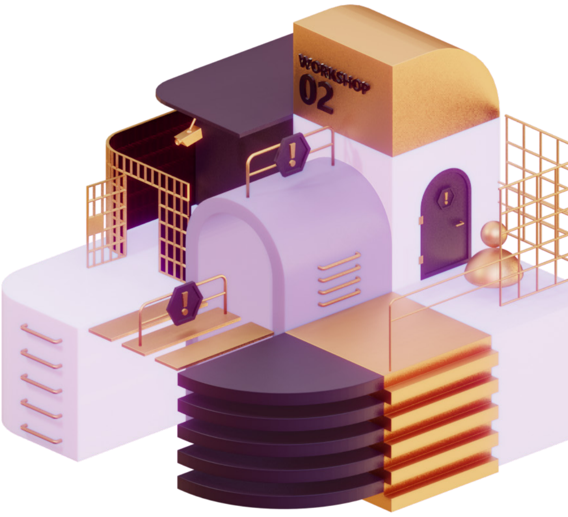
[4] Treasury Sanctions Russia- Linked Election Interference Actors. U.S. Department of the Treasury. (2020, September 10) United States Government **https://home.treasury.gov/news/press-releases/sm1118**;

[5] US intelligence says Russia seeking to "denigrate" Biden. Beavers, O. (2020, August 7). The Hill. **https://thehill.com/policy/national-security/511078-top-intelligence-official-warns-of-foreign-influence-ahead-of-2020**

[6] Rubio, Warner Release Joint Statement in Response to NCSC Director Evanina. Intelligence Committee (2020, August 10). US Senate Select Committee on Intelligence **https://www.intelligence.senate.gov/press/rubio-warner-release-joint-statement-response-ncsc-director-evanina**

[7] In October 2019, Microsoft identified Iran-linked hackers that targeted U.S. Presidential campaign **https://www.npr.org/2019/10/04/767274042/microsoft-says-iranians-tried-to-hack-u-s-presidential-campaign?t=1614948982572**

[8] Brandt, J. and Hanlon, B. (2021). Defending 2020: What Worked, What Didn't, and What's Next. Alliance for Securing Democracy. **https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf**



Workshop 2: What Constitutes Foreign Interference vs. Acceptable Nation State Influence

In order to tackle the problem of preventing malign interference by foreign actors in electoral and democratic processes, it is first necessary to establish what constitutes interference and how that differs from acceptable nation state influence. The second workshop of the Paris Call Community focused on drawing distinctions between the two concepts and making recommendations on how to define foreign interference.

The problem

Increasingly, democracies across the globe are working to prevent interference from malign foreign actors and are seeking to develop resilience against a wide array of threats, including cyber-attacks and disinformation campaigns. Amid this burgeoning activity, however, one thing is missing. There is little consensus on what exactly "foreign interference" is, and how the term "interference" is similar or different from other related concepts, such as "influence." The lack of a common framing of "foreign interference" can delay or complicate policymakers' initiatives and muddy civil society's efforts to build awareness and rally opposition against incursions into democratic processes.

Clearer definitions can draw the lines of permissibility, protect core democratic values, and give governments— and other pillars of democratic society like private industry and civil society — clearer guidelines for permissible and impermissible behavior in new domains, including in the digital realm.

Existing Definitions and Different Approaches

The starting point for a political definition is with the term "interference" itself. According to the Cambridge Dictionary, "to interfere" is "to involve yourself in a situation when your involvement is not wanted or is not helpful."[8] The term "interference" is negative, unlike the more neutral term "influence," and practitioners in the field should be careful to note that distinction. Interference should not be used to describe benevolent or benign nation-state activity beyond its borders.

The U.S. and Australian governments have definitions of "foreign interference" that focus on the malign intentions of foreign actors and seek to identify the lines between acceptable and unacceptable behavior. These definitions explicitly or implicitly feature concerns over effects on democratic processes.

The U.S. Department of Homeland Security (DHS) defines "foreign interference" as "malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."[9]

[8] Interfere. Cambridge Dictionary. (n.d.) Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/interfere

[9] Foreign Interference. Cybersecurity and Infrastructure Security Agency. (n.d). U.S. Department of Homeland Security. https://www.cisa.gov/publication/foreign-interference

Additionally, DHS suggests a foreign interference taxonomy: information activities, trade/strategic investment, coercion/corruption, migration exploitation, and international organization manipulation.

In Australia, Prime Minister Malcolm Turnbull drew boundaries around what constitutes interference: "We will not tolerate foreign influence activities that are in any way, covert, coercive or corrupt."[10] Furthermore, Australia's Department of Home Affairs provides guidance on how to distinguish legitimate nation-state influence from unacceptable interference: acts that are "coercive, covert, deceptive, clandestine"; as well as those that are "contrary to Australia's sovereignty, values and national interests." [11]

Academia offers a few examples of definitions. Charles Parton, Senior Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI), suggests that criteria for interference should include "some concept about the potential for interference" and "a lens of reciprocity" (that would examine whether "similar activities by UK actors [would] be allowed by the CCP in China"). [12]

More sophisticated criteria have been suggested for distinguishing between "influence" or "unacceptable influence" but not "interference." Duncan Hollis, Professor of Law at Temple Law School, argues that "unacceptable influence operations" can be distinguished from acceptable ones through five criteria: transparency, extent of deception, purpose, scale, and effects.[13] James Pamment, Senior Lecturer at Lund University, and colleagues suggest four criteria for "diagnosing illegitimate influence" (the "DIDI diagnosis"): deception, intention, disruption, and interference.[14]

In the private sector, Twitter offers guidelines on civic integrity: "You may not use Twitter's services for the purpose of manipulating or interfering in elections or other civic processes. This includes posting or sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process. In addition, we may label and reduce the visibility of Tweets containing false or misleading information about civic processes in order to provide additional context." [15] This policy pertains to political elections, censuses, major referenda and ballot initiatives, among others. Facebook has a different approach and defines "Foreign or Government interference" as "Coordinated Inauthentic Behavior conducted on behalf of a foreign or government actor." [16]

Interference versus other terms

The concept of interference is related to, but should be distinguished from, related terminology including foreign influence, sharp and soft power, hybrid threats, public diplomacy, coordinated inauthentic behavior, active measures, mis- and disinformation and illegitimate influence.

[10] Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017. Turnbull, M. (2019, December 7) Malcom Turnbull Website. https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an

[11] National Security: Countering Foreign Interference. Department of Home Affairs. (n.d). Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

[12] China- UK Relations: Where to Draw the Border Between Influence and Interference? Parton, C. (2019, February) Royal United Services Institute for Defence and Security Studies. https://rusi.org/sites/default/files/20190220_chinese_interference_parton_web.pdf; Pg 3.

[13] The Influence of War; The War for Influence. Hollis, D. (2018, April 3). B., Temple International & Comparative Law Journal, Vol. 32, No. 1, 2018, Temple University Legal Studies Research Paper No. 2018-19. https://ssrn.com/abstract=3155273; Pg 5.

[14] Countering Information Influence Activities: The State of the Art. Pamment, J., et al. (2018, July 1) Swedish Civil Contingencies Agency and Lund University. https://www.msb.se/RibData/Filer/pdf/28697.pdf; Pg 15

[15] Civic Integrity Policy. Twitter. (2021, January) Twitter, Inc. https://help.twitter.com/en/rules-and-policies/election-integrity-policy

[16] Community Standards: 20. Inauthentic Behavior. Facebook. (2021) Facebook, Inc. https://www.facebook.com/communitystandards/inauthentic_behavior

Effective Criteria and Guidelines

The workshop discussed key challenges in setting definitions for foreign interference and sought to agree on main principles that should be included in definitions of interference. The stakeholders supported two core criteria:

- **The notion of coercion**
- **The concept of deception, or lack of transparency and inauthenticity**

Why Coercion?

Coercion is broadly defined as "the use of force to persuade someone to do something that they are unwilling to do." [17] In the context of foreign interference, it is important to determine whether there is a power divide between nation states or actors that allows one to force the other into taking particular actions and to take such a condition into account in determining coercion.

Why Deception?

A common feature of interference activities is their covert or opaque nature. Foreign governments seek to use deception or non-transparent means to hide their efforts and destabilize a country's democracy. Various terms can be used to describe a lack of transparency, such as deception, covert behavior, and inauthenticity. These terms are often interchangeable. Notably, some experts find the criterion of deception especially important because it can indicate malign intent.

Challenging Criteria

More controversial criteria were "intent" and "impact". Intent is a significant but challenging criterion. It is important for policymakers to ask what a foreign actor is seeking to achieve, and whether it may be to disrupt, manipulate, damage or erode confidence in democratic institutions and processes. But intent is often very difficult to determine and to measure and therefore hard to include in definitions. Often a determination of intent can happen only after damage has been done. However, elements of the question of intent appear in multiple definitions, and intent is a crucial factor in penalties across justice systems.

Similarly, it is challenging to determine the impact of any particular action. In the information space, any individual piece of disinformation has a small impact, yet the combined effects can be significant.

[17] Coercion. Cambridge Dictionary. (n.d.) Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/coercion

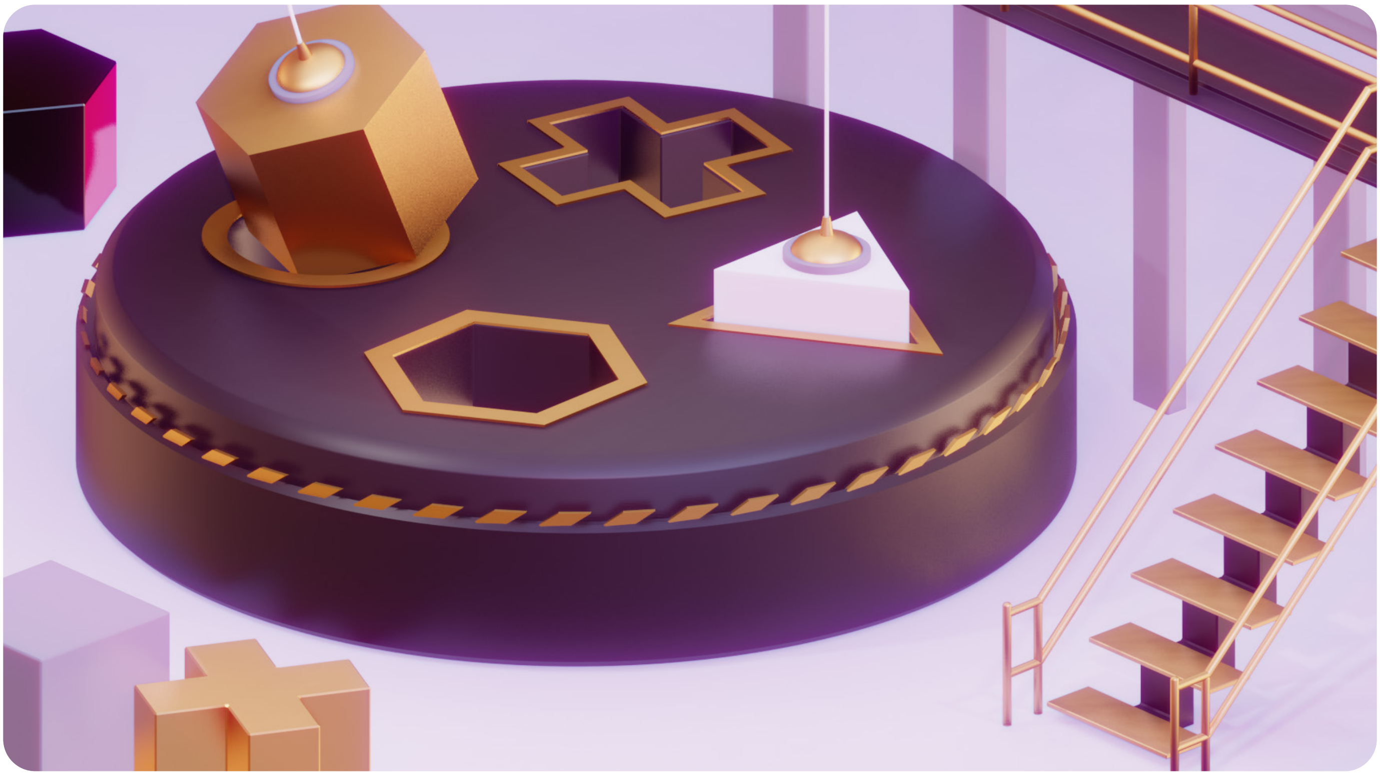
Additional Guidelines on Creating Definitions

Policymakers, civil society, and the private sector should carefully consider the scope of the definitions they suggest.

There is risk in creating overly narrow or broad definitions. If a definition is too broad, it could limit acceptable diplomatic behavior around elections and inhibit legitimate government practice. On the other hand, overly narrow definitions could exclude foreign interference acts that can take a wide array of forms and come through various threat vectors.

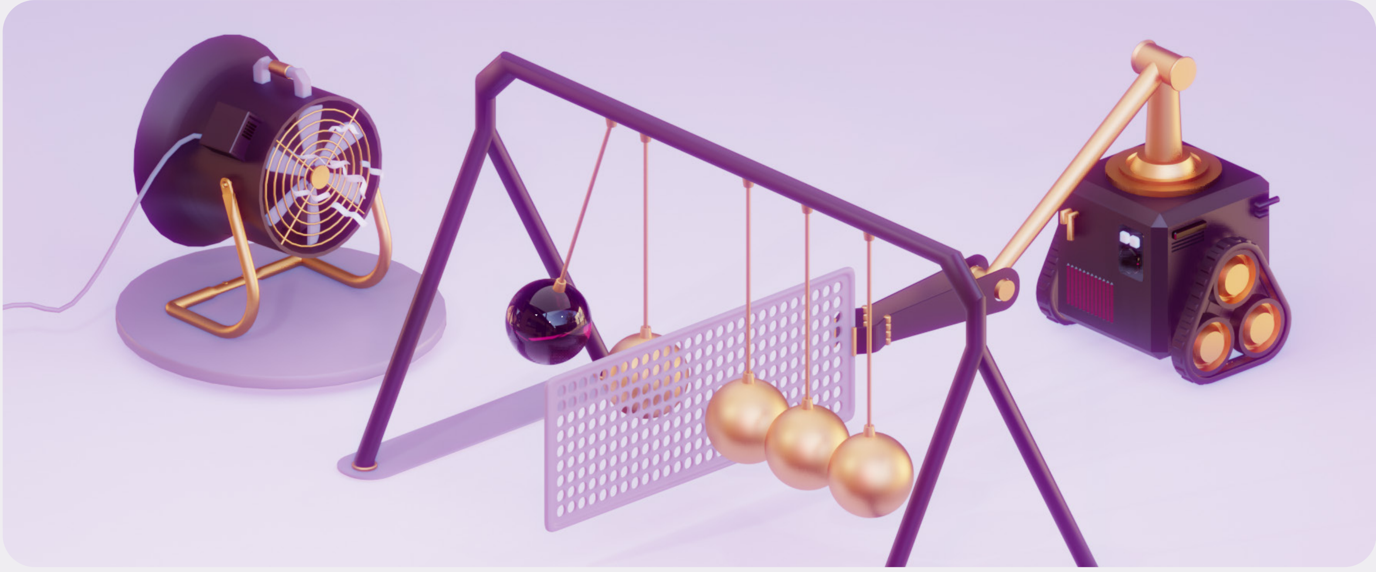
Furthermore, those setting definitions should determine whether their definition applies narrowly to governments (if so, which ones, e.g. only democracies) or to all stakeholders? If a wider definition is suggested, can it be easily applied by government, civil society, and the private sector?

There is no 'one size fits all' definition of foreign interference. Behavior and actions differ in 'acceptability' or 'unacceptability' when viewed through legal, ethical, or political lenses. Consider the political dimension where 'what is interference' depends on the country. An adversary's activities may be considered interference, whereas the same behavior from an ally is acceptable. A political definition can take the actor into account, and adjust when the policies of an adversary shift. Political definitions can apply to a broader range of threats than can definitions framed in terms of international law. Political definitions also may be more practical in a fast-changing environment.



Workshop 2

The Challenge of Defining Foreign Interference versus Foreign Influence



The challenge of distinguishing between acceptable foreign influence and malign foreign interference is bedeviling democracies. Societies which are open by design, are particularly vulnerable to clandestine, deceptive and coercive efforts by foreign actors to undermine national interests, including democratic institutions, processes and values. There is a clear grey zone between influence and interference that hostile actors are exploiting in pursuit of their geopolitical objectives.

In approaching this definitional challenge, it is important to begin with the objective. Is it to devise a universal definition for acceptable foreign influence versus unacceptable foreign interference? Or, more to the point, is it to determine what constitutes unacceptable foreign interference by authoritarian states vis-à-vis liberal democracies?

If the objective is a universal definition, then international law has to be the starting point. In international law, the prohibition on intervention in the internal affairs of another state is foundational, as reflected in the UN Charter and in numerous international agreements. It has wide scope, covering interventions by force (e.g., military operations or occupation, territorial annexation) as well as non-forcible interventions. It is clear that this fundamental rule remains applicable today in the face of new forms of foreign intrusion. What is less clear is precisely how the rule applies in given scenarios, which is the subject of considerable attention amongst legal experts in academia and government.

If the objective is unacceptable authoritarian state interference, then it is the task of democracies to determine which actions by authoritarian states – especially those that may be strategic rivals – are acceptable in domestic affairs and which are not, as a matter of both law and policy.

There are three elements commonly considered when defining foreign interference and delineating it from foreign influence: intent, transparency and impact. But here, again, there are challenges.

Determining intent is difficult, particularly the specific intent behind a particular action. For example, what can be known about a state's intent in interfering in an election? Is it attempting to sway the election in a candidate's favour, erode public confidence in democracy, or precipitate a shift in the world order? Intent is also difficult to ascertain when proxies or unwitting actors are employed, as is often the case, or when these activities take place in a crowded, transnational digital ecosystem that defies attribution.

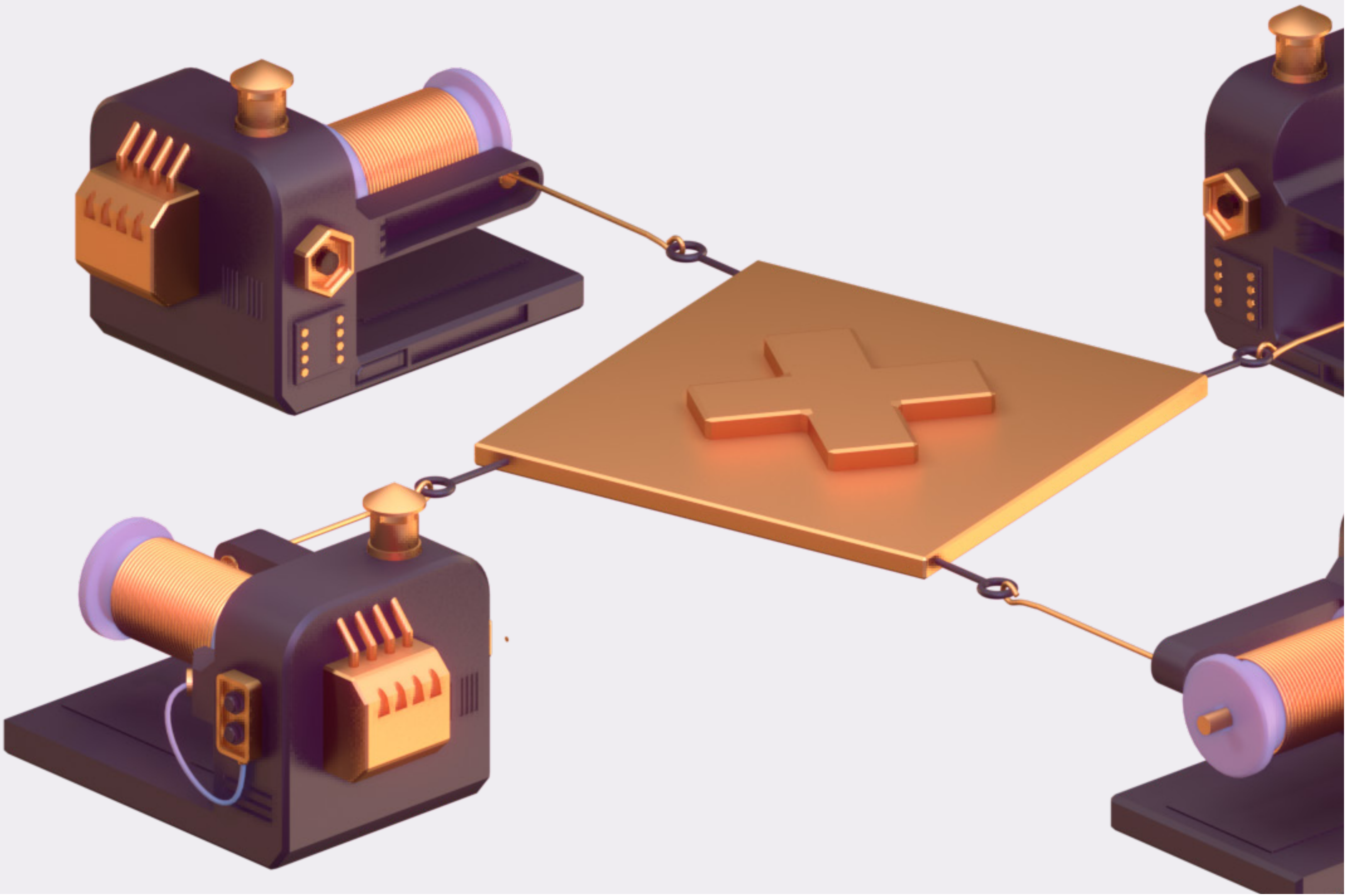
Transparency is also challenging. Covert foreign disinformation campaigns have been rife on social media platforms. But there are plenty of examples of state actors using overt means (e.g., state run media, official social media accounts) and messaging to sow confusion, seed division and erode confidence in democratic governments, including in the context of the COVID-19 pandemic.

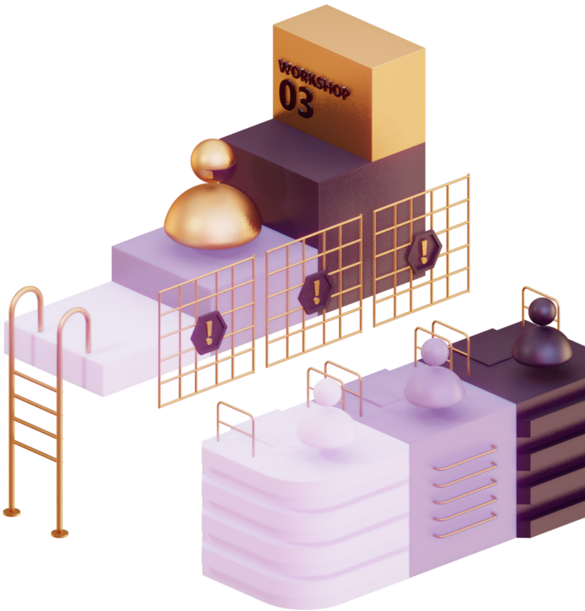
Evaluating the impact of foreign interference also remains elusive. Oftentimes, malign state actors employ a range of tactics, spanning multiple vectors of interference (e.g., cyber, digital, human), in order to achieve an objective or set of objectives. In this "death by a thousand cuts" scenario, it is of limited utility to attempt to evaluate the impact of a particular act of foreign interference, when it is precisely the confluence of a plurality of acts that is intended to affect a geopolitical outcome.

Moreover, evaluating impact is almost impossible with some forms of foreign interference. For example, how can one evaluate the impact of a disinformation campaign on an election outcome in view of the complexity of the information ecoystem and voter intentions? In recent elections, after extensive analysis, it is impossible to determine with confidence that foreign intervention swayed the result nor that it was chiefly responsible for greater polarisation.

The space between foreign influence and interference is clearly one that deserves greater thought and discussion among democratic partners with a view to clarification of how international law applies, the articulation of red lines and coordinated responses.

Gallit Dobner
Director, Centre for International Digital Policy, Global Affairs Canada





Workshop 3: COVID-19 Contingencies – Countering Election Interference in a Pandemic Environment

When the Paris Call Community set its intention to defend electoral processes, it focused on preventing malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities. Less than a year later, a most unexpected event – a global pandemic – disrupted life and impacted the execution of democratic processes, including elections. Those who seek to interfere in elections look for election infrastructure vulnerabilities and chasms – the places within democratic societal constructs where there is confusion, disagreement, or fear – to exploit. Across the globe, mis- and disinformation about COVID-19 cropped up and traveled across various information platforms. Election officials moved rapidly to adapt their processes for voting in a pandemic; there was significant concern that such changes, in combination with inaccurate information about COVID-19 could confuse voters. These vulnerabilities created an unprecedented opportunity for election interference. Adversaries could attempt to accomplish their goals through a variety of means, including information operations, cyberattacks, or social media campaigns. In the United States, physical safety concerns, and persistent cybersecurity and disinformation challenges impacted planning for the U.S. 2020 elections and posed significant challenges for other countries as well. The third workshop looked at how democracies determine how best to administer elections in an uncertain environment. It is important that those who help conduct them engage in contingency planning. Stakeholders must carefully consider where changes in voting procedures are necessary, as well as how such changes can create opportunities for election interference and determine how any interference can be mitigated.

As democracies shift rapidly to accommodate voting in a pandemic environment, there are guiding principles to keep in mind. Election officials need to consider how to lower the risk of COVID-19 spread, ensure that voting is accessible, and effectively implement changes to operations, procedures and facilities for voting. Voters should not have to choose between their health and casting a ballot, and need information on how to vote safely. In this environment, any option has risks – whether perception based, information based, technically based, or a combination – that provide opportunities for interference.

In terms of options, it is worth considering first which options exist and then explore their associated risks, and what thinking is there around protecting these processes, promoting security, and safeguarding election integrity.

Some such options include:

- In-person voting
- Portable Voting Systems (voting stations, either set up curbside at the normal polling place, or contained in a vehicle that can relocate to alternative voting locations)
- Mail-in voting and drop-box voting
- Electronic voting (web, email, fax)

Points to consider around each option:

- Where are the points of weakness in each approach? How do they make themselves vulnerable to interference?
- What are the points of strength in each approach? How do they help guard against interference, and how to best communicate the virtues of these strengths to the voting public to guard against the negative effects of interference?
- What solutions or tools are not being implemented but should be?

Effective Practices:

Build Trust

It is important to build trust in our EMBs over the long haul. People should trust in these bodies' independence and non-partisan nature. This can be achieved, in part, by (where appropriate) reminding voters that election officials are members of their community. Trust-building should not occur only around big elections, but over a sustained period.

Provide Credible Information

It is critical to ensure that people have reliable information – to "inoculate" the public – to counter potential misinformation and disinformation. A key challenge is reducing uncertainty (e.g., around how, where, and when to vote) which COVID has created and reduces participation. It is important to engage trusted local partners; empower them with training, tools, and resources; and promote their work to increase impact – particularly in relation to vulnerable communities, the number of which has increased significantly due to COVID.

It is important to develop ways of measuring the impact of efforts to combat disinformation. More research is needed to devise robust impact measurement techniques. Some useful ways of measurement currently include determining how many people are reached and how often they are reached by efforts to provide them reliable information; surveys to gauge public opinion and its evolution; surveying the community organizations with whom one engages; and assessing if people who would not earlier vote are voting.

Protect Election Integrity

The technology that supports and facilitates voting – from the poll books that list each voters' information to the machines voters use (in some jurisdictions) to cast a vote, to those that tally results on election night – have important benefits. These products and solutions can help protect the quality of the process, which can be especially vulnerable in crises that could decrease voter turnout. Governments around the world should invest for the long-term in bolstering their technical capacity, so that they can keep current with technology being used and the expertise required to maintain it, being proactive, and responding quickly. Security must remain a top priority; countries should build security into any infrastructure they create or change. Countries should invest in more research and development so that systems can be as refined and robust as possible.

Provide Reliable Technology

Where used, election technology, though helpful, should not be implemented hastily, haphazardly, or superficially (as a "band-aid" solution). Its use should also be accompanied by clear rules. However, these rules should not be overly prescriptive. Additionally, election technology should not be implemented in a way that reduces participation through issues of inequality and access; governments should not create different tiers of citizens when implementing election technologies. Access and security should be considered as equally important. Moreover, it is crucial – especially in the context of emerging democracies – to ensure that technological failure is not perceived as corruption and does not bring into question the legitimacy of elections.

Process and Power of the Vote

It is important to realize that how people vote influences who votes, which influences who governs.

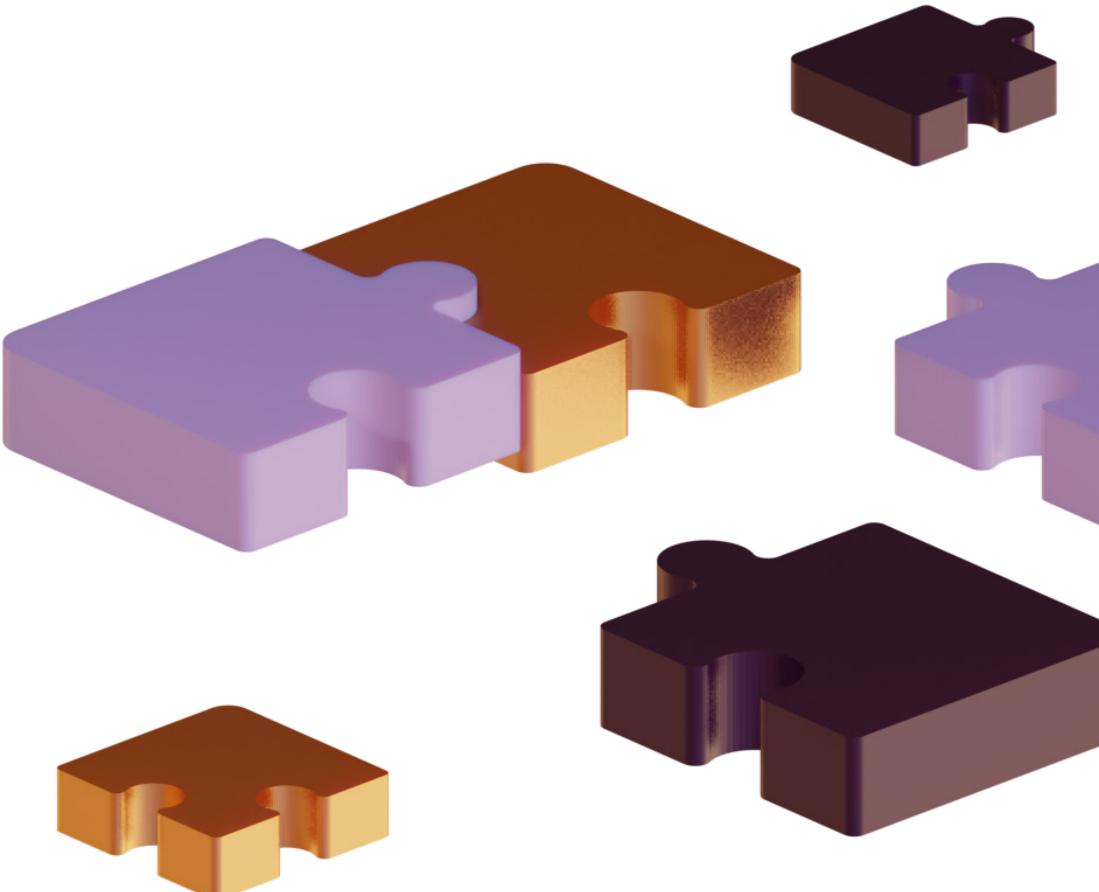
So governments around the world should likely (and will likely) seek hybrid approaches, that could include in-person voting, voting by mail, and portable voting, to ensure high participation.

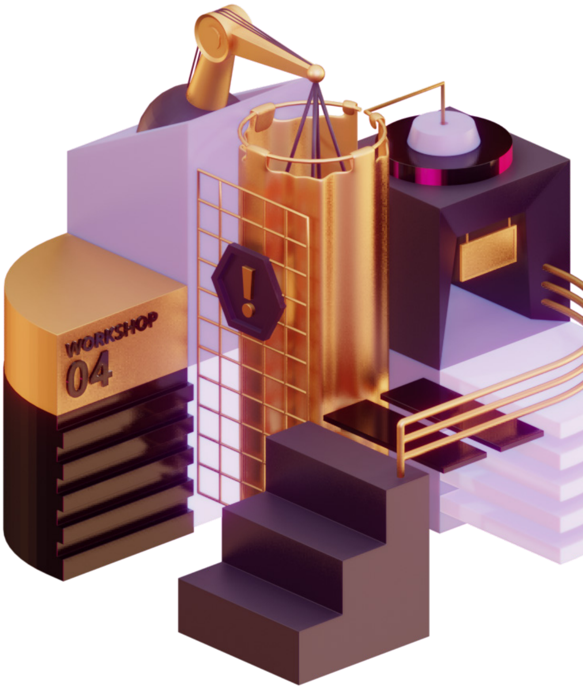
Customize the Solution

Each approach has its benefits and risks. When considering how to approach elections in a particular country, including (but not limited to) in relation to election technology, it is important to realize that what works in one country (e.g., a smaller country like Estonia) may not work in another (e.g., larger countries like the U.S. and Canada). Approaches may need to differ not just across countries but also across smaller regions such as different counties in the U.S. When preparing for contingencies, it is important to have a comprehensive communication plan and implement it quickly, even if it is not perfect.

It is also vital to have a "plan B" ready to go. For example, to prepare for the possibility that an electronic reporting website stops working, it would be important to have an alternate website.

It is critical to realize that election officials have many competing priorities, because of the pandemic, so there is a risk that cybersecurity issues (which were issues even before the pandemic) get deprioritized. Election officials should be reminded of the importance of addressing these issues despite the other issues they are tackling. Fundamentally, it is important to collaborate closely across, and learn lessons from, governments (within a country and internationally), civil society, and industry.





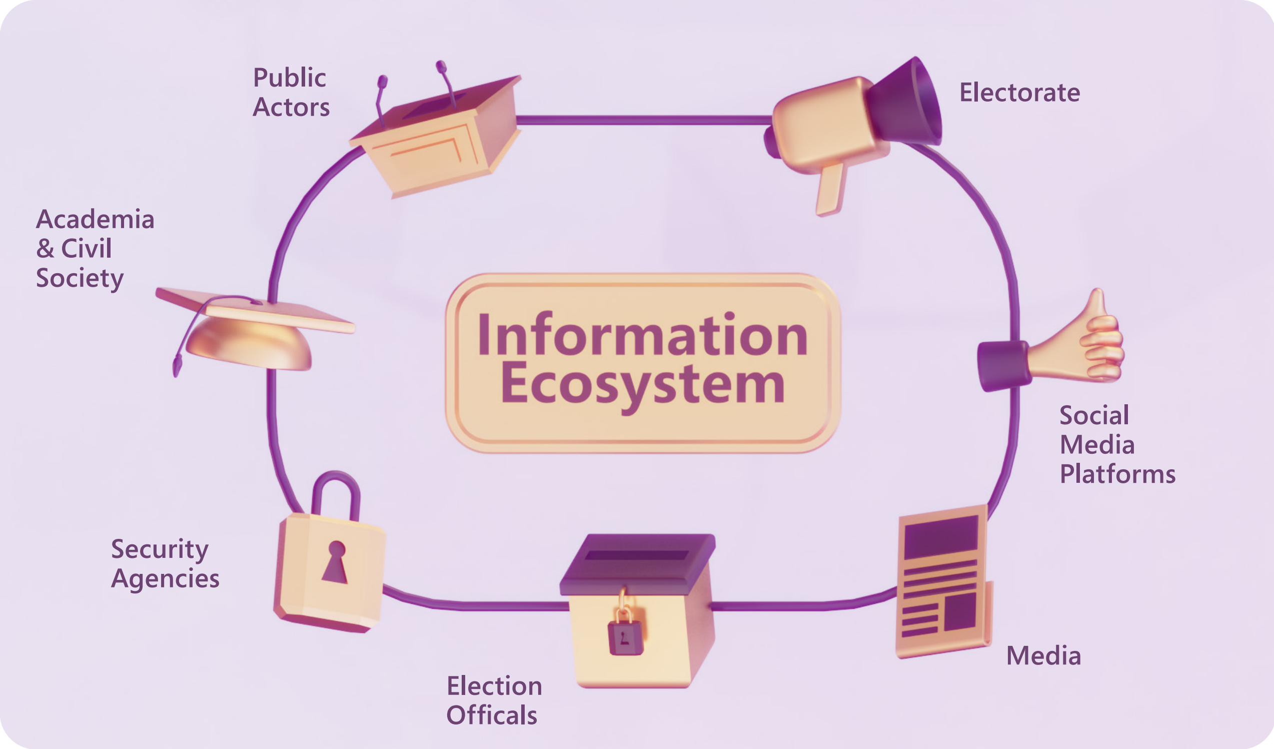
Workshop 4: Countering Election Interference in the Information Environment: Mitigation & Response

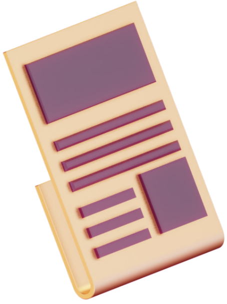
The internet has provided people with a gateway to a seemingly endless stream of information. At the same time, the internet has also brought a host of new opportunities for malicious actors, both foreign and domestic, to undermine faith in democratic institutions. Many of these actors have directed disinformation campaigns against democracies in an attempt to interfere with elections by sowing doubt in electoral processes, aggravating societal polarization, and applying a host of other nefarious tactics. Adding complexity to the task of countering disinformation is the challenge that the distinction between foreign and domestic sources is not always clear.

Protecting democratic institutions, including free and fair elections, from malicious interference is a shared responsibility. Governments, traditional media, social media platforms, academia and civil society are all part of an information ecosystem. All members of this ecosystem play a critical role in countering electoral interference.

The fourth workshop heard from key actors in the information ecosystem – notably experienced journalists – and examined the challenges of determining when and how to respond to attempts at election interference presents. Particularly when it comes to disinformation, there is a risk that responding to an incident can make the situation worse.

Ultimately, however, citizen resilience is the best safeguard against these hostile actions. Citizens must be empowered with reliable information in order to draw their own conclusions, hold governments and individuals to account, and participate in meaningful and civil public debate.





Media and Journalists

According to Reuters Institute Digital News Report 2019, people's trust in the news has been decreasing over a number of years, coinciding with a rise in populism and political polarization. [18] Given this trend, journalists are increasingly examining ways that they can work to increase and maintain trust. This can be particularly challenging in light of the hyper-politicization of many significant global issues such as climate change, Covid-19, and vaccinations.

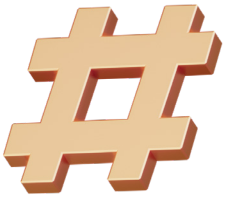
Maintaining impartiality by considering personal biases and blind spots in how information is portrayed, manipulated or omitted helps build and maintain an audience's trust. However, being impartial does not mean all issues have two sides. For example, giving excessive space to a small number of scientists who believe vaccinations are harmful can create the belief that there is serious disagreement over the issue, when in fact, vaccinations have overwhelming scientific support. The audience should be empowered and provided with the facts to reach their own conclusions.

Journalists can do their part to ensure that they do not contribute to foreign interference by asking critical questions of themselves and by providing the appropriate context. For example, asking who is leaking the information, why and how they were able to access it. They should critically assess what the leaker's broader agenda may be. These questions can help determine if the information is legitimate or if it is being used to manipulate the media.

Additionally, responding quickly to provide timely and accurate information is key as disinformation thrives in a vacuum. Without such efforts, citizens may resort to less reliable sources of information, thereby increasing their vulnerability to disinformation and misinformation.

Social Media Platforms

Social media platforms experience their own challenges when faced with malicious actors using their platform to interfere in elections. Both foreign disinformation campaigns and domestically-driven disinformation present challenges when it comes to social media companies responding. It may be difficult to distinguish between the two, and arguably there can be freedom of expression concerns in some countries when it comes to removing domestic accounts and content.



Relying on policies that look at the behaviour of platform members rather than the content that they post can possibly mitigate free speech concerns. For example, this approach focusses on behaviour-based violations such as impersonation, use of bots or multiple accounts to amplify messaging and can be enforced by shutting down

[18] 'Yellow Vest' Protesters Knock Wind out of French Business, Economy. Landauro, I, and Myriam R. (2018, December 3) Thomson Reuters. www.reuters.com/article/us-france-protests-economy-idUSKBN1O21IA. For example, trust levels in France have fallen to 24% after the media saw criticism over its coverage of the Yellow Jacket demonstrations.

Workshop 4

Collaborative Partnerships

The need to fight disinformation has prompted traditionally competitive media organisations to partner in new ways. One of the most prominent examples of this form of radical sharing is an initiative called Cross-Check.

In 2017, 37 newsrooms in France and the UK came together to fact-check the French presidential election campaign. Cross-check was initiated by First Draft, a non-profit group with funding from philanthropic organizations, digital platforms and other independent sources. Cross-check has now grown into an international coalition that fights disinformation beyond election campaigns, including scientific disinformation relating to Covid-19. It also provides training for journalists on collaborative fact-checking techniques.

Increasing disinformation has prompted many media organisations to create their own fact-checking teams and programs. In Canada, Radio-Canada, the French-language public broadcaster, as well as Agence France Presse, partner with Facebook to debunk false information, both during and between election campaigns. Established media also share fact-checking during special political events, such as leaders' debates. Many of them belong to larger associations such as the International Fact-Checking Network, which is run by the Poynter Institute, a recognized leader in journalistic ethics and development. The need to collaborate in larger investigative international projects has led journalists to create new network organisations such as the International Consortium of Investigative Journalists, which revealed, among other stories, the Panama Papers tax scheme.

New forms of collaborative electoral fact-checking are also emerging at the local and regional levels. In one such initiative, more than a hundred media outlets belonging to the Colorado News Collaborative (COLab) pooled fact-checking and reporting resources during the 2020 US presidential election. COLab has taken media collaboration to a new level. Its affiliated newsrooms specialise in civic local news stories that are solutions based, often inspired by citizens, and that create new forms of engagement between reporters and their communities.

The fight against disinformation also goes beyond fact-checking, which remains a defensive measure. It is recognized now that building trust and increasing the visibility and promotion of recognized credible journalistic content is crucial to stem the flow of false news.

One such proactive project is the Journalism Trust Initiative (JTI), a joint effort by Reporters Without Borders, the European Broadcasting Union, Agence-France-Presse and the Global Editors Network. It consists of creating a certification system for journalists and media organisations. They qualify through a questionnaire about their editorial practices, journalistic standards and corporate structure and funding. The certification process is run by standards organisations like AFNOR in France but determination on whether a news organisation qualifies for the standard rests with panels of media professionals.

JTI, which is now in its pilot phase in a number of countries, including Canada, can also be used as a tool by citizens and by non media organisations. Ultimately, JTI could be used by platforms to promote content that is JTI certified; discussions are ongoing with international advertisers associations to favor JTI certified media for ad placements in secure digital spaces; JTI can also be used as a benchmark by private philanthropic entities and government departments that distribute financial aid to media organisations.

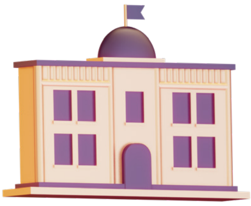
Michel Cormier
Journalism Trust Initiative

accounts and removing content with less risk of appearing partisan or facing accusations of violating freedom of expression or speech.

Many social media platforms publish reports and statistics on violations of their policies. Immediately informing the public of coordinated interference campaigns during an election is one way that social media companies can more effectively contribute to a healthier information ecosystem. Being more aware of the magnitude of manipulation may help platform users to be more critical about what they come across and think twice before passing along information that may not be credible.

Collaboration and information sharing between social media platforms and stakeholders is key. These efforts should include governments, academia, investigative journalists, and fellow industry peers. Problems should be "open-source" – identified and made apparent – and shared with experts to help devise solutions. The expertise of NGOs, think tanks, and other civil society organization can provide context and further understanding.

Government



Defending democracy and democratic institutions is a core government responsibility. However, there are risks for the government in power to calling out interference during an election. In addition to accusations of partisanship, there is the possibility that any announcement of interference could influence the results of the election. It may also erode confidence in the election and affect the perception of legitimacy of the results.

Given the potential impact of an intervention, it is critical that governments consider a very high threshold for intervening during elections both to ensure public confidence and legitimacy.

Intervention should not be based on inflexible rules, but rather be subject to nuanced judgement.

Experienced, non-partisan decision-makers should ensure that actions consider the values and priorities of, and impacts on, the country and its citizens. Thought also should be given to the purpose of the communication, the type of information threat, who it was directed towards, as well as when and where the occurrence took place. As reflected in Canada's experience with the Critical Election Incident Public Protocol, it is critical to have the right decision-makers, a clear mandate, and access to real-time unclassified and classified information.

A comprehensive approach should be taken, in which government, industry and civil society work collaboratively as appropriate to combat foreign interference. This helps to ensure the right voices are responding from government, industry, the media, academia, and think tanks. However, situations will vary from country to country as each could face unique challenges with electoral interference. Their legal, political, and electoral processes vary greatly and there is not a one-size fits all approach.

Workshop 4

Canada's Critical Election Incident Public Protocol

The Protocol

The Critical Election Incident Public Protocol was the mechanism for communicating with Canadians during the 2019 General Election in a clear, transparent, and impartial manner if there had been an incident that threatened the election's integrity (e.g., hacking of a government website, wide-scale disinformation).

The Protocol is grounded in the view that any announcement during an election campaign that could have an impact on that election should best come from a trusted, non-partisan source, in this case senior public servants.

The Panel

The Panel is comprised of senior public servants who have extensive experience in national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the Canadian Charter of Rights and Freedoms. The Panel met regularly during the writ period and was kept apprised of the threat environment on an ongoing basis.

The Threshold

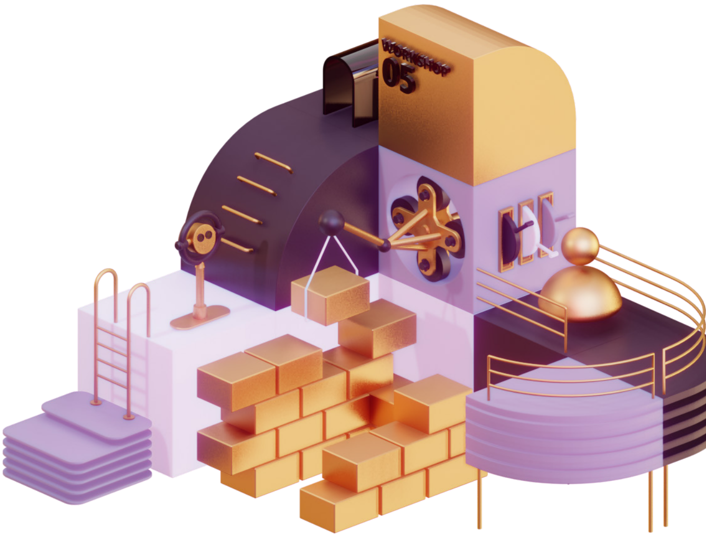
The Protocol is not used as a means to referee the election, and the threshold for making an announcement is very high and limited to exceptional circumstances. These considerations are assessed against various parameters, including the scope and impact of the incident(s). In respect of the type of incidents at issue, the Protocol stipulates: the focus should be on interference that threatens the integrity of a general election.

The Announcement

The Panel must reach consensus on any decision to make an announcement. Barring any national security concerns, Canadians are informed of what is known about the incident and any steps they should take to protect themselves.

Democratic Institutions Secretariat,
Privy Council Office, Government of Canada

Workshop 5: Defend, Detect, and Recover: Countering Threats of Interference in an Election Environment



Protecting election infrastructure is an essential part of countering foreign interference in democratic processes. Election infrastructure protection goes beyond what happens on election day. Critical steps need to be taken before, during, and after election day to ensure that elections systems are protected. The fifth workshop in the Paris Call Community series focused on outlining the full array of infrastructure involved in elections, assessing vulnerabilities they face, and proposing solutions to reduce those vulnerabilities.

Election Infrastructure and Key Vulnerabilities

Countries around the world conduct elections differently. Some have paper-based systems while others use voting machines and other digital tools to register voters, vote, and tabulate results. But all elections now involve digital technologies and communications, whether for vote transmission or for reporting results to news organizations and citizens. Improving election infrastructure security requires first understanding the range of infrastructure involved in electoral processes and then carefully assessing the risks they face.

Before election day, many pieces of infrastructure are already in use, each of which can be vulnerable, these include:

- **Online voter registration systems,** which may be susceptible to website spoofing as attackers can create a malicious copy of the official website to capture sensitive info or give voters the perception that their info was altered. Targeted denial of service or outage attacks could prevent voter registration.
- **Internal communication systems or election official social media accounts,** which could be compromised as attackers may use legitimate accounts from these systems to send out false information, such as incorrect voting locations and election dates, to election officials, poll workers, voters, and others.
- **Storage locations,** which could be vulnerable to physical tampering or destruction of voting equipment by bad actors.

Election day receives the most attention and resources for protecting election infrastructure security. In countries such as the United States, electronic and digital infrastructure play a significant role in the voting process. In others, including Estonia and Switzerland, voting has even happened online.

In more traditional voting scenarios, the following pieces of infrastructure are of critical concern:

- **Electronic poll books (electronic lists of voter rolls)** could be susceptible to compromise by malicious attackers who could gain access to the poll books either using a wireless connection or because the physical device is not properly secured. A compromise to a poll book could allow voters to manipulate voter rolls either deleting or modifying actual voter registration data. This could result in confusion when voters show up to vote on Election Day.

- **Voter registration systems** could see access blocked. Data and backups could be encrypted or erased through ransomware by attackers until a ransom is paid. This could also result in theft or irreversible encryption of voter registration databases and other sensitive records, causing disruption to election activities and a potential decline in public trust.

- **Vote cast devices,** depending on the device, could be vulnerable to physical tampering using removable media or remotely using a wireless connection. A compromised vote casting device could allow a malicious actor to modify a vote during an election.

- **Election night reporting** also depends on the flow of information about the vote results, is a critical element of the election process, and contains technological elements. Inaccurate reporting of election results could lead to or escalate already existing tensions.

After the election, certain vulnerabilities remain. Attention needs to be paid to election managements systems, official websites, and to auditing processes.

- **Election Management Systems** could be compromised due to commercial software or hardware with security weaknesses or configuration errors in network connections. A successful breach could lead to manipulation of results during electronic transmission of vote tallies.

- **Official websites** could be susceptible to compromise as attackers could replicate official election websites and post different results than are being reported.

Effective Practice

Protecting election infrastructure requires sustained activity across the full election cycle.

Certain solutions to reduce vulnerability are applicable to the whole cycle, while others are only relevant to specific moments in the election process. The possible solutions noted below represent a collection of ideas proposed by workshop participants from the public, private, and civil society sectors.

General Good Practice

Human risk is present throughout the election cycle. It is essential for all individuals working on elections, either those executing an election or working related to one, such as media covering the election or political parties and candidates participating in one, to practice good cyber hygiene.

Personnel and equipment suppliers involved in elections can constitute points of vulnerability. EMBs and related institutions and vendors should ensure that adequate protections are put in place to vet personnel and equipment.

For example, election staff are often temporary and the process for screening staff may not adequately take security into account. More robust background checks would reduce risk. Similarly, high scrutiny should be placed on vendors – those who produce and manage voting machines, election management systems, and other equipment. A certification mechanism could be put in place to would require vendors to demonstrate they follow good cybersecurity practices.

Effective Practice on Cyber Security

Maintaining cybersecurity is an ongoing process

It is important to understand that incident response (responding to cybersecurity incidents within a technical system) is a "lifecycle" that requires high visibility into the system's existing security posture and continuously improving that posture through lessons learned. Quick detection and quick response are key.

Cybersecurity tips include the following:

- Observing metadata – such as the location of a given cyber activity – which can help identify suspicious behavior.
- Implementing the use of "containers" – mechanisms that would allow individuals to open potentially damaging attachments without suffering any damage.
- Breaches can be discovered by auditing whether individuals in an organization are downloading documents and printing them, as well as by scanning e-mailboxes to check for external forwarding.
- For individuals involved in elections processes, it is important to check who has access to mailboxes and to confirm that auditing is enabled. Malicious actors often disable auditing.

Policymakers should allow firms with expertise in cybersecurity to support election campaigns' cybersecurity needs if the firms' goal is to support electoral integrity. In the United States, this is consistent with the U.S. Federal Election Commission's guidelines. Such support is critical because campaigns often do not have the expertise or capacity to handle cybersecurity issues, thereby jeopardizing electoral integrity.

Effective Practice on Voter Registration Systems

In order to protect voter registration systems, EMB's should have robust backups in place. Officials should consider instituting encrypted backups, including remote mirrored sites, as well as paper backups.

To address the inherent vulnerabilities of personnel, individuals working on voter registration systems should only have privileges that are essential for them to complete their task. The principle of least privilege is key. Similarly, individuals' roles should be isolated within a system.

Lastly, it is important to ensure that information that can lead to wiping back-ups is extremely secure because this has been a target for attacks by hostile actors.

Effective Practice on Poll Books and Voting Machines

Election administrators should consider using electronic poll books, but at the same time, protect against the risks they create. Advantages of electronic poll books include quicker voting and real-time synchronization with other poll books and with back-end voter registration databases. This helps reliably record that a voter has checked in, cast a ballot, and not voted more than once. However, electronic poll books frequently fail, as they did in the 2020 election primary in Los Angeles County, which can delay the voting process.

Cyberattacks pose another threat to electronic poll books, and it is possible that a cyberattack could change information on a poll book. To protect against these risks, policymakers should require election administrators to stock large amounts of back-up materials such as paper poll books and envelopes that can let voters vote provisionally.

Similar back-up measures are also effective for voting machines, as stocking large quantities of paper ballots can help if the voting machines are attacked.

Effective Practice on Communications

If election infrastructure has been breached, elections officials should communicate thoughtfully with all stakeholders involved, including the voters and the public more broadly. It is important to convey what happened, how damaging it was (for example, some hacks do not actually change the data), and where the public can go for accurate information.

Effective Practice on Audits and Other Confidence-Building Measures

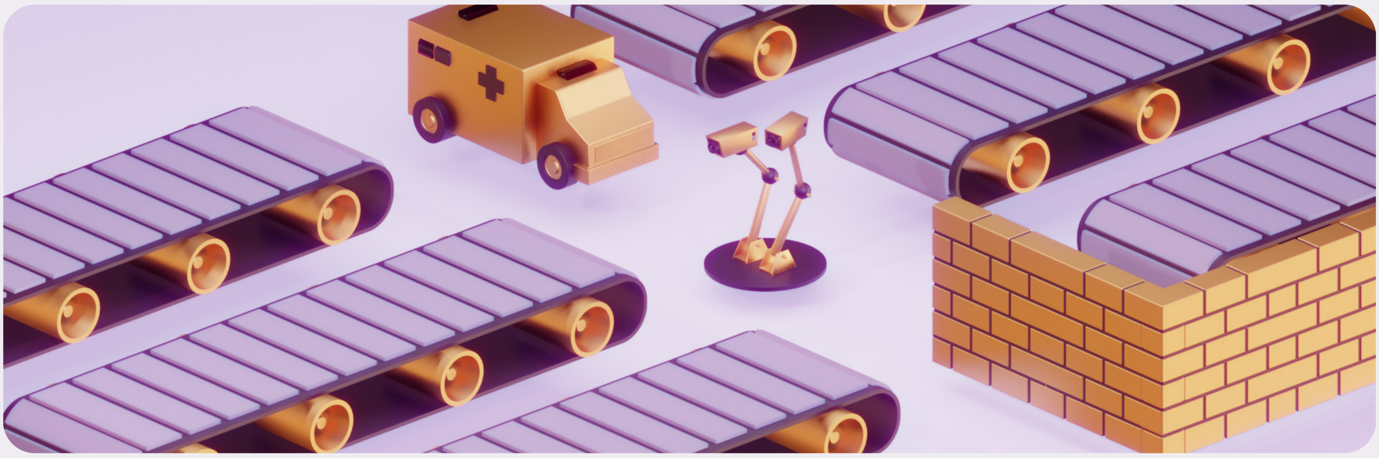
Post-election audits are important for boosting confidence in election results. Risk Limiting Audits (RLAs) offer advantages over traditional audits. RLAs are more efficient – they are dynamic, sample and audit only as much is needed to confirm the result of the election, and they confirm only the winner, not the margin by which the winner won.

Other confidence-boosting measures should be considered, including:

- Giving the public the ability to check for themselves that the tallying was done properly,
- Educating the public about all aspects of the voting process (especially given changes stemming from Covid-19),
- Improving cooperation between all stakeholders within and outside government, and within government at the federal, state, and local levels. For example, in the U.S. this process has been facilitated through designating electoral infrastructure as "critical infrastructure."

Workshop 5

Protect Election Infrastructure: Defend, Detect and Recover



- Preventing malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities largely boils down to three things: defence, detection and recovery. Unfortunately, there is no way to completely secure an election from bad actors, so the focus must be on ensuring that the election system is resilient enough to withstand attack.

- Defending an election system from foreign actors requires sufficient cyber security resources. This includes having enough personnel who can understand the foreign interference threat, identify vulnerabilities, make recommendations to mitigate the vulnerabilities, implement those recommendations, and recover from any compromises. It also includes ongoing training for how best to protect election systems from malicious cyber activities and strategies for quickly sharing threats and cyber-related incidents that occur.

- Detecting potential problems in election systems requires mapping out all potential vulnerabilities and putting in processes to detect issues that could arise from any of the vulnerabilities being exploited. For example, robust post-election-audits, like risk-limiting audits, help ensure that the voting equipment and procedures used to count votes during an election worked properly, and that the election yielded the correct outcome.

- Finally, for each vulnerability identified, it is important to practice what should happen if the vulnerability is exploited, and how best to recover. For example, if an optical scan voting machine goes down, election officials should have procedures in place to ensure that voters can continue to cast ballots if problems with the voting machine arise.

David Levine
Elections Integrity Fellow at the Alliance for Securing Democracy

Workshop 5

Threats to and Resiliency Measures for Election Day Voting in The United States

Voter registration databases and electronic poll books

Registration databases contain lists of registered voters and identifying information that determines what contests a voter is eligible to vote in. They contain the data that is used to produce poll books for Election Day voting. Poll books contain lists of voter rolls for an individual polling place and are used to check in voters as they arrive to cast their ballots. Electronic poll books are simply electronic versions of these, often on a tablet such as an iPad.

Threats

Agents of the Russian government targeted voter registration databases in the United States in 2016[19], heightening concern that access to and integrity of the databases and the electronic poll books could be compromised, whether by malicious attackers or by unintentional errors produced during data transfers and software updates. Compromise could result in the deletion of voters from the database or poll book, encryption of data through ransomware, incorrect information about whether voters have requested and/or returned absentee ballots, and incorrect information about whether voters have already voted. This could result in confusion when voters show up to vote on Election Day, with voters being incorrectly told that they are not on the list of eligible voters, have already voted, or have requested an absentee ballot.

Resiliency measures that many state and local election officials implemented prior to November 2020:

- Backing up registration databases
- Printed paper poll book backups in every polling place
- Keeping plenty of provisional voting materials on hand at each polling place

Voting Devices

Voting devices in the US include scanners that voters place their voted paper ballots into for tabulation, Direct Record Electronic (DRE) devices on which voters make their selections and that directly record and tabulate the choices, and Ballot Marking Devices (BMDs) on which voters make their selections which are then printed onto a paper ballot and ultimately cast.

[19] See, for example: Senate Report No. 116-290, Vol. 1, at 6 (2020). Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure, with Additional Views. **https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf**

Threats

Depending on the device, it could be vulnerable to physical tampering using removable media or remotely using a wireless connection. It could also be vulnerable to programming errors.   Compromise of a vote casting device could allow a malicious actor to modify a vote during an election or cause a device to become unusable, leading to long lines.

Resiliency measures that many state and local election officials implemented prior to November 2020:

- Tabulation audits, in particular risk-limiting audits
- Emergency paper ballots in every polling place

Discussion: Are US elections Resilient Against Insider Threats?

Decentralization of election administration can be a form of resiliency. The scope of the damage that someone can do through "insider work" is limited to a single jurisdiction, usually a county or municipality. However, election vendors are not as decentralized as election administrators, as there are just a few major vendors of vote casting devices and other forms of election infrastructure in the United States. Possible improvements in this area include government certification that vendors follow good cybersecurity and personnel practices, in order to protect against insider threats.

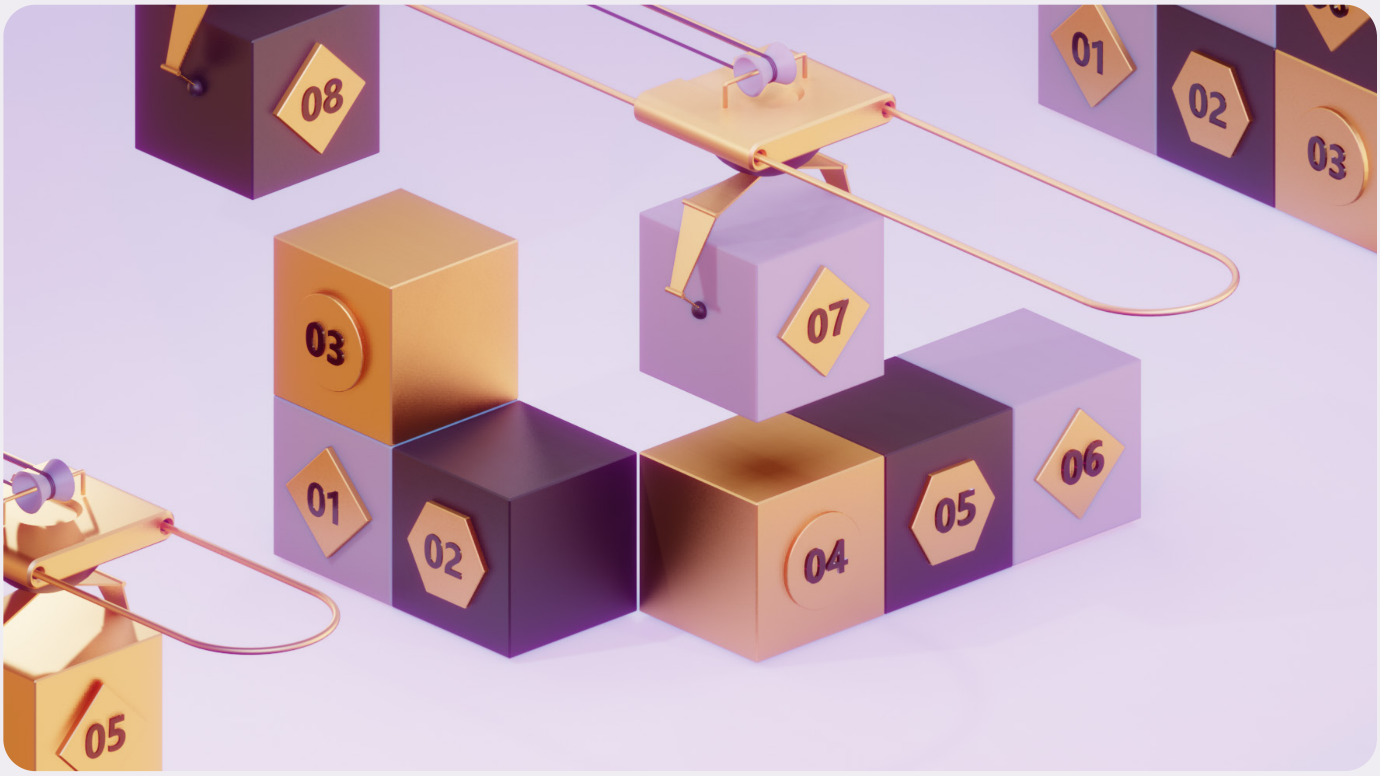
Gowri Ramachandran
Counsel, Democracy, Brennan Center for Justice

Workshop 5

10 Best Practices that Apply to All Election Jurisdictions

1. Create a proactive security culture.
2. Treat elections as an interconnected system.
3. Have a paper vote record.
4. Use audits to show transparency and maintain trust in the elections process.
5. Implement strong passwords and two-factor authentication.
6. Control and actively manage access.
7. Prioritize and isolate sensitive data and systems.
8. Monitor, log, and back up data.
9. Require vendors to make security a priority.
10. Build public trust and prepare for information operations.

From The State and Local Election Cybersecurity Playbook.
The Belfer Center for Science and International Affairs, Harvard University (2018)

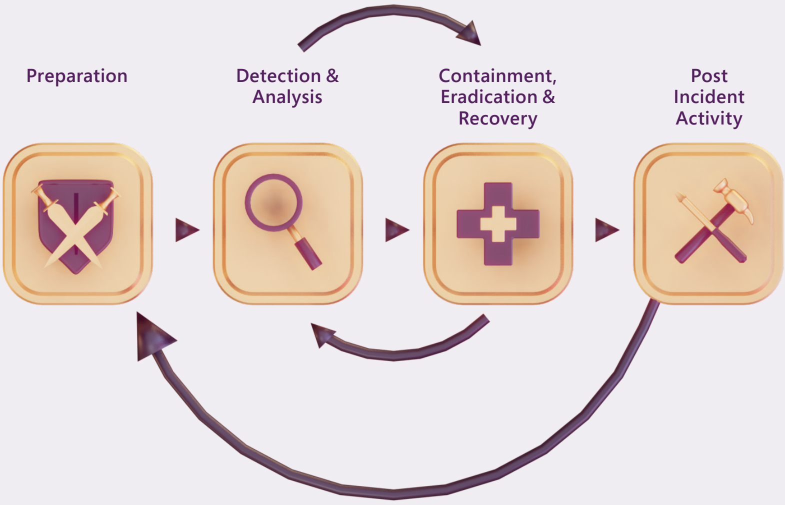


Workshop 5

Proactive and Reactive Cyber Security

Identity is critical for a company's internal functioning. It determines what users can log into, allows communication of sensitive business information, and protects the environment from external actors. However, this is exactly why it is a prime target for attackers. Once a user account has been compromised, an attacker can utilize it to download email inboxes, move laterally to other machines in the network, or even sell the credentials online for a profit.

Incident response is not just about detecting these events and recovering from the damage – Microsoft likes to think about the process as a continuous lifecycle where insights are incorporated back into the chain to learn and grow from. Each event that occurs in an environment creates an opportunity to gain visibility into what is "normal" and what is "suspicious". The best incident response strategies make use of this data over time to provide a complete picture of an organization.



Preparation

What tools and systems are currently used to prepare for an incident – this can include software that protects users as well as planning for what will happen if an incident is discovered. Having a strategy in place to handle a compromise will help respond faster and mitigate the damage done.

Tools:

- Application Guard for containerized downloads to protect machines from ransomware and other malicious files from being executed successfully.
- O365 Impersonation Protection for email security against phishing campaigns. Phishing campaigns are often the initial attack vector that hackers use to gain access to a system.

Processes:

- Establish a **security baseline** – who has access to what, systems that should be accessing each other, what is considered sensitive, and the activities that are allowed by these systems.
- Implement the rule of least privilege for accounts. It is easy for an attacker to guess passwords or successfully "phish" a user. But if this user cannot provide an attacker with further value, even if they manage to get in, the damage done is minimal. The privilege levels and which users/systems can have privileged access should be defined and held to as a standard.
- Multi-factor Authentication (MFA) for all users.
- Do not enable mailboxes for privileged roles (System Administrator, Database Administrator).
- Disable legacy authentication.
- Monitor code repositories for company secrets and API keys. People often accidentally commit code that is insecure to public storage. Hackers will browse GitHub and other sources for this information to gain access into the environment.
- Keep public facing systems up to date. Attackers will perform reconnaissance on a company's publicly accessible machines to figure out software version information. If the attacker sees that a web server is running a vulnerable version of Apache, they can use published exploit kits to easily break in.

Detection & Analysis

Have visibility into what is considered "normal" in the environment.

Establishing knowledge around what is expected, helps detect when an event occurs that is not a usual business process. Where are there potential security holes? Every company is going to have flaws as they work towards improving their posture, but if unknown, holes insecurity are exploitable vulnerabilities.

Tools:

- Utilize **Microsoft Secure Score** to view recommendations for the environment as well as the group's current security posture.
- Leverage Power BI to visualize **sign-in** data to create a picture of where and how people normally sign in.
- **Monitor the applications** that users are interacting with programmatically through Microsoft Cloud App Security to detect potentially suspicious ones
- Create alerts to notify system administrators of any changes in activity. An example of this would be triggering an alert on a downloaded file that has a hash that has not previously been seen in the environment.

Containment and Eradication

During an investigation, there is iteration between detecting and containing as new indicators of compromise (IOCs) emerge. For example, if in the analysis of sign in logs there is a suspicious login to a single machine, it's possible to "pivot" to search for activity across all machines using that IP address. This might widen the scope of compromised machines that will need remediation but having this mindset will allow for more peace of mind that nothing was missed in the future.

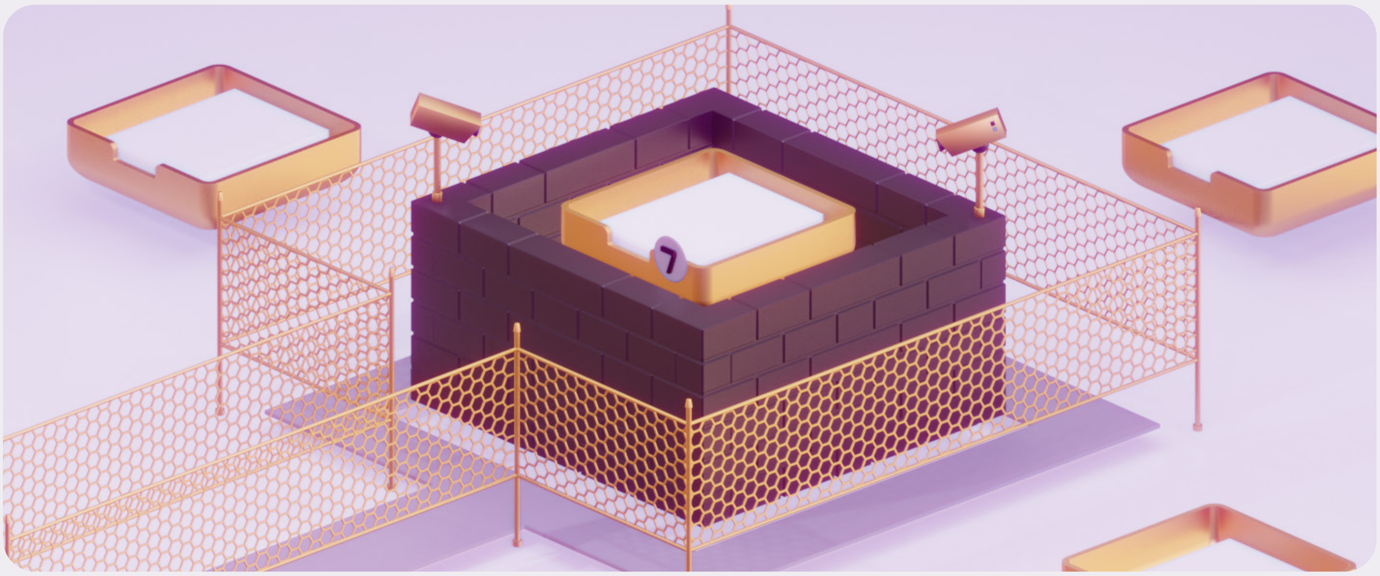
Tools:

- Use **Automated Incident Response in O365** to automatically analyze suspicious emails and pull them from inboxes before being clicked on.

Post-Incident Activity

Identify lessons learned and determine how to cycle back through the preparation stage to better prepare for the next one.

If the attacker got in via email, what are some tools to secure a user's inbox? This is the time to ask questions about what worked and what didn't and update the strategy accordingly.



Drew Robinson,
Microsoft Detection and Response Team (DART)

Workshop 5

The Basics of Risk-Limiting Audits

Good auditing is critical to providing confidence in the integrity of elections. Several kinds of auditing are available.

- Compliance audits involve inspection of election processes and equipment to evaluate the procedures involved in conduction an election.
- Administrative audits are conducted by election administrators – ideally in public view – to check physical ballots against machine counts in order to establish confidence in the correctness of the machine counts.
- Public audits allow members of the public to directly check that their votes have been correctly recorded and counted.

Administrative audits typically consist of some portion of physical ballots being randomly selected and compared to expectations. This has traditionally been accomplished by following pre-set criteria. For instance, it may be decided before an election that 2% of precincts will be selected at random and their ballots will be hand counted to see if they match the machine tallies.

The concern about traditional audits is that the pre-set criteria can be insufficient to gain confidence in close elections while being unnecessarily burdensome for elections with large margins of victory.

Risk-limiting audits (RLAs) are a dynamic alternative to traditional administrative audits. The risk limit is determined before the start of an RLA and describes the maximum probability that a full hand count would produce a different result (winner). By considering the margin of victory and performing statistical computations during the audit, an RLA can often achieve high confidence while examining far fewer ballots or continue auditing beyond a pre-set stopping point when necessary to achieve sufficient confidence in a close election. Although usually far more efficient, one disadvantage of an RLA is that the dynamic nature makes it difficult to allocate time and resources because there is no certainty in advance of how long the audit might continue.

The principal varieties of RLAs are ballot-polling audits and ballot-comparison audits. In ballot-polling audits, physical ballots are selected at random and a running tally is computed that is expected to converge to the previously announced tally.

In ballot-comparison audits, an *electronic cast-vote record* (CVR) of the contents of each ballot is recorded. Physical ballots are then selected at random and compared to corresponding CVRs. Since every match should be perfect, one needn't wait for convergence and can therefore achieve the risk limit by touching far fewer ballots.

One challenge with ballot-comparison audits is how to manage the list of CVRs. Publishing the full list of CVRs can enable coercion because a voter can be instructed to cast a vote with a very specific pattern of selections, and a coercer can subsequently check the public record to see if a ballot with that pattern is present in the voter's precinct. However, if the CVRs are not published, then the audit is not convincing – from the perspective of an observer, administrators have merely selected ballots and claimed without proof that they match the undisclosed list of CVRs.

The challenge can be solved by publishing encryptions of all of the CVRs together with publicly-verifiable proofs that the CVRs match the announced tallies. After the audit is complete, the audited CVRs can be decrypted and shown to match the corresponding physical ballots. Since only a small fraction of CVRs are revealed, voter privacy is preserved. A benefit of this approach is that existing tools for public auditing can be used to encrypt ballots and produce the necessary proofs.

Josh Benaloh,
Senior Cryptographer, Microsoft Research

Workshop 5

End-to-End Verifiable Election Technologies to Improve Voting System Security

Across the world's democracies, various computer systems are increasingly being used in the official casting and counting of ballots during an election. These technologies - such as ballot marking devices, optical scanners for reading hand-marked paper ballots, or even experimental online/remote voting solutions - provide significant benefit to elections administration including scale, meeting accessibility needs, and speed & accuracy of counting. However, these systems must be trusted and properly secured in order to be effective, and there must be significant cybersecurity considerations given to all electronic components.

End-to-End Verifiability (E2E-V) is a set of technology and encryption solutions that aim to answer the question: "How can I trust the **accuracy** of an election outcome... if I worry that the software, hardware, transmission infrastructure, or personnel responsible for conducting the election could be untrustworthy?" Unlike banking software or other high-security industries, secret ballot elections require a unique set of security requirements because an individual's data (votes) must always be kept a secret, and there can be no direct tie between a person's **identity and their vote.**

E2E-V honors this by focusing on two primary principles:

- **Privacy** – Nobody except the voter should know the contents of any one particular vote. All votes are encrypted immediately upon casting and no one vote is ever decrypted.
- **Integrity** – Voters are issued a unique Verification Code to check that their vote was included in the final tally, anyone can verify that the recorded votes have been correctly tallied, and the software cannot "cheat" and announce an incorrect tally without it being obviously detectable.

In its 2018 report "**Securing the Vote**," the National Academy of Sciences recommended that state and local jurisdictions should conduct and assess pilots of end-to-end-verifiable elections systems.

Microsoft recently launched a free, open-source development kit (SDK) called **ElectionGuard** that implements the principals of E2E-V. ElectionGuard is designed to run on new or existing voting systems to make voting more secure, auditable, verifiable, and trustworthy. As of early 2021, ElectionGuard has been used in public elections and legislative secret-ballot elections in the United States and is currently being explored for use on multiple continents. Information on ElectionGuard can be found at **www.electionguard.vote**.

ElectionGuard can also be used to enhance the security and privacy of post-election audits, such as Risk Limiting Audits (RLAs). Public auditing and administrative auditing are crucial to provide confidence that elections have been conducted and tallied properly, but these audits sometimes compromise voter privacy by publicly revealing and opening sealed ballots. ElectionGuard can be helpful in preserving voter privacy by encrypting data during these post-election audits.

Ethan Chumley,
Senior Security Strategist, Defending Democracy Program, Microsoft

Workshop 5

A Look at the 2020 U.S. Election - Improved Practice: Communication and Coordination on Cyber and Election Infrastructure Security Increased Substantially, But There is Still Room for Improvement

Ahead of the 2020 U.S. election, the U.S. government, private sector, and civil society organizations made substantial progress in coordinating on election infrastructure and cybersecurity. New institutions and agencies played an important role in facilitating communication and cooperation between federal, state, and local officials, as well as with political campaigns.

After the 2016 election, the federal government and civil society partners established new mechanisms to close gaps between federal and state authorities, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

In 2020, coordination between federal, state, and local officials, as well as between cross-sector stakeholders, increased dramatically. CISA and EI-ISAC built and maintained extensive relationships to open lines of communication for sharing information and good practices. EI-ISAC hosted a joint "virtual situational awareness room" that brought together hundreds of election officials, CISA and EI-ISAC staff, social media company staff, and political party representatives to share information, monitor threats, and provide guidance around election security in the hours before, during, and after the election.[20] EI-ISAC also operated an election day war room with incident-response, intelligence, and engineering teams on standby to monitor threats and provide support to state and local members as needed.[21]

Federal agencies and civil society partners offered a wealth of resources and assistance to state and local jurisdictions, as well as to campaigns, to help secure and carry out the election, providing support that officials may not have otherwise had. These efforts deserve to be applauded, but there is still room to achieve greater buy-in and security. For example, while almost 3,000 state and local election authorities have joined the EI-ISAC as of November 2020, there are more than 10,000 jurisdictions that run elections across the country.[22]

From the Alliance for Securing Democracy's assessment of the 2020 U.S. election:
Brandt, J. and Hanlon, B. (2021, March 30). ***Defending 2020: What Worked, What Didn't, and What's Next.***[23]

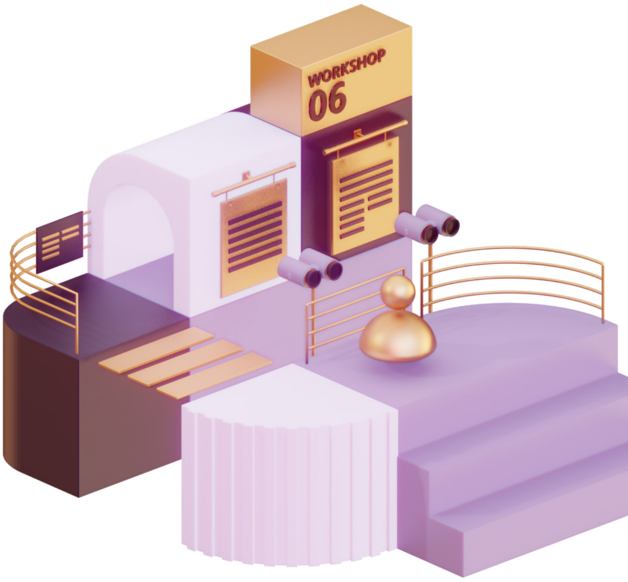
[20] MS-ISAC hits 10,000 members, eyes continued growth with local governments. Freed, B. (2020, December 14). **https://statescoop.com/ms-isac-10000-members-cis-20th-anniversary/;** International Election Observation Mission. Organization for Security and Cooperation in Europe Parliamentary Assembly (2020, November 3) **https://www.osce.org/files/f/documents/9/6/469437.pdf;** Election Administration at State and Local Levels. National Conference on State Legislatures. (2020, February 3). **https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx**

[21] 'No bar' to what election officials shared on Election Day, DHS says. Freed, B. (2020, November 05). **https://statescoop.com/no-bar-to-what-election-officials-shared-on-election-day-dhs-says/;** 'This is how it was all supposed to work': The EI-ISAC readies for Election Day. Freed, B. (2020, November 3) **https://statescoop.com/election-infrastructure-prepares-election-day-2020/;** How US security officials are watching for threats ahead of Election Day. Lyngaas, S. (2020, October 22). **https://www.cyberscoop.com/2020-election-cybersecurity-chris-krebs/**

[22] 'This is how it was all supposed to work': The EI-ISAC readies for Election Day. Freed, B. (2020, November 3). **https://statescoop.com/election-infrastructure-prepares-election-day-2020/**

[23] Brandt, J. and Hanlon, B. (2021). Defending 2020: What Worked, What Didn't, and What's Next. Alliance for Securing Democracy. **https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf**

Workshop 6:
Building Citizen Resilience



A well-informed and engaged citizenry is crucial to a stable and properly functioning democracy.

As such, citizens need access to diverse and reliable sources of information in order to develop informed views, make good decisions and exercise sound judgement. Unfortunately, the ever-growing problem of widespread disinformation and toxic online commentary found in countless social media posts is eroding citizens' faith in legitimate sources of information. Disseminated by both foreign and domestic actors, disinformation is, therefore, a threat to democracy itself, including elections.

The distrust of mainstream news outlets is particularly concerning as more and more people seek out their news and information online, where it can sometimes be challenging to distinguish between legitimate and illegitimate sources. Compounding this threat, malicious actors increasingly target specific segments of society in order to deliberately exploit, amplify and exacerbate existing divisions and tensions. Together, these phenomena have contributed to increasing polarization and the coarsening of public debate on issues such as climate change, immigration, and more recently, public health and the response to the COVID-19 pandemic.

The sixth workshop looked at how governments, industry, and civil society organizations can develop policies and programs to help citizens critically assess what they read and share in order to build community resilience to the corrosive impact of disinformation. As with all challenges of this magnitude, a comprehensive and collaborative approach is especially important to safeguarding the integrity of elections and electoral processes.

Good Practices and Strategies for Government, Digital Literacy and Fact-Checking

Community-based approaches are effective, in part, because information received from a credible community source can be a supplement to government communications. Organizations and leaders who have established networks are most likely to be trusted, especially within hard to reach or vulnerable groups.

Important considerations for governments, civil society organizations, traditional or social media platforms when partnering with communities are:

- realizing that an organization may not represent the whole community,
- ensuring people and organizations tackling information threats in various communities are connected to each other, as they can share tools and information, and
- understanding what community partners are already doing, and what they need in order to continue or extend their reach.

Being prepared and proactive—pre-bunk! Proactive measures against disinformation contribute to citizen resiliency. "Flood" the information space with accurate and helpful information, through frequent press conferences, government websites, and reliable social media accounts (e.g. EMBs or public health authorities). Focus on process issues, underscoring the mechanics and procedures relating to elections. Because disinformation travels so quickly, a purely reactive approach increases the likelihood that a false narrative will result in real harm to individuals, groups or organizations.

Develop tangible suggestions and nurture a positive, civic-minded narrative. Focus on the virtues of democracy, strengthening the country's sovereignty, shared values, and national interest. This should be done in a manner that fosters social cohesion and applies to all countries, by focusing on the content or behaviour rather than the actor. When tackling information threats, it is also necessary to avoid platitudes and broad generalizations.

Building Civic and Digital Literacy.

Know the audience. To instill a clear sense of the democracy and democratic institutions, education and digital literacy programs should be tailored to specific demographic groups and communities. This includes students from grade school to post-secondary, as well as adults older than 65, and training programs for media companies, to help them identify information influence campaigns.

Tailor programs and content for specific communities. Target communities marginalized due to factors including income, access to technology and immigration status, and ensure education and digital literacy efforts are appropriate for those populations. It is also necessary to recognize which educational tools are effective for different populations. For example, social media or online tools may be effective for youth engagement, whereas in-person workshops at community centres and libraries may be more effective for older populations. Content should be simple and non-judgmental. It should encourage people to pause and reflect on what they see online before believing or sharing it.

Digital tools are essential. Effective digital literacy efforts increasingly require access to digital tools to identify fake social media accounts, manipulated images and video, and the original source of the information. These tools are often free, inexpensive and open-source. In addition, it is crucial to ensure that reliable research and legitimate content is made widely accessible to help citizens recognize disinformation.

Workshop 6

The Importance of Fact-Checking

The profile of fact checking has increased significantly over the past decade. Fact checkers are now a trusted source of information for millions of people around the world. There is increasing evidence that fact checking works. Studies have found that if you show people an example of misinformation, then show some of them a correction, and the others nothing, belief in the incorrect misinformation is significantly reduced in the group who see the correction.

The information ecosystem in which fact checkers are operating now is complex and rapidly changing. Over recent years online misinformation has become a growing concern, with the internet's speed and scale presenting opportunities for misinformation to spread like never before. As the UK's independent fact checking charity, Full Fact has seen first-hand how bad information promotes hate, damages people's health, and hurts democracy.

Fact checkers are at the front line of finding and assessing misinformation. In a report published in 2020 we found that the challenges involved are varied. For example, within the monitoring and selection process, fact checkers grapple with large pools of potential claims to check, questions over how to define virality, the opaque nature of some platforms, and responding to high volumes of audience requests.

In researching the accuracy of a claim, fact checkers experience challenges including accessibility of information and the transparency of authorities, highly repetitive claims and research tasks, and changes to or discontinuation of online investigation tools. When publishing and distributing their work, fact checkers face other challenges such as trying to balance the demand for fact checks from internet companies and the impact of these partnerships as well as internet shutdowns, the large effort required to set up new social media channels, and the difficulty of sustaining media partnerships.

While technology assists many fact checkers, there are limits to its effectiveness. Technology cannot immediately resolve issues such as obtaining information from certain governments or lack of transparency and access to information - and it has the potential for unintended consequences such as racial bias.

Bad information is as old as humanity, but tackling it globally when lives are in danger, while respecting freedom of expression, is a new challenge. There is a need for much greater collaboration between all of those who contribute to the information ecoystem: internet companies such as Twitter, Facebook and Google, fact checkers around the world, health bodies, researchers and civil society groups. If we have prepared responses that are already discussed and researched, we will all be able to move faster and much more effectively. That is why Full Fact has been developing a new framework for tackling information incidents, with funding support from Facebook.

Fact checkers play a helpful role within the information ecosystem but they cannot solve the problem alone. We must all play our part to ensure accurate information prevails.

Full Fact

Workshop 6

Canadian Heritage's work on funding projects in advance of the 2019 election

Prior to the 2019 Canadian general election, there were concerns that Canadian citizens could be targeted by online disinformation that could either influence the outcome of the election and/or sow societal discord.

In response to these concerns, on January 30, 2019, the Minister of Democratic Institutions announced the Government of Canada's approach to protecting Canada's democracy. This allowed the Department of Canadian Heritage (PCH) to create the Digital Citizen Initiative (DCI) and **invest $7 million** in citizen-focused activities to support democracy and social cohesion in Canada, ahead of the 2019 Federal Election. The strategic objective of these citizen-focused activities was to build citizen resilience against online disinformation and build partnerships with civil society to support a healthy information ecosystem. More than 20 projects in the form of civic, news and digital media literacy offered through third-party activities and programming were funded by PCH and the DCI, ranging from awareness sessions and workshops to development of learning materials to foster digital media and civic awareness.

Specifically, projects that received funding aimed to help Canadians critically assess online information; understand how algorithms work and when they might impact a user's online experience; recognize how and when malicious actors exploit online platforms; acquire skills to avoid online manipulation.

In order to maximize the efficiency and impact of the projects ahead of the 2019 Federal Election, the DCI prioritized initiatives that could reach a wide range of participants varying in age, geographical location, ability, employment, identity, and with a range of different offerings. The funding would also enable both direct and indirect participation in citizen-focused activities.

"Direct" participants are those who took part in workshops and educational activities, social media engagement, working groups, distributed educational materials, challenges and competitions. "Indirect" participants are those Canadians who were reached by DCI funded activities through less direct methods. This includes ads on online platforms and social media, further workshops led by directly engaged participants ("train the trainer" approaches) and informally shared knowledge by youth, educators and adults.

The 2019 Federal Budget granted the DCI $19.4M over 4 years to continue its activities and expand them beyond the scope of elections. Now, the DCI runs annual calls for funding for citizen-focused activities through a dedicated contribution program and is a key part of the ecosystem of actors that seeks to build citizen resilience in Canada.

Canadian Heritage

Workshop 6

A Look at the 2020 U.S. Election, What Went Well: Civil Society Conducted Essential Resilience-Building Activity in the Information Space

Throughout the 2020 election cycle, civil society organizations conducted resilience building activities that filled important gaps between government and the private sector—monitoring the domestic information space, publicly informing citizens and preparing them for false narratives, and facilitating information sharing and coordination across sectors. These activities were fueled by a high degree of public interest and considerable philanthropic support. It is a model that generated substantial, impactful activity, but it may not be a sustainable one. Yet institutionalizing these efforts could pose significant challenges of its own, given concerns around rights to privacy and free expression.

Among the most impactful civil society efforts in this space was the Election Integrity Partnership (EIP), a coalition of research organizations that aimed to foster real-time information sharing between researchers, civil society organizations, social media platforms, government agencies, and election officials.[23] EIP served as an important clearinghouse for information sharing among government, platforms, and researchers. It played an important role in flagging harmful content for companies. And it communicated regularly with the public, producing real-time analyses of disinformation tactics and narratives and holding frequent public briefings.[24]

Myriad other civil society organizations – from Election SOS to the National Task Force on Election Crises and the Disinfo Defence League -- provided election officials, journalists, and domestic audiences with tools to identify and counter mis and disinformation[25]

From the Alliance for Securing Democracy's assessment of the 2020 U.S. election: Brandt, J. and Hanlon, B. (2021, March 30). *Defending 2020: What Worked, What Didn't, and What's Next.*[26]

[23] Announcing the EIP. Stamos, A. (2020, July 31). **https://www.eipartnership.net/news/announcing-the-eip**

[24] Election Delegitimization: Coming to you Live. Miller, C.M. et al. (2020, November 18). **https://www.eipartnership.net/rapid-response/election-delegitimization-coming-to-you-live;** Weaponizing projections as tools of election delegitimization. Bak-Coleman, J. (2020, November 05). **https://www.eipartnership.net/rapid-response/weaponizing-projections-as-tools-of-election-delegitimization**

[25] Meet the researchers and activists fighting misinformation. Birnbaum, E. (2020, November 17). **https://www.protocol.com/election-day-2020-misinfomation-disinformation;** The Fight Against Disinformation Requires the Right Tools. PEN America. (2020, December 03). **https://pen.org/the-fight-against-disinformation-requires-the-right-tools/;** Resources. The National Task Force on Election Crises. (n.d.). **https://www.electiontaskforce.org/resources;** Three New Ways Civil Society Is Protecting the U.S. Election. Quarcoo, A. (2020, October 28). **https://carnegieendowment.org/2020/10/28/three-new-ways-civil-society-is-protecting-u.s.-election-pub-83063**

[26] Brandt, J. and Hanlon, B. (2021). Defending 2020: What Worked, What Didn't, and What's Next. Alliance for Securing Democracy. **https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf**

Bibliography

Workshop 1

Beavers, O. (2020, August 7). *US intelligence says Russia seeking to "denigrate" Biden.* The Hill. https://thehill.com/policy/national-security/511078-top-intelligence-official-warns-of-foreign-influence-ahead-of-2020

Brandt, J. and Hanlon, B. (2021). *Defending 2020: What Worked, What Didn't, and What's Next.* Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf

Intelligence Committee (2020, August 10). *Rubio, Warner Release Joint Statement in Response to NCSC Director Evanina.* US Senate Select Committee on Intelligence https://www.intelligence.senate.gov/press/rubio-warner-release-joint-statement-response-ncsc-director-evanina

Internet Crime Complaint Center (IC3) (n.d.). *Frequently Asked Questions.* Federal Bureau of Investigation, United States of America Department of Justice. https://www.ic3.gov/#

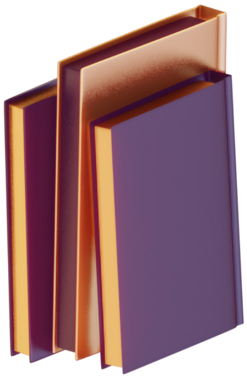
Nakashima, E. (2020, November 3). *U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election.* The Washington Post. https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html

Nakashima, E. et al. (2020, October 22). *U.S. government concludes Iran was behind threatening emails sent to Democrats.* The Washington Post. https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/

Ratcliffe, J. (October 22, 2020). *DNI John Ratcliffe's Remarks at Press Conference on Election Security.* Office of the Director of National Intelligence. https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security

Rosenstedt, L. (2021, February 5). Hybrid CoE Paper 5: *Improving cooperation with social media companies to counter electoral interference.* The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-paper-5-improving-cooperation-with-social-media-companies-to-counter-electoral-interference/

U.S. Department of the Treasury. (2020, September 10). *Treasury Sanctions Russia-Linked Election Interference Actors.* United States Government https://home.treasury.gov/news/press-releases/sm1118



Workshop 2

Cybersecurity and Infrastructure Security Agency. (n.d). *Foreign Interference. U.S. Department of Homeland Security.* https://www.cisa.gov/publication/foreign-interference

Cambridge Dictionary. (n.d.). *Coercion.* Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/coercion

Cambridge Dictionary. (n.d.). *Interfere.* Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/interfere

Department of Home Affairs. (n.d). *National Security: Countering Foreign Interference.* Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Facebook. (2021). *Community Standards: 20. Inauthentic Behavior.* Facebook, Inc. https://www.facebook.com/communitystandards/inauthentic_behavior

Hollis, D. (2018, April 3). *B., The Influence of War; The War for Influence. Temple International & Comparative Law Journal, Vol. 32, No. 1, 2018.* Temple University Legal Studies Research Paper No. 2018-19. https://ssrn.com/abstract=3155273

Pamment, J., et al. (2018, July 1). *Countering Information Influence Activities: The State of the Art.* Swedish Civil Contingencies Agency and Lund University. https://www.msb.se/RibData/Filer/pdf/28697.pdf

Parton, C. (2019, February). *China- UK Relations: Where to Draw the Border Between Influence and Interference?* Royal United Services Institute for Defence and Security Studies. https://rusi.org/sites/default/files/20190220_chinese_interference_parton_web.pdf

Twitter. (2021, January). *Civic Integrity Policy.* Twitter, Inc. https://help.twitter.com/en/rules-and-policies/election-integrity-policy

Turnbull, M. (2019, December 7). *Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.* Malcom Turnbull Website. https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an

Workshop 3

COVID Working Group by the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council. (n.d.). *Assisting Sick, Exposed, Symptomatic, and quarantined voters.* United States of America Election Assistance Commission. https://www.eac.gov/sites/default/files/electionofficials/gcc/Assisting_Sick_Exposed_Sympomatic_and_Quarantined_Voters_092920.pdf

Cortes, E. et al. (2020, June 5). *A Guide for Election Officials: Preparing for Cyberattacks and Technical Problems During the Pandemic*. Brennan Center for Justice. https://www.brennancenter.org/sites/default/files/2020-06/2020_06_PreparingforAttack_Checklist.pdf

Norden, L. et al. (2020, March 19). *Estimated Costs of COVID-19 Election Resiliency Measures.* Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/estimated-costs-covid-19-election-resiliency-measures

Workshop 4

Canadian Centre for Cyber Security. (2019, April 5). *2019 Update: Cyber Threats to Canada's Democratic Process*. Government of Canada. https://cyber.gc.ca/en/guidance/2019-update-cyber-threats-canadas-democratic-process

Canadian Centre for Cyber Security. (2019, April 5). *Update on cyber threats to Canada's democratic process.* Government of Canada. https://cyber.gc.ca/en/guidance/update-cyber-threats-canadas-democratic-process

Democratic Institutions. (2019, July 9). *Cabinet Directive on the Critical Election Incident Public Protocol.* Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html

Democratic Institutions. (2019, July 9). *Critical Election Incident Public Protocol.* Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html

Democratic Institutions. (2019, November 20). *Critical Election Incident Public Protocol: Backgrounder.* Government of Canada. https://www.canada.ca/en/democratic-institutions/news/2020/10/the-critical-election-incident-public-protocol.html

Democratic Institutions. (2019, July 9). *Critical Election Incident Public Protocol: Graphic.* Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/public-protocol.html

Democratic Institutions. (2020, March 19). *Expecting social media platforms to act: Backgrounder.* Government of Canada. https://www.canada.ca/en/democratic-institutions/news/2019/01/encouraging-social-media-platforms-to-act.html

Democratic Institutions. (2020, March 19). *Protecting Democracy- Safeguarding our elections and Democratic Institutions.* Government of Canada.https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html

Democratic Institutions. (2019, February 7). *Security and Intelligence Threats to Elections (SITE) Task Force: Graphic.* Government of Canada. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html

Journalism Trust Initiative. (n.d.). *The Problem. The Solution. The Process.* Journalism Trust Initiative. https://jti-rsf.org/en/

Landauro, I, and Myriam R. (2018, December 3). *'Yellow Vest' Protesters Knock Wind out of French Business, Economy.* Thomson Reuters. www.reuters.com/article/us-france-protests-economy-idUSKBN1O21IA.

Workshop 5

Berger, M., et al. (2018). *The State and Local Election Cybersecurity Playbook*. The Belfer Center for Science and International Affairs, Harvard University, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Brandt, J. and Hanlon, B. (2021). *Defending 2020: What Worked, What Didn't, and What's Next.* Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf

Cortés, E., et al. (2020). *Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials.* Brennan Center for Justice, New York University School of Law, https://www.brennancenter.org/our-work/research-reports/preparing-cyberattacks-and-technical-problems-during-pandemic-guide.

Chander, G. (2019, September 9). *Automated incident response in Office 365 ATP now generally available.* Microsoft. https://www.microsoft.com/security/blog/2019/09/09/automated-incident-response-office-365-atp-now-generally-available/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Election Infrastructure Cyber Risk Assessment and Infographic.* United States of America. https://www.cisa.gov/publication/election-cyber-risk

Cybersecurity and Infrastructure Security Agency. (n.d.). *Mail-in Voting Risk: Infrastructure and Process*. United States of America. https://www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-infographic_508.pdf

Department of Homeland Security. (2020, July 14). *Election Security: US Electoral Process*. United Stated of America. https://www.dhs.gov/topic/election-security

Freed, B. (2020, December 14). *MS-ISAC hits 10,000 members, eyes continued growth with local governments.* https://statescoop.com/ms-isac-10000-members-cis-20th-anniversary/

Freed, B. (2020, November 05). *'No bar' to what election officials shared on Election Day, DHS says.* https://statescoop.com/no-bar-to-what-election-officials-shared-on-election-day-dhs-says/

Freed, B. (2020, November 3). *'This is how it was all supposed to work': The EI-ISAC readies for Election Day.* https://statescoop.com/election-infrastructure-prepares-election-day-2020/

Levine, D. (2020). *The Election Official's Handbook: Six steps local officials can take to safeguard America's election systems,* German Marshall Fund of the United States, https://securingdemocracy.gmfus.org/the-election-officials-handbook-six-steps-local-officials-can-take-to-safeguard-americas-election-system/

Lyngaas, S. (2020, October 22). *How US security officials are watching for threats ahead of Election Day.* https://www.cyberscoop.com/2020-election-cybersecurity-chris-krebs/

Microsoft. (n.d.). *Anti-phishing policies - Office 365*. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide

Microsoft. (2020, October 05). *Automated incident response in Office 365 ATP now generally available.* https://www.microsoft.com/security/blog/2019/09/09/automated-incident-response-office-365-atp-now-generally-available/

Microsoft. (n.d.). *Azure identity & access security best practices.* https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Microsoft. (n.d.). *Investigate risky OAuth apps.* https://docs.microsoft.com/en-us/cloud-app-security/investigate-risky-oauth

Microsoft. (2021). ElectionGuard. http://www.electionguard.vote./

Microsoft. (n.d.). *Microsoft Defender Application Guard (Windows 10)* - Windows security. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview

Microsoft. (2014). *Mitigating Pass the Hash Attacks and Other Credential Theft.* Microsoft. https://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

Microsoft. (n.d.). *Sign-in activity reports in the Azure Active Directory portal.* https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Mitre, *Election Integrity: Resources for 2020 and Beyond*, https://electionintegrity.mitre.org/

National Conference on State Legislatures. (2020, February 3). *Election Administration at State and Local Levels.* https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx

Organization for Security and Cooperation in Europe Parliamentary Assembly (2020, November 3). *International Election Observation Mission.* https://www.osce.org/files/f/documents/9/6/469437.pdf

Senate Report No. 116-290, Vol. 1, at 6 (2020). *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure, with Additional Views.*

Workshop 6

Bak-Coleman, J. (2020, November 05). *Weaponizing projections as tools of election delegitimization.* https://www.eipartnership.net/rapid-response/weaponizing-projections-as-tools-of-election-delegitimization

Birnbaum, E. (2020, November 17). *Meet the researchers and activists fighting misinformation*. https://www.protocol.com/election-day-2020-misinfomation-disinformation

Brandt, J. and Hanlon, B. (2021). *Defending 2020: What Worked, What Didn't, and What's Next.* Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/Defending-2020.pdf

Canadian Heritage. (2019, July 2). *Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation.* Government of Canada. https://www.canada.ca/en/canadian-heritage/news/2019/07/helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html

Communications Security Establishment. (n.d.). *Cyber Hygiene*. Government of Canada. https://www.cse-cst.gc.ca/en/cyberhygiene-pratiques-cybersecurite

Cybersecurity and Infrastructure Security Agency. (n.d.). *#protect2020 Rumor vs. Reality*. United States of America. https://www.cisa.gov/rumorcontrol

Cybersecurity and Infrastructure Security Agency. (n.d.). *Resilience Series Graphic Novels*. United States of America. https://www.cisa.gov/cfi-resilience-series-graphic-novels

Full Fact. (n.d.). *About us: Contact*. Full Fact. https://fullfact.org/about/contact/

Full Fact. (n.d.). *About us: Full Fact's Research*. Full Fact. https://fullfact.org/about/research/

Full Fact. (2020, December 17). *Blog: Bringing together the UK government, Facebook, and others to combat misinformation crises*. Full Fact. https://fullfact.org/blog/2020/nov/framework-combat-misinformation/

Full Fact. (2020, December 17). *Blog: The challenges of online fact checking: how technology can (and can't) help*. Full Fact. https://fullfact.org/blog/2020/dec/the-challenges-of-online-fact-checking-how-technology-can-and-cant-help/

Government of Canada. (2020, October 17). *Online Disinformation- Digital Citizen Initiative*. Government of Canada. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html

Miller, C.M. et al. (2020, November 18). *Election Delegitimization: Coming to you Live*. https://www.eipartnership.net/rapid-response/election-delegitimization-coming-to-you-live

PEN America. (2020, December 03). *The Fight Against Disinformation Requires the Right Tools*. https://pen.org/the-fight-against-disinformation-requires-the-right-tools/

Quarcoo, A. (2020, October 28). *Three New Ways Civil Society Is Protecting the U.S. Election*. https://carnegieendowment.org/2020/10/28/three-new-ways-civil-society-is-protecting-u.s.-election-pub-83063

Stamos, A. (2020, July 31). *Announcing the EIP*. https://www.eipartnership.net/news/announcing-the-eip

The National Task Force on Election Crises. (n.d.). *Resources*. https://www.electiontaskforce.org/resources