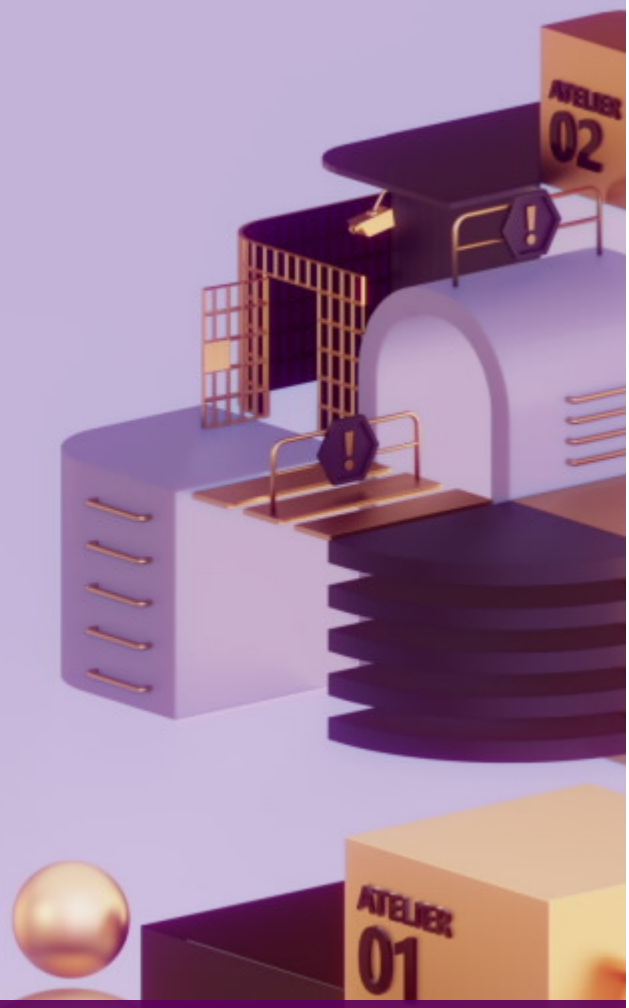
L’approche multipartite

Recueil sur la défense des processus électoraux



Microsoft

alliance for securing democracy
GMF

Canada

Lettre de presentation

Les gouvernements, la société civile et l'industrie reconnaissent l'importance d'un espace d'information numérique sûr, stable et accessible, particulièrement dans l'environnement exigeant et imprévisible d'aujourd'hui.

En novembre 2018, le gouvernement de la France a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace (Appel de Paris), soulignant que « [l]e cyberespace joue désormais un rôle capital dans tous les aspects de notre vie » et qu'« il relève de la responsabilité d'un grand nombre d'acteurs, chacun dans son domaine propre, de le rendre plus fiable, plus sûr et plus stable. »

L'Appel de Paris, le plus important accord volontaire multipartite sur la cybersécurité, est appuyé par plus de 1100 entités dans le monde, dont plus de 75 gouvernements et des centaines d'organisations de l'industrie et de la société civile. Il repose sur un ensemble de neuf principes visant à rendre le cyberespace sécuritaire ainsi qu'à orienter la discussion et l'action sur les cybermenaces, notamment celles qui concernent l'ingérence électorale.

Cochampions du principe 3 : Défendre les processus électoraux – en vertu de l'Appel de Paris, l'Alliance for Securing Democracy (ASD), le gouvernement du Canada et Microsoft travaillent ensemble au renforcement de notre capacité collective de prévenir l'ingérence malveillante qu'exercent des acteurs étrangers au moyen de cyberactivités pour nuire aux processusélectoraux.

La confiance dans le processus électoral et dans la légitimité des résultats des élections est fondamentale pour la démocratie. Le défi de l'ingérence dans nos institutions démocratiques touchant tous les secteurs de la société, protéger ces institutions exige une utilisation judicieuse de la technologie ainsi que de nouveaux modèles de partenariat et de coopération. À un moment où la confiance dans nos institutions est mise à l'épreuve sur tant de fronts, réunir un large éventail de parties intéressées pour augmenter notre résilience face à ces menaces en évolution contribuera à maintenir la confiance des citoyens dans la façon dont leurs représentants sont choisis.

Tout au long de 2020, les cochampions ont réuni la communauté mondiale dans des ateliers multipartites, chacun de ceux-ci abordant une question cruciale liée à la prévention de l'ingérence dans les processusélectoraux. Au cours de cesateliers, des observations clés, des idées et des pratiques efficacesont été recueillies auprès d'un groupe diversifié d'experts, de praticiens et d'intervenants. Surla base de ce que nous avons entendu et appris au cours de cesdiscussions, nous avons mis au point un recueil de bonnes pratiques qui offre aux organes d'administration des élections, aux gouvernements et aux autres acteurs de la démocratie une ressource utile pour soutenir leurs efforts visant à protéger les élections et la démocratie.

Les idées et les points de vue exprimés au cours de ces discussions et figurant dans le présent recueil reflètent les divers points de vue et l'expertise d'un groupe véritablement multipartite, et non pas nécessairement les points de vue des différents participants ou des cochampions. Pourtant, c'est précisément pour cette raison que cette approche multipartite en matière de sécurité électorale est si cruciale. En effet, étant donné que les processus électoraux – de même que les menaces et les vulnérabilités – varient considérablement d'un pays à l'autre, ce recueil reconnaît qu'il n'existe pas d'approche unique pour protéger la démocratie. Toutefois, en travaillant ensemble, comme nous l'avons fait ici, nous continuerons à approfondir notre savoir-faire et nos connaissances mondiales des moyens de contrer l'ingérence, qui sont efficaces et appropriés dans différentes situations.

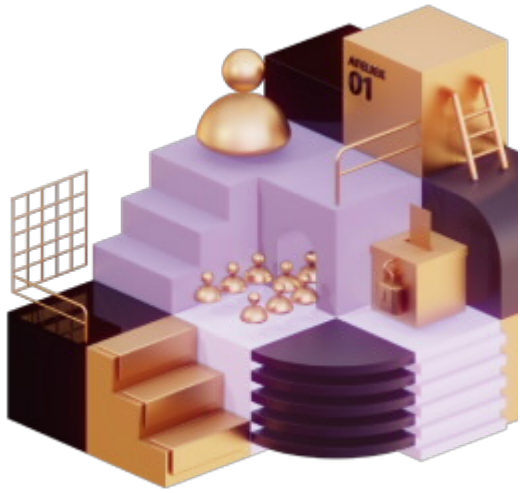
Le cyberespace devient un lieu de plus en plus important pour l'exercice de la démocratie, mais également pour les menaces qui pèsent sur lui. Dans ce contexte, nous sommes résolus à protéger les élections de l'ingérence étrangère et offrons ce recueil de bonnes pratiques à ceux qui partagent cet objectif. Nos efforts collectifs pour protéger la confiance envers nos institutions démocratiques contribueront à ce que les citoyens demeurent mobilisés et informés, ce qui, au bout du compte, représentele meilleur rempart de la démocratie.

Brad Smith,
President,
Microsoft

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

L'honorable Dominic LeBlanc, c.p.,c.r.,député
Président du Conseil privé de la Reine pour le Canada et ministre des Affaires intergouvernementales

Table des matières

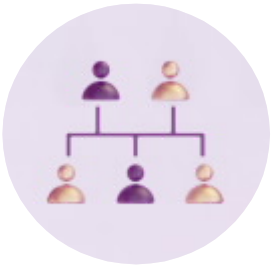


Atelier 1 : Améliorer l'échange multilatéral d'information

Rassembler des communautés pour examiner des menaces et trouver des solutions pratiques favorise la résilience à l'égard des menaces hybrides. À de nombreux endroits, les services de renseignement et les autorités électorales se connaissent mal ou se parlent peu. Le manque de résilience est une vulnérabilité bureaucratique, mais on peut atténuer celle-ci par des efforts soutenus de décloisonnement au sein des secteurs public et privé ainsi qu'entre ceux-ci. Le défi de l'échange d'information devient encore plus important entre les secteurs public et privé.

Dans la détermination des vulnérabilités, il convient d'envisager l'écosystème dans son ensemble – chaque partie du cycle électoral est potentiellement sujette à l'ingérence et a besoin de protection. De plus, il est important de réaliser que l'ingérence vient autant d'acteurs étatiques que d'acteurs non étatiques. L'ingérence n'est pas nécessairement un acte unique; elle résulte parfois des effets cumulatifs de gestes individuels qui, additionnés, se traduisent par un acte d'ingérence qui a des conséquences, p. ex. l'ingérence et la désinformation numériques. La présence de désinformation dans un environnement électoral, est souvent indicatrice de la présence de menaces hybrides à plus grande échelle. Puisque les démocraties souffrent des conséquences de cet effet cumulatif, il est important de parler des menaces, des leurs auteurs et des réponses en dans un langage commun, ce qui n'est actuellement pas le cas. Enfin, il faut réaliser que les menaces évoluent tout comme les réponses.

Pratiques efficaces :



Établir des relations multipartites

Premièrement, il importe de désigner rapidement des points de contact au gouvernement, dans la société civile et dans le secteur privé ainsi que de gérer la taille du groupe. Lorsque ces points de contact sont choisis, il faut que les lignes de communication soient le plus simples et directes possible, et que les attentes soient claires sur l'échange d'information (tendances en matière de menaces, tactiques, techniques et protocoles). Pour assurer une communication continue durant la période électorale, des plateformes et des espaces de coopération multipartite doivent être disponibles avant et pendant l'élection. Par ailleurs, ces relations peuvent être bonifiées par une planification commune de scénarios et par des exercices de réponse rapide qui permettent de comprendre de quelle façon les personnes et les organisations réagissent. Pour accroître les perspectives, il est pertinent de travailler avec les États qui partagent nos valeurs, car les problèmes vécus par un pays ne lui sont pas propres. Des progrès peuvent être réalisés par toutes les parties grâce à l'échange de leçons apprises et à la recherche de possibilités d'actions communes.

Coordinationintragouvernementale

L'instauration d'une collaboration entre les diverses organisations et l'obtention de l'appui du sommet de la hiérarchie (le Cabinet) contribuent à assurer une communication constante. Parmi les liens importants à établir, on notera ceux entre les organismes de gestion électorale (OGE) et les experts en technologie dans le domaine de la sécurité nationale; les agents de renseignement et les spécialistes des communications; les agences centrales à l'intersection de la fonction publique et des acteurs politiques; et les spécialistes de la sensibilisation qui travaillent avec les groupes vulnérables. Pendant l'élection, il est utile de former un groupe d'experts non partisan chargé de recevoir et d'évaluer les rapports d'ingérence électorale et d'aviser le public lorsque de l'ingérence a été commise. Cela encourage les fonctionnaires à faire des signalements sans crainte de politisation. Enfin, il est primordial d'avoir une démarche inclusive en assurant la participation de tous les partis politiques, y compris les plus petits et les moins connus, afin que toutes les entités concernées sachent quoi faire et avec qui communiquer en cas d'incident. De plus, il convient d'envisager un partage de ressources avec les localités et les organisations de petite taille, par exemple les programmes de « cybernavigateurs », qui aident les autorités électorales à se défendre contre les cyberinfractions, à détecter les cyberattaques et à se remettre de celles-ci. Il en résulte un point de contact unique pour le secteur privé et une spécialisation accrue.

Élaboration de méthodes de communication

Dans toutes ces initiatives, les communications doivent se faire dans un langage clair et simple qui fournit aux citoyens des outils pour augmenter leur résilience aux tentatives d'ingérence. De plus, il convient d'évaluer le public cible et de cerner les possibilités d'éduquer et de communiquer. Chaque fois que cela est possible, on améliorera et fera connaître la méthodologie utilisée pour déterminer ce que constitue de l'ingérence et de l'influence, dans le domaine de l'information mais également dans celui de la technologie. D'abord, on établira des relations et on communiquera avec les médias dès le départ, en gardant à l'esprit que ceux-ci peuvent aussi être des vecteurs d'ingérence s'ils sont manipulés. Puis, on classifie les rapports au niveau le plus bas possible pour en maximiser la diffusion. Lorsque des incidents surviennent, on tiendra compte du pouvoir d'attribution. Les actions du gouvernement, du secteur privé et de la société civile auront des conséquences politiques distinctes; chacun de ces acteurs doit faire preuve d'un maximum de transparence dans ses critères et sa méthodologie.

Il faut tenir compte du fait que lorsqu'une entité est victime d'ingérence, cela place les parties affectées au centre des conversations. À titre de victimes, elles ont le pouvoir de libérer les acteurs du secteur privé et du gouvernement des obligations qui, autrement, empêcheraient la communication de l'information; on aura recours aux lignes de communication et aux communautés créées par la communication pour utiliser ces situations efficacement et de manière à avoir un impact. Les utilisateurs doivent être informés lorsqu'un système informatique a été compromis, mais aussi lorsqu'une tentative a été déjouée.

Enfin, on créera à l'intention de tous les pays un référentiel des bonnes pratiques afin que ces renseignements ne dépendent pas uniquement de relations individuelles. Cela est d'une importance particulière pour les petits États, qui peuvent disposer de moins de ressources ou qui comptent moins d'expériences propices à l'apprentissage.

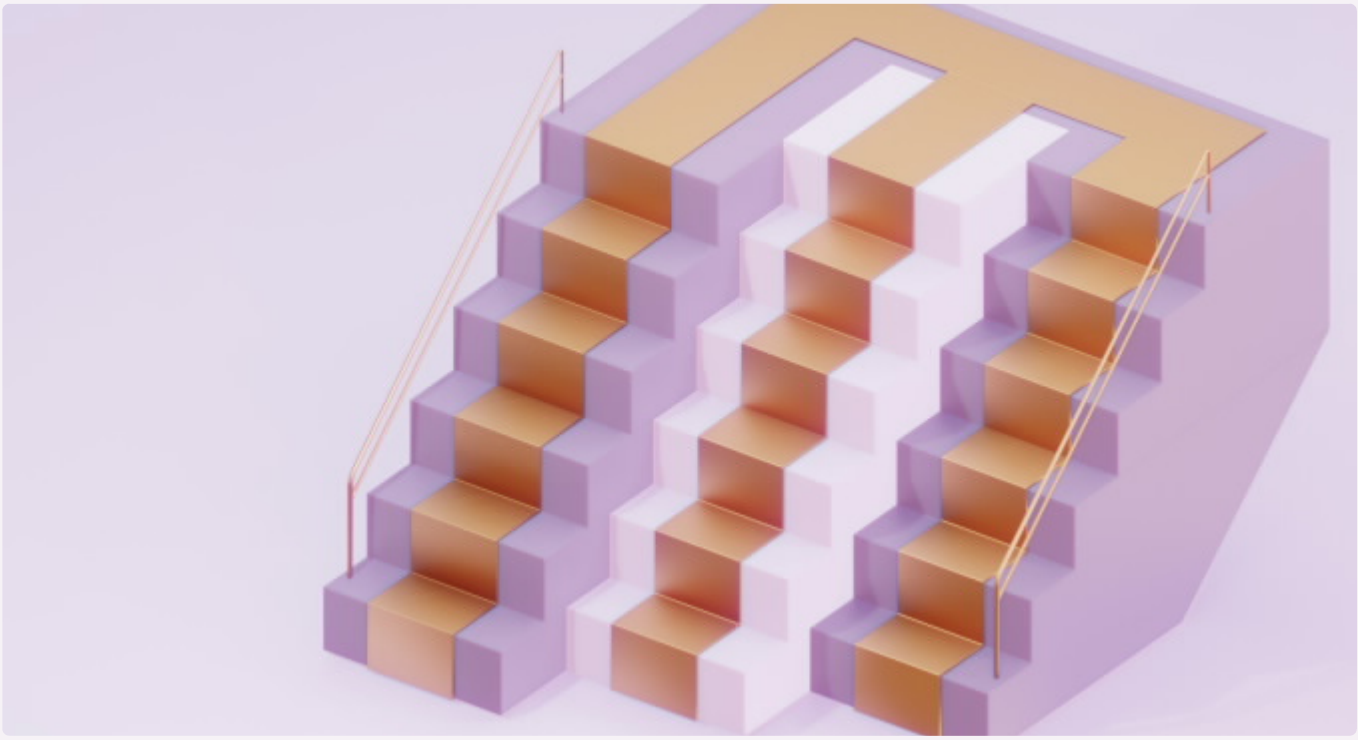
Coordination public-privé en matière de changements aux politiques

Il est important de donner au secteur privé assez de temps pour s'adapter aux changements apportés aux règles et de savoir que les grandes entreprises ont parfois plus de facilité à s'adapter que les petites.

Atelier 1

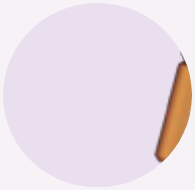
Trois façons d'améliorer la coopération pour protéger les processus démocratiques

En 2019 et 2020, le Centre européen d'excellence pour la lutte contre les menaces hybrides a réalisé un projet de défense contre l'ingérence électorale dans nos États participants. Des séminaires, des conférences et des exercices ont été offerts aux participants issus de gouvernements, d'entreprises privées et du milieu universitaire. L'objectif était de trouver des façons pratiques de contrer l'ingérence électorale; les trois bonnes pratiques suivantes sont le fruit de l'expérience que nous avons tirée du projet. Ces pratiques adoptent une approche multipartite pour contrer l'ingérence électorale en établissant une connaissance de la situation, en améliorant la compréhension et en rendant possible une réponse efficace à l'activité malveillante.



Le projet de protection des processus démocratiques du Centre européen d'excellence pour la lutte contre les menaces hybrides se poursuivra en 2021.

D'autres travaux, y compris la version intégrale du présent document, seront publiés sur www.hybridcoe.fi dans les prochains mois.

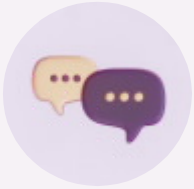


1.
La création d'une cellule multidisciplinaire gouvernementale favorise l'établissement d'une connaissance de la situation.

La cellule multidisciplinaire doit prioritairement s'employer à observer l'environnement d'information avant les élections et durant celles-ci. L'équipe peut être constituée de membres de l'équipe d'intervention en cas d'urgence informatique, de communicateurs stratégiques, d'analystes du renseignement de sources ouvertes, de la communauté du renseignement, du ministère des Affaires étrangères et de l'agence gouvernementale chargée de l'organisation de l'élection. Il convient de mener une réflexion transversale entourant la composition de l'équipe, en ne se limitant pas aux seuls ministères chargés des questions de sécurité, et d'inclure des praticiens susceptibles d'offrir une variété de points de vue.

2.
Les exercices conjoints améliorent la compréhension.

Les exercices auxquels prennent part divers acteurs, p. ex. des entreprises des médias sociaux, des organes médiatiques et le monde universitaire, sont des occasions précieuses de définir les préoccupations et les risques clés ainsi que de s'exercer à répondre de manière concertée en amont la tenue de l'élection. Les exercices sont une occasion de se familiariser avec le fonctionnement d'autres organisations, p. ex. les plateformes de médias sociaux. Ils sont également une excellente occasion de s'entretenir avec différentes parties intéressées, de poser des questions et d'établir la confiance.



3.
La mobilisation rapide de différents groupes d'intervenants assure une réponse efficace.

De nombreux pays font partie de mécanismes de coopération multilatérale visant à contrer la menace d'ingérence électorale. Ces mécanismes étant souvent liés au secteur privé, ils peuvent constituer des voies utiles pour établir des liens avec les plateformes de réseaux sociaux. Communiquer avec des pairs étatiques qui ont récemment organisé des élections peut donner lieu à un échange d'expériences précieuses et de bonnes pratiques, touchant notamment sur des nouvelles tendances ou tactiques. Le milieu universitaire est peut-être en mesure de présenter aux praticiens gouvernementaux ses analyses sur les risques associés à une prochaine élection. L'essentiel est d'établir des relations et une confiance mutuelle bien avant les élections. Tenter d'établir des relations pendant une crise risque d'être inefficace et d'empêcher de réagir en temps opportun à une activité malveillante.

Lina Rosenstedt –
Coordinatrice de projets,
Centre européen d'excellence pour la lutte contre les menaces hybrides

Atelier 1

Une étude de casen Finlande

Finlande : Groupe de coopération sur l'état de préparation à la sécurité des élections

Pour être en mesure de maintenir la stabilité du système électoral dans un environnement opérationnel en évolution, une coopération permanente entre les autorités et une meilleure compréhension de l'ingérence électoralesont nécessaires.

C'est la raison pour laquelle le ministère de la Justice finlandais a formé un Groupe de coopération sur l'état de préparation à la sécurité des élections (2.3.2020 - 30.6.2023). Le Groupe est fondé sur le projet de formation du ministère de la Justice, qui s'est déroulé entre 2018 et 2019 et a axé ses efforts sur la sensibilisation à l'ingérence électorale. Le projet de formation a conclu, par exemple, qu'un groupe de coopération permanent soutiendrait une perspective à plus long terme et des réponses plus rapides dans l'environnement informationnel changeant, également entre les élections. Le Groupe de coopération est également lié au programme national pour la démocratie de 2025, qui comprend des mesures visant à renforcer la démocratie et la participation.

Les tâches du Groupe de coopération sur l'état de préparation à la sécurité des élections sont les suivantes :

- Suivre le débat international et les rebondissements de l'ingérence et de la sécurité des élections entre les élections nationales, notamment en participant aux travaux du réseau de coopération européenne sur les élections;
- Améliorer l'échange d'informations sur les changements survenant dans les activités d'influence, les menaces hybrides, la cybersécurité et la société, qui peuvent se répercuter sur le déroulement des élections ou la confiance du public dans les élections;
- Mettre le savoir-faire à disposition et coordonner la coopération avec d'autres acteurs clés dans le domaine desélections;
- Aider le ministère de la Justice et les autres autorités électorales à améliorer la sécurité des élections.

Heini Huotarinen
Conseiller Ministériel, ministère de la Justice

JohannaKaunisvaara
Chef de Projet, ministère de la Justice

Atelier 1

Un regard sur les élections américaines de 2020 - ce qui a bien fonctionné : amélioration de la communication intersectorielle sur l'ingérence étrangère et exposition publique de celle-ci

Dans les mois qui ont précédé les élections américaines de 2020, le gouvernement, les médias et les acteurs du secteur privé ont pris des mesures préventives pour communiquer au peuple américain la menace croissante de l'ingérence étrangère.

En 2020, les acteurs gouvernementaux ont régulièrement informé le public au sujet des acteurs et des activités malveillants. Des responsables de l'Office of the Director of National Intelligence (ODNI), du FBI, de la Cybersecurity and Infrastructure Security Agency (CISA) et d'autres organismes ont fait périodiquement des points de situation publics mettant en évidence les acteurs menaçants, exposant les efforts et les activités d'influence, signalant les voies potentielles d'ingérence et informant le public des mesures prises par les organismes fédéraux pour sécuriser les élections[1].

À la suite d'une campagne iranienne visant à usurper l'identité d'un groupe d'extrême droite et à intimider les électeurs, les responsables américains ont rapidement attribué l'opération, affirmant publiquement l'effort iranien dans les 27 heures suivant l'incident – l'attribution de responsabilité la plus rapide par les responsables américains à ce jour – et informant rapidement les citoyens[2]. Les responsables ont également rassuré le public en affirmant que la communauté du renseignement avait « repéré cette activité immédiatement » et « agi rapidement en réponse à la menace ». Le FBI et la CISA ont ensuite publié quelques jours plus tard un avis de cybersécurité révélant comment les acteurs iraniens avaient accédé aux informations sur les électeurs et donnant des conseils pour atténuer la menace.

Dans les mois précédant l'élection, le Trésor américain a également sanctionné le législateur ukrainien Andrii Derkach, qu'il a décrit comme un « agent russe », pour avoir tenté d'interférer dans l'élection en diffusant de fausses informations et de faux récits sur Joe Biden, un des candidats[4]. Les efforts de Derkach avaient déjà été révélés par William Evanina, le directeur du National Counterintelligence and Security Center (NCSC)[5]. Ces actions ont suscité des appels bipartites pour que les acteurs nationaux n'utilisent pas les récits de Derkach comme une arme, ce qui a pu dissuader ou affaiblir les tentatives des législateurs et des acteurs politiques américains d'exploiter l'opération soutenue par le Kremlin pour influencer l'élection[6].

Les acteurs du secteur privé ont également rédigé des rapports périodiques et publics sur l'ingérence étrangère tout au long du cycle électoral. Des entreprises technologiques comme Microsoft, Google et Cloudflare ont surveillé les tentatives de piratage ciblant les campagnes politiques et d'autres intervenants clés, signalant souvent publiquement les tentatives de piratage et d'exploration, et attribuant la responsabilité lorsque c'était possible[7]. Facebook et Twitter ont également pris des mesures pour supprimer les comptes et réseaux inauthentiques de leurs plateformes avant l'élection, Facebook publiant de brèves explications, ainsi qu'un échantillon de contenu et une attribution provisoire à des acteurs étrangers.

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) (sans date.). 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. (le 3 novembre 2020). 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. E. Nakashima et coll. (le 22 octobre 2020). 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. J. Ratcliffe (le 22 octobre 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**

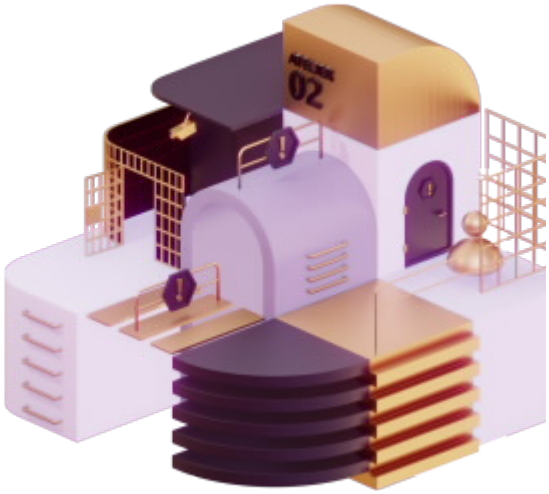
4 Treasury Sanctions Russia- Linked Election Interference Actors. U.S. Department of the Treasury (le 10 septembre 2020). Gouvernement des États-Unis. **https://home.treasury.gov/news/press-releases/sm1118**

5 US intelligence says Russia seeking to "denigrate" Biden. O. Beavers (le 7 août 2020). 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 (le 10 août 2020). 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**



Atelier 2 : Qu'est-ce qui constitue une ingérence étrangère par rapport à une influence acceptable d'un État-nation

Pour s'attaquer à la question de l'ingérence malveillante par des acteurs étrangers dans les processus électoraux et démocratiques, on doit d'abord définir ce que constitue l'ingérence et la distinguer de l'influence acceptable d'un État-nation. Le deuxième atelier de la communauté de l'Appel de Paris a été consacré aux distinctions entre les deux concepts et à la formulation des recommandations sur la façon de définir l'ingérence étrangère.

Le problème

De plus en plus, les démocraties s'emploient à prévenir l'ingérence d'acteurs étrangers malveillants et à développer leur résilience contre une vaste gamme de menaces, dont les cyberattaques et les campagnes de désinformation. Cependant, au milieu de cette activité naissante, il y a un élément absent. Il n'y a guère de consensus sur ce qu'est précisément l'« ingérence étrangère » ou sur le degré de similitude du terme « ingérence » avec des concepts connexes tels que celui d'« influence ». L'absence d'une définition commune de l'« ingérence étrangère » risque de retarder ou de compliquer les initiatives des décideurs et d'embrouiller les efforts que déploie la société civile pour faire de la sensibilisation et rallier l'opposition contre les incursions dans les processus démocratiques.

Des définitions claires établiraient les limites de ce qui est admissible, protégeraient les valeurs démocratiques fondamentales et fourniraient aux gouvernements — et aux autres piliers de la société démocratique tels que l'industrie et la société civile — de meilleures lignes directrices sur les comportements admissibles et inadmissibles dans de nouveaux domaines, notamment le monde numérique.

Définitions actuelles et autres approches

Une définition politique part du terme même d'« ingérence ». Selon le dictionnaire Larousse, « s'ingérer » consiste à « [s]'introduire indûment dans quelque chose, intervenir sans invitation ». Le mot « ingérence » est péjoratif, contrairement au mot « influence » qui est neutre[8]. Il s'agit là d'une distinction dont les praticiens devraient prendre bonne note. Ainsi, « ingérence » ne convient pas pour décrire une activité bienveillante ou bénigne d'un État-nation à l'extérieur de ses frontières.

Les définitions de l'« ingérence étrangère » des gouvernements des États-Unis et de l'Australie mettent l'accent sur les intentions malveillantes des acteurs étrangers et visent à tracer la ligne séparant le comportement acceptable du comportement inacceptable. De façon explicite ou implicite, il ressort de ces définitions des préoccupations quant aux effets sur les processus démocratiques.

Pour le département américain de la Sécurité intérieure, l'expression « ingérence étrangère » (foreign interference) s'applique aux [traduction] « actions malveillantes posées par des gouvernements ou des acteurs étrangers pour semer la discorde, manipuler le discours public, discréditer le système électoral,

8 S'ingérer. Dictionnaire Larousse (sans date). Dictionnaire Larousse https://www.larousse.fr/dictionnaires/francais/s_ing%c3%a9rer/43067

influer sur les politiques ou perturber les marchés afin de nuire aux intérêts des États-Unis et de leurs alliés[9]. Le département propose également une taxonomie de l'ingérence étrangère : activités d'information, commerce/investissement stratégique, coercition/corruption, exploitation liée à la migration et manipulation des organismesinternationaux.

En Australie, le premier ministre Malcolm Turnbull a tracé les contours de ce qui constitue une ingérence : [traduction] « Nous ne tolérerons pas les activités d'influence étrangère qui sont, de quelque manière que ce soit, secrètes, coercitives ou corrompues[10]. » En outre, le ministère australien de l'Intérieur fournit des conseils sur la manière de distinguer l'influence légitime de l'État-nation de l'ingérence inacceptable : les actes qui sont « coercitifs, secrets, trompeurs, clandestins », ainsi que ceux qui sont « contraires à la souveraineté, aux valeurs et aux intérêts nationaux de l'Australie[11] ».

Quelques définitions sont offertes par le milieu universitaire. Selon Charles Parton, chercheur associé principal au Royal United Services Institute for Defence and Security Studies (RUSI), les critères d'identification de l'ingérence devraient inclure [traductions] « une certaine notion du potentiel d'ingérence » et « une dimension de réciprocité » (une analyse visant à déterminer si « des activités semblables par des acteurs du Royaume-Uni seraient permises en Chine par le Parti communiste chinois »)[12].

Des critères plus sophistiqués ont été suggérés pour établir une distinction entre « influence » et « influence inacceptable », mais pas pour l'« ingérence ». Selon Duncan Hollis, professeur de droit à la Temple Law School, la distinction entre les activités d'influence acceptables et inacceptables se fait au moyen de cinq critères : transparence, degré de dissimulation, objectif, ampleur et impact[13]. James Pamment, maître de conférences à la Lund University, et ses collègues proposent quatre critères pour « diagnostiquer l'influence illégitime » : duplicité, intention, perturbation et ingérence[14].

Dans le secteur privé, Twitter propose des lignes directrices sur l'intégrité civique : « Il est interdit d'utiliser les services de Twitter dans le but de manipuler des élections ou d'interférer dans des élections ou autres processus civiques. Cela inclut la publication ou le partage de contenu susceptible d'empêcher la participation d'électeurs ou de tromper les gens sur les modalités de participation à un processus civique, notamment le moment et l'endroit où il a lieu. En outre, nous pouvons marquer les tweets contenant des informations fausses ou trompeuses sur des processus civiques afin de fournir plus de contexte à leur sujet[15].» Cette politique concerne entre autres les élections politiques, les recensements, les grands référendums et les initiatives de vote. Pour sa part, Facebook définit l'« [i]nterférence gouvernementale ou étrangère » comme un « [c]omportement trompeur organisé au nom d'un acteur étranger ou gouvernemental »[16].

Ingérence et autres termes

Le concept d'ingérence est voisin d'autres expressions, mais doit en être distingué : influence étrangère, pouvoir de subversion et pouvoir de convaincre, menaces hybrides, diplomatie publique, comportements trompeurs coordonnés, mesures actives, mésinformation, désinformation, influence illégitime, etc.

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

10 Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017. M. Turnbull (le 7 décembre 2019). Site Web de Malcom Turnbull. 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. (sans date). 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, février) 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. D. Hollis (le 3 avril 2018). Temple International & Comparative Law Journal, vol. 32, no 1, 2018, Temple University Legal Studies Research Paper No. 2018-19. https://ssrn.com/abstract=3155278 Pg 5.

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

15 Politique en matière d'intégrité civique. Twitter (janvier 2021). Twitter, Inc. https://help.twitter.com/fr/rules-and-policies/election-integrity-policy

16 Standards de la communauté: 20. Comportement trompeur. Facebook (2021). Facebook, Inc.https://fr-fr.facebook.com/communitystandards/inauthentic_behavior

Lignes directrices et critères efficaces

L'atelier a été l'occasion de discuter des principales difficultés liées à l'établissement de définitions pour le concept d'ingérence étrangère et de tenter de convenir des grands principes qui devraient figurer dans ces définitions. Les intervenants ont approuvé deux critères fondamentaux :

- **La notion de coercition**
- **Le concept de duplicité, ou manque de transparence et inauthenticité**

Pourquoi « coercition »?

La coercition est définie de manière générale comme étant « l'usage de la force pour contraindre une personne à entreprendre une action contre son gré[17] ». Dans le contexte de l'ingérence étrangère, il importe de déterminer s'il existe une inégalité de pouvoir entre les États-nations ou les acteurs étatiques qui permettrait à l'un de contraindre l'autre à agir de façon particulière, et de tenir cette dynamique en compte dans la détermination de l'existence ou non d'une dynamique de coercition.

Pourquoi « duplicité »?

Une caractéristique commune de l'ingérence est sa nature clandestine ou opaque. Les gouvernements étrangers tentent d'utiliser le mensonge ou des moyens opaques pour cacher leurs efforts et déstabiliser la démocratie d'un pays. Différents termes décrivent le manque de transparence, comme le mensonge, les actions clandestines, la non-authenticité. Ces expressions sont souvent interchangeables. À noter que certains experts estiment que le critère du mensonge ou de la duplicité est particulièrement important, car il peut indiquer une intention malveillante.

Critèresposantproblème

Les critères d'« intention » et d'« impact » ont suscité davantage de controverse. L'intention est un critère important, mais qui pose problème. Il est important que les responsables des politiques se demandent ce qu'un acteur étranger tente d'accomplir et déterminent si son intention est de perturber, de manipuler, ou de saper la confiance dans les institutions et les processus démocratiques. Or, l'intention est souvent très difficile à déterminer et à mesurer. Il est donc difficile de l'inclure dans les définitions. Cependant, des éléments touchant la question de l'intention apparaissent dans plusieurs définitions, et l'intention est un facteur crucial pour l'imposition de pénalités dans tous les systèmes de justice.

Il est également difficile de déterminer l'impact d'une action particulière. Dans le domaine de l'information, tout élément de désinformation a, en lui-même, peu de conséquences, mais le cumul des effets est parfois considérable.

17 Coercion. Cambridge Dictionary. (sans date) Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/coercion [traduction]

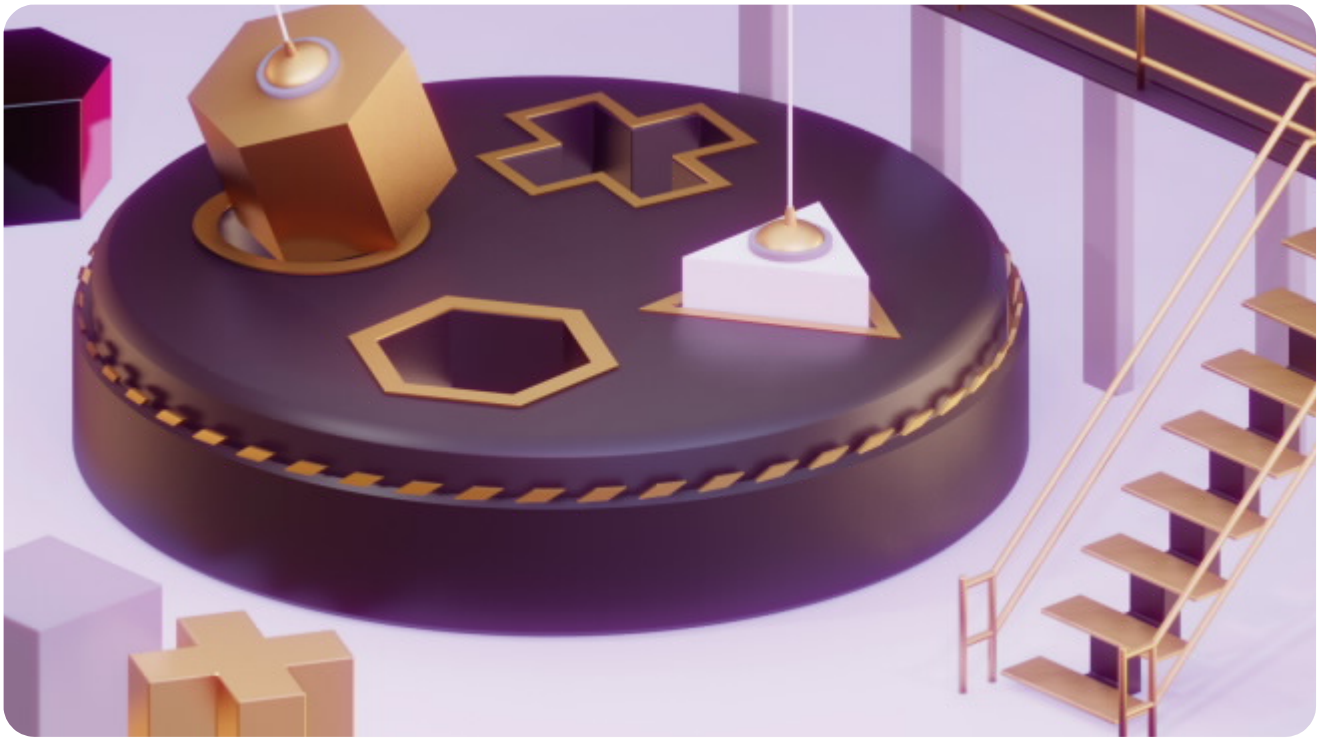
Autres lignes directrices sur l'élaboration de définitions

Les décideurs politiques, la société civile et le secteur privé devraient tous tenir compte de la portée des définitions qu'ils proposent.

La création de définitions trop étroites ou trop larges n'est pas sans risque. Une définition trop large risque de restreindre le comportement diplomatique acceptable en temps d'élection et gêner les pratiques gouvernementales légitimes. À l'opposé, des définitions trop étroites risquent d'exclure l'ingérence étrangère susceptible de prendre des formes très diverses et d'être induite par différents vecteurs de menace.

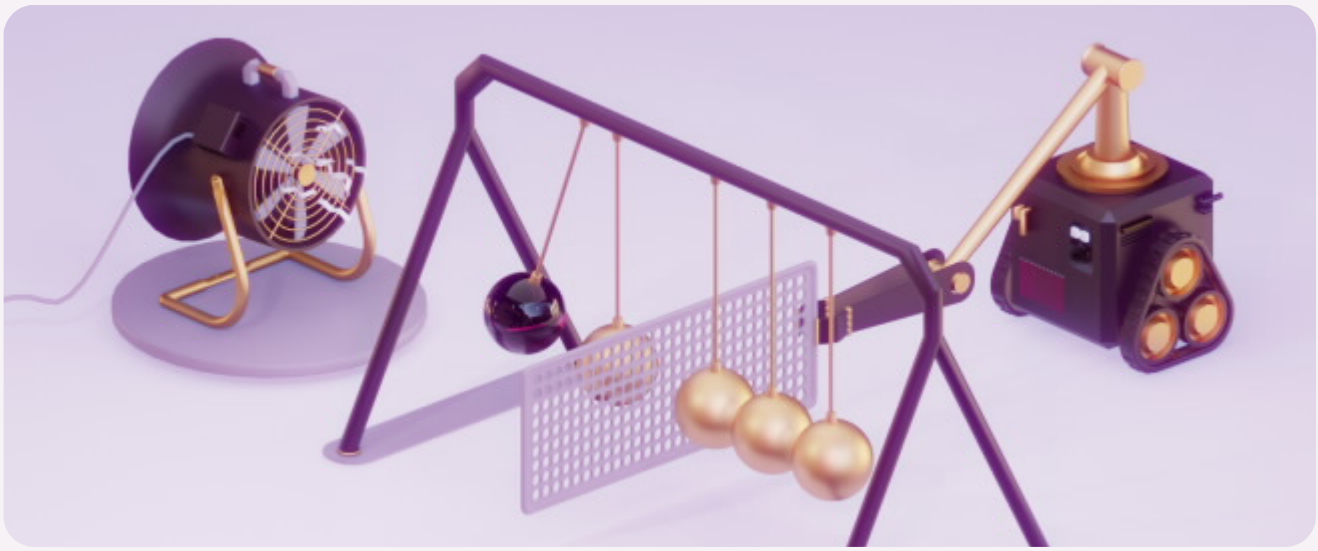
Par ailleurs, il convient de préciser si les définitions s'appliquent uniquement aux gouvernements (dans l'affirmative, préciser lesquels, p. ex. uniquement les démocraties) ou si elles s'appliquent à tous les intervenants. Si une définition large est suggérée, peut-elle être facilement appliquée par le gouvernement, la société civile et le secteur privé?

Il n'existe pas de définition universelle de l'ingérence étrangère. Le caractère « acceptable » ou « inacceptable » des comportements et des actions diffère selon qu'on adopte un point de vue juridique, éthique ou politique. La dimension politique d'un tel jugement est illustrée par le fait que l'identité des pays en question peut déterminer si un geste constitue ou non de l'ingérence. Les activités d'un adversaire peuvent être considérées comme de l'ingérence alors que les mêmes activités menées par un allié seront jugées acceptables. Une définition politique peut prendre l'acteur en considération, et être modifiée lorsque les politiques d'un adversaire changent. Les définitions politiques s'appliquent à une plus grande variété de menaces que les définitions qui ont trait au droit international. De plus, les définitions politiques peuvent être plus pratiques dans un environnement en constante évolution.



Atelier 2

Le défi : Distinguer l'ingérence étrangère de l'influence étrangère



Les démocraties sont confrontées au défi de distinguer l'influence étrangère acceptable de l'ingérence étrangère malveillante. Les sociétés dites ouvertes sont particulièrement vulnérables aux efforts clandestins, sournois et coercitifs des acteurs étrangers visant à saper l'intérêt national, y compris les institutions, les processus et les valeurs démocratiques. Les acteurs hostiles n'hésitent pas à exploiter cette zone grise entre l'influence et l'ingérence afin d'atteindre leurs objectifs géopolitiques.

Pour aborder le défi posé, il faut d'abord préciser l'objectif visé. S'agit-il de produire une définition universelle de l'influence étrangère acceptable, par opposition à l'ingérence étrangère inacceptable? Ou cherche-t-on plus précisément à déterminer ce qui constitue de l'ingérence étrangère exercée par des États autoritaires sur des démocraties libérales?

Si l'objectif est de produire une définition universelle, il faut d'abord se tourner vers le droit international. En droit international, l'interdiction d'intervenir dans les affaires internes d'un autre État constitue un principe de base, comme en témoignent la Charte des Nations Unies et de nombreux autres accords internationaux. Ce principe de large portée s'applique aux interventions par la force (p. ex., opération ou occupation militaire, annexion de territoire) de même qu'aux interventions qui ne font pas appel à la force. Il est clair que cette règle fondamentale doit continuer de s'appliquer à la lumière des nouvelles formes d'intrusion étrangère. Il est toutefois plus difficile d'appliquer ce principe à des scénarios donnés, et c'est pourquoi ces considérations retiennent l'attention des spécialistes du droit dans les milieux universitaires et gouvernementaux.

Si l'objectif est de déterminer ce qui constitue une ingérence étrangère inacceptable de la part d'un État autoritaire, il revient alors aux démocraties de préciser quels gestes posés par des États autoritaires – en particulier les rivaux stratégiques – sont acceptables ou inacceptables, tant sur le plan du droit que sur celui de la politique.

Trois éléments sont généralement pris en compte pour définir l'ingérence étrangère et la distinguer de l'influence étrangère : l'intention, la transparence et l'impact. Encore une fois, cela n'est pas simple.

Il est difficile de déterminer l'intention, en particulier celle qui motive une action donnée. Par exemple, comment présumer de l'intention d'un État qui interfère dans une élection? Est-ce que l'État tente de faire pencher l'élection en faveur d'un candidat, d'éroder la confiance du public dans la démocratie ou de précipiter une transformation dans l'ordre mondial? Il est également difficile de vérifier une intention lorsque des intermédiaires ou des acteurs involontaires sont en cause, comme c'est souvent le cas, ou lorsque les activités se déroulent dans un écosystème numérique transnational surchargé qui prévient leur attribution à un acteur précis.

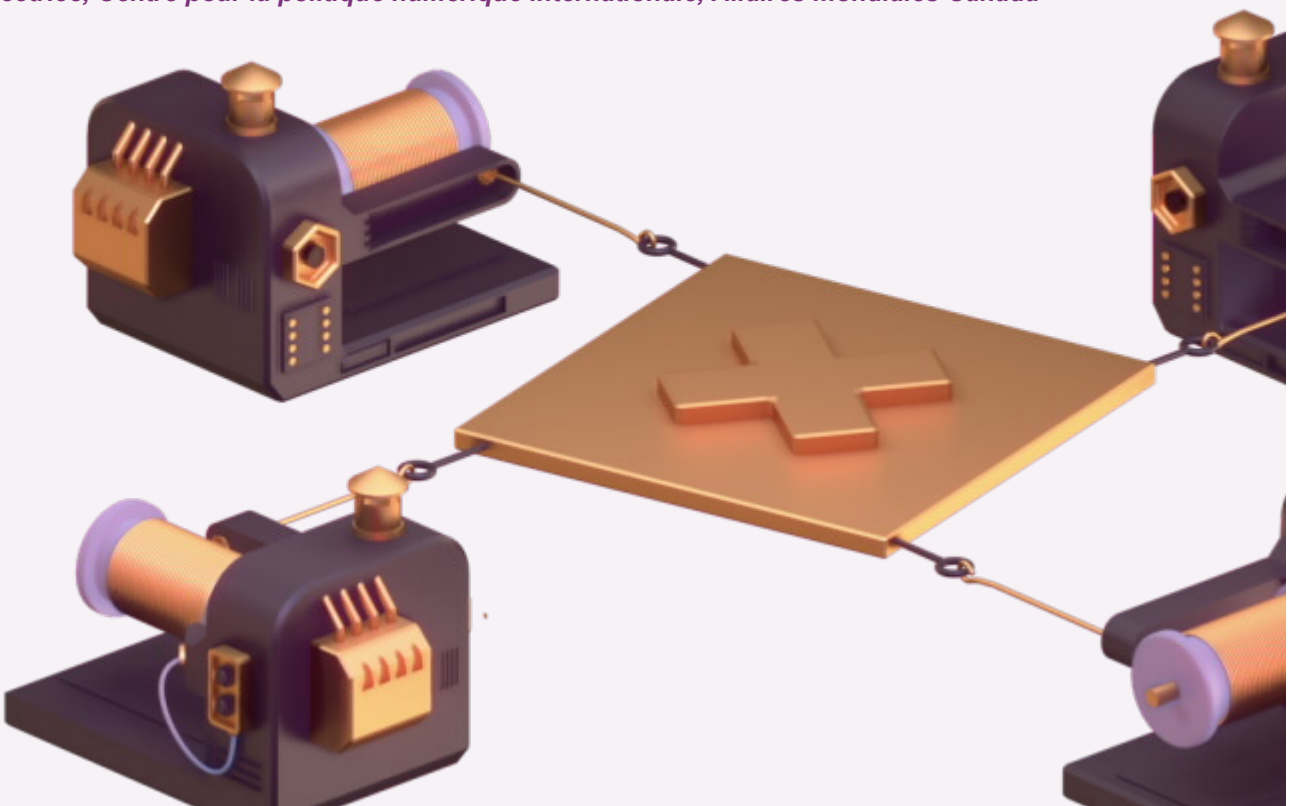
L'évaluation de la transparence pose également des problèmes. Les campagnes de désinformation étrangères clandestines sont répandues sur les plateformes de médias sociaux. Toutefois, on note d'innombrables exemples d'acteurs étatiques qui utilisent des moyens (p. ex., des médias contrôlés par l'État, des comptes de médias sociaux officiels) et des messages manifestes pour semer la confusion, provoquer la division et miner la confiance dans les gouvernements démocratiques, y compris dans le contexte de la pandémie de COVID-19.

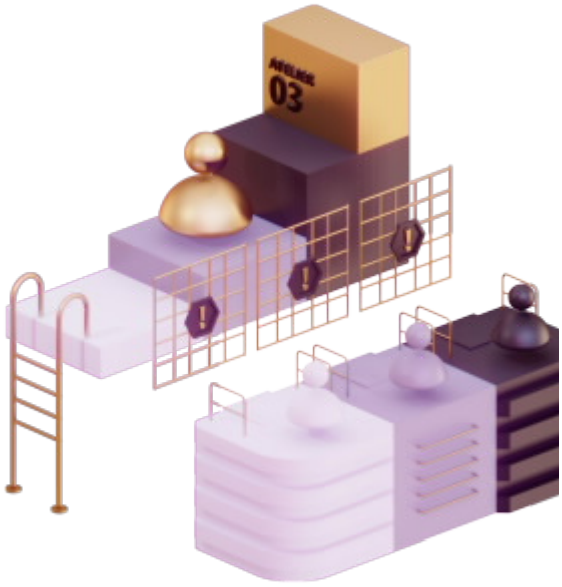
Il demeure également difficile d'évaluer l'impact de l'ingérence étrangère. Il arrive que des acteurs étatiques malveillants utilisent un éventail de tactiques couvrant de multiples vecteurs d'ingérence (p. ex., cybernétique, numérique, humaine) afin d'atteindre un objectif précis ou un ensemble d'objectifs. Dans ce scénario de « mort à petit feu », il est plus ou moins utile d'essayer d'évaluer l'impact d'un acte d'ingérence étrangère en particulier, car c'est plutôt la combinaison d'une pluralité d'actes qui visa à avoir un impact géopolitique.

Qui plus est, il est pratiquement impossible d'évaluer l'impact de certains types d'ingérence étrangère. Par exemple, comment évaluer l'impact d'une campagne de désinformation sur les résultats d'une élection compte tenu de l'environnement informationnel complexe et des intentions de vote? Des analyses poussées réalisées après de récentes élections n'ont pas permis de déterminer avec certitude si l'intervention étrangère avait influencé ou non les résultats ou si elle était la principale cause de la polarisation accrue.

Les partenaires démocratiques auront tout intérêt à accorder une attention accrue à cette zone grise entre l'ingérence étrangère et l'influence étrangère, afin de clarifier l'application du droit international, de définir les lignes rouges et de coordonner nos actions.

Gallit Dobner,
Directrice, Centre pour la politique numérique internationale, Affaires mondiales Canada





Atelier 3 : La COVID-19 – Contrer l'ingérence électorale dans un environnement pandémique

Lorsque les signataires de l'Appel de Paris se sont donné l'objectif de défendre les processus électoraux, ils ont mis l'accent sur la prévention de l'ingérence malveillante par des acteurs étrangers ayant pour but de miner les processus électoraux au moyen de cyberactivités hostiles. Moins d'un an plus tard, une pandémie mondiale venait perturber le cours de la vie et des processus démocratiques, y compris les élections. Ceux qui tentent de s'ingérer dans une élection cherchent à exploiter les vulnérabilités et les gouffres dans l'infrastructure électorale – ces composantes des constructions sociétales démocratiques où s'installent la confusion, le désaccord ou la peur. À l'échelle de la planète, la mésinformation et la désinformation au sujet de la COVID-19 ont surgi et pris d'assaut diverses plateformes d'information. Les fonctionnaires électoraux ont rapidement adapté leurs processus pour faciliter le vote en temps de pandémie, mais des préoccupations ont été soulevées selon lesquelles ces changements, combinés à l'information inexacte qui circulait sur la COVID-19, risquaient de semer la confusion chez l'électorat. Ces vulnérabilités ont ouvert la porte à l'ingérence électorale comme jamais auparavant. Les adversaires disposaient maintenant de divers moyens pour atteindre leurs objectifs, y compris des opérations d'information, des cyberattaques et des campagnes dans les médias sociaux. Aux États-Unis, les risques pour la sécurité physique et les défis constants sur les plans de la cybersécurité et de la désinformation ont influé sur la planification de l'élection de 2020 et posé des défis considérables à d'autres pays. Le troisième atelier portait sur la meilleure façon pour les démocraties de tenir une élection dans un environnement incertain. Il est important pour les intervenants qui participent à l'organisation d'une élection de se livrer à un exercice de planification d'urgence exhaustif. Ils doivent soigneusement décider quels changements apporter aux procédures de scrutin, déterminer si ces changements risquent de faciliter l'ingérence électorale et prévoir des mesures d'atténuation en conséquence.

À mesure que les démocraties s'adaptent pour soutenir le vote pendant la pandémie, elles doivent garder en tête certains principes directeurs. Les fonctionnaires électoraux doivent prévenir les risques de transmission de la COVID-19, garantir l'accessibilité du vote et assurer la mise en œuvre efficace des changements aux opérations, procédures et établissements de vote. Les électeurs ne devraient pas avoir à choisir entre leur santé et leur droit de vote. Ils voudront aussi savoir comment voter en toute sécurité. Dans ce contexte, toutes les options s'accompagnent de risques – qu'ils soient fondés sur la perception, l'information, la technologie ou une combinaison de ces facteurs – ouvrant de ce fait la voie à l'ingérence.

En ce qui concerne les options, il faut d'abord établir celles qui existent, puis explorer les risques qui y sont associés, toujours dans l'optique de protéger les processus, de promouvoir la sécurité et de préserver l'intégrité électorale.

Les options comprennent notamment les suivantes :

- Vote en personne
- Systèmes de vote portables (bureaux de scrutin installés sur le trottoir dans les lieux de vote réguliers ou dans des véhicules pouvant être déplacés d'un lieu de vote à un autre)
- Vote postal et boîte de réception pour les bulletins
- Vote électronique (Web, courriel, télécopieur)

Facteurs à considérer pour chacune de ces options :

- Quelles sont les faiblesses de chaque option? En quoi ces faiblesses ouvrent-elles la porte à l'ingérence?
- Quelles sont les forces de chaque option? En quoi ces forces protègent-elles contre l'ingérence? Comment communiquer les avantages à l'électorat pour prévenir les effets négatifs de l'ingérence?
- Quels sont les outils et les solutions qui devraient être mis en œuvre, mais qui ne le sont pas?

Pratiques efficaces

Bâtir la confiance

Il est important de bâtir une confiance durable dans nos OGE. Les gens devraient avoir confiance en la nature indépendante et non partisane de ces dernières. On peut y arriver, en partie, en rappelant aux électeurs que les fonctionnaires électoraux sont des membres de leur communauté (lorsqu'il est convenable de le faire). On ne devrait pas seulement travailler à établir la confiance lorsqu'une élection importante a lieu, mais plutôt s'y consacrer sur une période prolongée.

Fournir de l'information crédible

Il est essentiel de fournir de l'information fiable – de façon à « inoculer » le public – pour contrer les risques de mésinformation et de désinformation. L'un des défis clés consiste à dissiper l'incertitude générée par la COVID-19 (p. ex., sur la façon de voter, ainsi que le moment et l'endroit pour le faire), qui entraîne une baisse de la participation. Il est important de mobiliser les partenaires de confiance dans la communauté, de leur fournir de la formation, des outils et des ressources, ainsi que de promouvoir leur travail afin d'accroître l'impact, en particulier dans les communautés vulnérables, dont le nombre a augmenté en flèche en raison de la COVID-19.

Il faut aussi mettre au point des techniques robustes pour mesurer l'impact des efforts de lutte contre la désinformation, mais de plus amples recherches s'imposent d'abord. À l'heure actuelle, les approches suivantes s'avèrent utiles : déterminer le nombre de personnes qui ont été rejointes par les efforts visant à fournir de l'information fiable, et le nombre de fois qu'elles ont été contactées; mener des sondages pour évaluer l'opinion publique et suivre son évolution; sonder les organisations communautaires mobilisées; évaluer si les personnes qui avaient choisi de ne pas voter ont changé d'idée.

Protéger l'intégrité électorale

La technologie qui soutient et facilite le vote offre de nombreux avantages précieux – des registres de scrutin contenant de l'information sur chaque électeur aux appareils de vote (dans certaines circonscriptions), en passant par les machines qui compilent les résultats le soir de l'élection. Ces produits et solutions peuvent contribuer à protéger la qualité du processus électoral, dont la vulnérabilité particulière en temps de crise pourrait entraîner une baisse de la participation. Les gouvernements du monde entier devraient investir pour renforcer leur capacité technique à long terme, de manière à rester à l'affût des technologies courantes et de l'expertise requise pour l'exploiter, à se montrer proactifs et à réagir rapidement. La sécurité doit demeurer une priorité absolue : les pays doivent intégrer des dispositifs de sécurité à toute infrastructure qu'ils créent ou adaptent, et ils devraient investir dans la recherche et le développement pour mettre au point les systèmes les plus perfectionnés et robustes qui soient.

Fournir une technologie fiable

Lorsqu'employée, la technologie électorale ne devrait jamais être mise en œuvre à la hâte, de manière désordonnée ou en surface (comme « solution de fortune »). Son utilisation devrait également s'accompagner de règles claires, mais non trop contraignantes. De plus, la technologie électorale ne devrait pas réduire la participation en créant des inégalités ou en limitant l'accès; l'instauration de technologies électorales par les gouvernements ne devrait pas créer différentes classes de citoyens. L'accès et la sécurité devraient revêtir une importance égale. Par ailleurs, il faut absolument s'assurer que les défaillances technologiques ne soient pas perçues comme étant dues à la corruption et ne remettent pas en cause la légitimité des élections, en particulier lorsqu'il s'agit de scrutins dans des démocraties émergentes.

Processus et pouvoir de voter

Il faut comprendre que la méthode de vote influence qui exercera son droit de vote, ce qui influence à son tour l'identité de ceux et celles qui gouverneront.

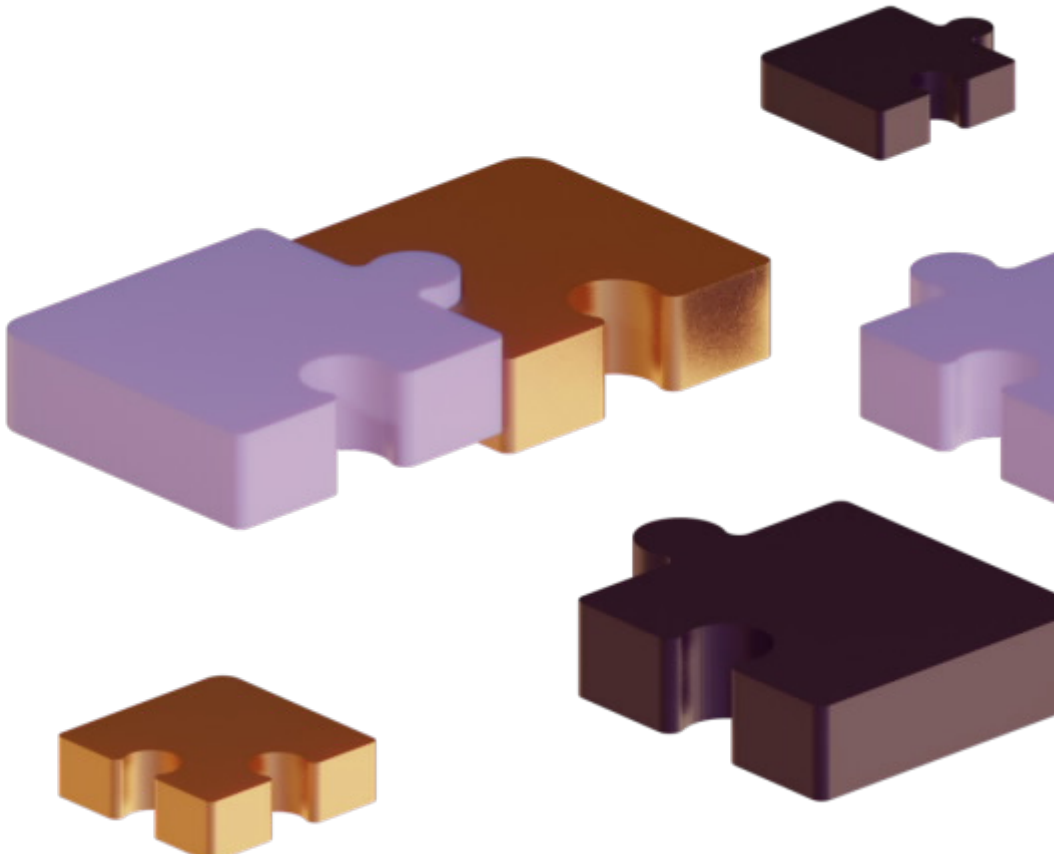
C'est pourquoi les gouvernements du monde entier devraient rechercher (et rechercheront probablement) des approches hybrides qui allient le vote en personne, le vote postal et le vote portable, pour garantir des taux de participation élevés.

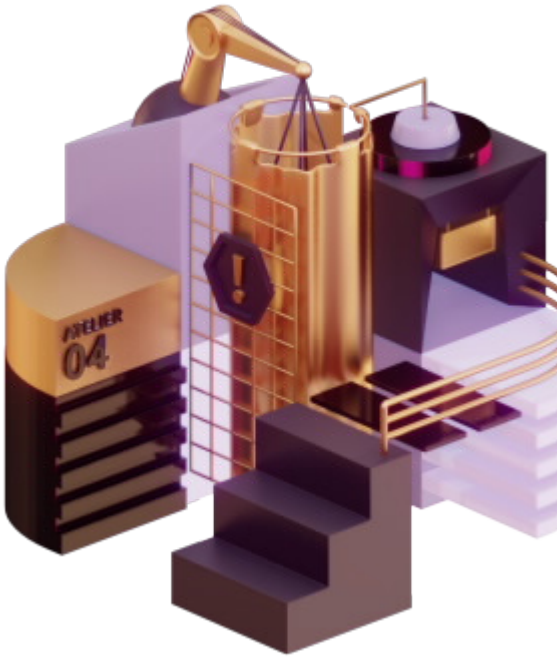
Personnalisez la solution

Chaque approche comporte ses avantages et ses risques. Pour décider de la façon d'organiser une élection dans un pays donné, y compris sur le plan de la technologie électorale (sans toutefois s'y limiter), il faut reconnaître que ce qui fonctionne dans un pays (p. ex., un plus petit pays comme l'Estonie) ne fonctionnera pas nécessairement dans un autre (p. ex., un vaste pays comme les États-Unis ou le Canada). Il peut même être nécessaire de varier les approches au sein d'un même pays pour tenir compte des plus petites régions, comme c'est le cas des différents comtés aux États-Unis. Dans le cadre de la planification des urgences, il faut produire un plan de communication détaillé et le mettre en œuvre rapidement, même s'il n'est pas parfait.

Il est également crucial d'avoir un « plan B ». Il faut comprendre que les fonctionnaires électoraux doivent composer avec des priorités concurrentielles en raison de la pandémie.

Il se pourrait donc que les questions de cybersécurité (qui existaient avant même la pandémie) soient reléguées au second plan. Il faut donc rappeler aux fonctionnaires électoraux l'importance d'aborder ces questions, malgré l'existence d'autres défis. Essentiellement, il faut encourager une collaboration étroite et l'échange de leçons apprises entre les gouvernements (au sein d'un même pays comme à l'échelle internationale), la société civile et l'industrie.





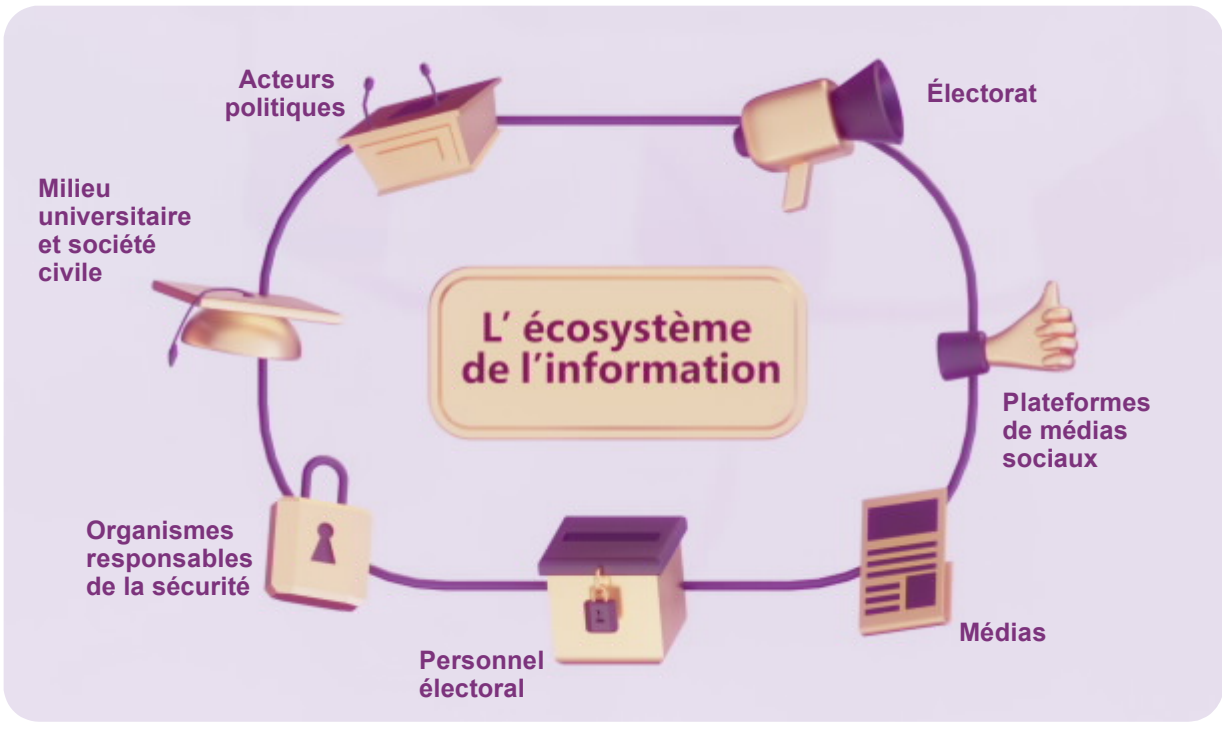
Atelier 4 : Ingérence dans l'environnement de l'information : Atténuation et réponse

D'une part, l'internet procure un accès à un flux d'information apparemment illimité. D'une autre, elle offre aux acteurs malveillants, nationaux et étrangers, de nouvelles possibilités pour miner la confiance dans les institutions démocratiques. Bon nombre de ces acteurs ont dirigé des campagnes de désinformation contre des démocraties en vue d'interférer dans des élections en semant le doute à l'égard des processus électoraux, en aggravant la polarisation sociétale et en employant un éventail de tactiques répréhensibles. Lorsqu'il s'agit de contrer la désinformation, il est d'autant plus difficile de distinguer entre les sources étrangères et nationales, ce qui ajoute à la complexité de la tâche.

La protection des institutions démocratiques, y compris les élections libres et justes, contre l'ingérence malveillante est une responsabilité partagée. Les gouvernements, les médias traditionnels, les plateformes de médias sociaux, le milieu universitaire et la société civile font tous partie d'un écosystème de l'information et jouent rôle fondamental dans la lutte contre l'ingérence électorale.

Le quatrième atelier a permis d'entendre des acteurs clés de l'écosystème de l'information – notamment des journalistes chevronnés – et était axé sur les enjeux que pose l'intervention (quand et comment) en cas d'ingérence électorale. En présence de désinformation, tout particulièrement, la réponse donnée à un incident peut aggraver une situation.

Au bout du compte, c'est la résilience citoyenne qui offre la meilleure protection contre ces actions hostiles. Les citoyens doivent disposer d'informations fiables pour tirer leurs propres conclusions, tenir les gouvernements et les individus responsables de leurs actes, et participer aux débats publics civils et pertinents.



Les médias et les journalistes

Selon le Reuters Institute Digital News Report de 2019, la confiance de la population dans les nouvelles s'est érodée au cours des dernières années, coïncidant avec une hausse du populisme et de la polarisation politique[18]. À la lumière de cette tendance, les journalistes cherchent sans cesse des moyens pour accroître et maintenir la confiance. Cette tâche peut s'avérer particulièrement ardue vu l'hyper-politisation de nombreux enjeux mondiaux d'importance, comme le changement climatique, la COVID-19 et la vaccination.

On peut bâtir et maintenir la confiance du public en faisant preuve d'impartialité, plus précisément en tenant compte des préjugés personnels et des écueils dans la présentation, la manipulation et l'omission d'information. Cependant, l'impartialité ne sous-entend pas que tous les enjeux ont deux côtes. Par exemple, en accordant trop d'espace au petit nombre de scientifiques qui jugent la vaccination dangereuse, on risque de donner l'impression qu'il existe des divergences d'opinions marquées sur la question, tandis qu'en réalité, la communauté scientifique y est massivement favorable. La population devrait donc avoir les faits à sa disposition pour être en mesure de tirer ses propres conclusions.

Les journalistes peuvent jouer un rôle dans la limitation de l'ingérence étrangère en se posant des questions fondamentales et en établissant un contexte pertinent. Ils devraient notamment se demander qui divulgue l'information, pourquoi et d'où elle vient. Ils devraient également évaluer de manière critique les motifs qui poussent l'auteur à divulguer une telle information. Ces questions pourraient les aider à déterminer si l'information est légitime ou si elle sert à manipuler les médias.

Qui plus est, il est essentiel de répondre rapidement en fournissant de l'information exacte, puisque la désinformation se développe dans le vide. En l'absence d'une telle réponse, les citoyens pourraient se tourner vers des sources d'information moins fiables, augmentant leur vulnérabilité à la désinformation et la mésinformation.

Lesplateformesde médiassociaux

Les plateformes de médias sociaux font face à leurs propres défis lorsque des acteurs malveillants utilisent les plateformes de médias sociaux pour s'ingérer dans des élections. Les entreprises de médias sociaux font face à des défis différents selon qu'il s'agit de répondre à des campagnes de désinformation étrangères ou nationales. Les préoccupations relatives à la liberté d'expression pourraient être atténuées par l'application de politiques régissant le comportement des membres d'une plateforme plutôt que le contenu qu'ils diffusent.

18 'Yellow Vest' Protesters Knock Wind out of French Business, Economy. Landauro, I., et R. Myriam (le 3 décembre 2018). Thomson Reuterswww.reuters.com/article/us-france-protests-economy-idUSKBN1O21IA
Par exemple, le niveau de confiance en France a chuté pour s'établir à 24 % après que les médias ont été critiqués pour leur couverture des manifestations des gilets jaunes.

Atelier 4

Partenariats collaboratifs

Le besoin de contrer la désinformation a amené des organisations médiatiques qui se faisaient traditionnellement concurrence à envisager de nouveaux partenariats. L'initiative CrossCheck est l'un des exemples les plus éminents de cette forme de partage radical.

En 2017, 37 salles de nouvelles de la France et du Royaume-Uni se sont associées pour vérifier les faits entourant la campagne électorale présidentielle en France. L'initiative a été lancée par First Draft, un groupe sans but lucratif financé par des organisations philanthropiques, des plateformes numériques et d'autres sources indépendantes. CrossCheck forme aujourd'hui une coalition internationale qui lutte contre la désinformation bien au-delà des campagnes électorales. Elle s'est d'ailleurs penchée sur la désinformation scientifique entourant la COVID-19 et elle offre de la formation aux journalistes sur les techniques de vérification collaborative des faits.

La hausse de la désinformation a encouragé de nombreuses organisations médiatiques à instaurer leurs propres équipes et programmes de vérification des faits. Au Canada, Radio-Canada, le radiodiffuseur public de langue française, et l'Agence France-Presse ont établi un partenariat avec Facebook pour discréditer l'information erronée durant les campagnes électorales et entre celles-ci. Des médias reconnus partagent également le fruit de leur vérification de faits durant les événements politiques spéciaux, comme le débat de chefs. Nombre d'entre eux sont membres de plus grandes associations, comme l'International Fact-Checking Network, dirigé par le Poynter Institute, un chef de file reconnu de l'éthique et du développement journalistiques. La nécessité de collaborer à des projets d'enquête internationaux de plus large échelle a poussé les journalistes à créer de nouveaux réseaux, comme l'International Consortium of Investigative Journalists, qui a fait la lumière sur des affaires comme le stratagème fiscal des Panama Papers.

De nouvelles formes de vérification collaborative des faits voient également le jour sur la scène locale et régionale. Ainsi, durant l'élection présidentielle de 2020 aux États-Unis, plus de cent médias appartenant au Colorado News Collaborative (COLab) ont mis en commun leurs ressources journalistiques et de vérification des faits. COLab a poussé la collaboration médiatique vers de nouveaux sommets. Ses salles de nouvelles affiliées se spécialisent dans les reportages locaux qui sont axés sur les solutions, et souvent inspirés des citoyens, et qui génèrent de nouvelles formes d'associations entre les journalistes et leurs communautés.

La lutte contre la désinformation va toutefois au-delà de la vérification des faits, qui demeure une mesure défensive. Il est désormais admis que le fait de bâtir la confiance et d'accroître la visibilité et la promotion du contenu journalistique crédible et reconnu est essentiel pour endiguer la propagation des fausses nouvelles.

La Journalism Trust Initiative (JTI), un effort conjoint de Reporters sans frontières, de l'Union européenne de radio-télévision, de l'Agence France-Presse et du Global Editors Network, fait partie de ces projets proactifs. Son but est de créer un système de certification pour les journalistes et les organisations médiatiques, qui se qualifient en remplissant un questionnaire sur leurs pratiques éditoriales, leurs normes journalistiques, ainsi que la structure et le financement de leur entreprise. Le processus de certification est administré par des organisations de normalisation comme l'AFNOR, en France, mais l'admissibilité des organes de presse à la certification est déterminée par des groupes de professionnels des médias.

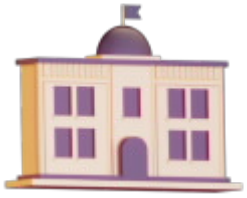
La JTI, qui est en phase pilote dans divers pays, y compris le Canada, peut également servir d'outil aux citoyens et aux organisations non médiatiques. Au bout du compte, les plateformes pourraient promouvoir le contenu certifié par la JTI. Des discussions sont en cours avec des associations internationales de publicité pour que les médias certifiés par la JTI aient un accès privilégié dans les espaces numériques sécurisés pour le placement des publicités. La JTI peut aussi servir d'étalon pour les entités philanthropiques privées et les ministères gouvernementaux qui offrent de l'aide financière aux organisations médiatiques.

Michel Cormier
Journalism Trust Initiative

Cette approche met l'accent sur les infractions fondées sur le comportement comme l'usurpation d'identité ainsi que l'utilisation de robots ou de comptes multiples pour amplifier le message. Elle permet de fermer des comptes et de supprimer leur contenu, tout en minimisant les risques de partisanerie perçue ou de poursuites pour violation de la liberté d'expression.

Plusieurs plateformes de médias sociaux publient des rapports et statistiques sur les violations à leurs politiques. En informant le public des campagnes d'ingérence électorale coordonnées dès qu'elles surviennent, les entreprises de médias sociaux contribuent à la santé de l'écosystème de l'information. S'ils sont plus au fait de l'ampleur des manipulations, les utilisateurs des plateformes pourraient voir d'un œil plus critique ce qu'ils lisent et y penser attentivement avant de transmettre de l'information qui semble peu crédible.

La collaboration et le partage d'information entre les plateformes de médias sociaux et les intervenants sont essentiels et exigent les efforts des gouvernements, du milieu universitaire, des journalistes d'enquête et des homologues de l'industrie. Les problèmes devraient être « de source ouverte » — déclarés et rendus publics — et être communiqués à des experts qui participeront à la conception de solutions. L'expertise des organisations non gouvernementales, des groupes de réflexion et d'autres organisations de la société civile peut fournir du contexte et améliorer la compréhension.



Le gouvernement

La défense de la démocratie et des institutions démocratiques est au cœur des responsabilités d'un gouvernement. Cela dit, il est risqué pour le gouvernement au pouvoir d'affirmer qu'il y a ingérence durant une élection. En plus de susciter des accusations de partisanerie, toute annonce d'ingérence pourrait influencer les résultats de l'élection. Elle pourrait aussi éroder la confiance du public dans l'élection et affecter sa perception quant à la légitimité des résultats.

Compte tenu de l'impact possible d'une intervention, il est essentiel pour les gouvernements de respecter un seuil d'intervention très élevé en période électorale, afin de préserver la confiance du public et la légitimité.

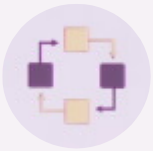
Les interventions ne devraient pas être fondées sur des règles rigides, mais plutôt sur des jugements nuancés.

Des décideurs expérimentés et non partisans devraient veiller à ce que les mesures soient prises en fonction des valeurs et des priorités du pays et de ses citoyens, ainsi que de l'influence qu'elles auront sur ces derniers. Il faudrait aussi considérer l'objectif de la communication, le type de menace informationnelle, le public cible, de même que le moment et l'endroit où l'incident s'est produit. Comme le démontre l'expérience du Canada avec le Protocole public en cas d'incident électoral majeur (voir l'encadré ci-dessous), il est nécessaire de compter sur des décideurs compétents, d'avoir un mandat clair et de pouvoir accéder à des renseignements non classifiés et classifiés en temps réel.

Une approche globale s'impose pour permettre au gouvernement, à l'industrie et à la société civile de collaborer dans la lutte contre l'ingérence étrangère. Cela permet de donner une voix aux personnes appropriées au sein du gouvernement, de l'industrie, des médias, du milieu universitaire et des groupes de réflexion. Cependant, les situations varieront d'un pays à l'autre, chacun étant confronté à différents incidents d'ingérence électorale. Puisque les processus juridiques, politiques et électoraux varient grandement, il ne peut y avoir une seule et unique approche.

Atelier 4

Protocole public du Canada en cas d'incident électoral majeur



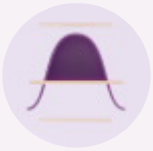
Le Protocole

Le Protocole public en cas d'incident électoral majeur est le mécanisme par lequel il aurait été possible de communiquer de manière claire, transparente et impartiale avec la population lors de l'élection générale de 2019 en cas d'incident menaçant l'intégrité de l'élection (p. ex., piratage d'un site Web du gouvernement, désinformation à grande échelle).

Le Protocole est fondé sur l'opinion voulant que toute annonce durant la campagne électorale susceptible d'avoir un impact sur l'élection doive provenir d'une source fiable et non partisane, c'est-à-dire dans le cas présent de hauts fonctionnaires.

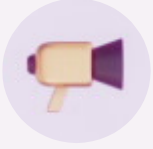
Le Comité

Le comité est formé de hauts fonctionnaires qui ont une expérience élargie de la sécurité nationale, des affaires étrangères, de la gouvernance démocratique et des perspectives juridiques, y compris une compréhension manifeste des droits démocratiques enchâssés dans la Charte canadienne des droits et libertés. Le comité s'est rencontré régulièrement durant la période électorale et a été tenu au courant de l'environnement de la menace sur une base continue.



Le Seuil

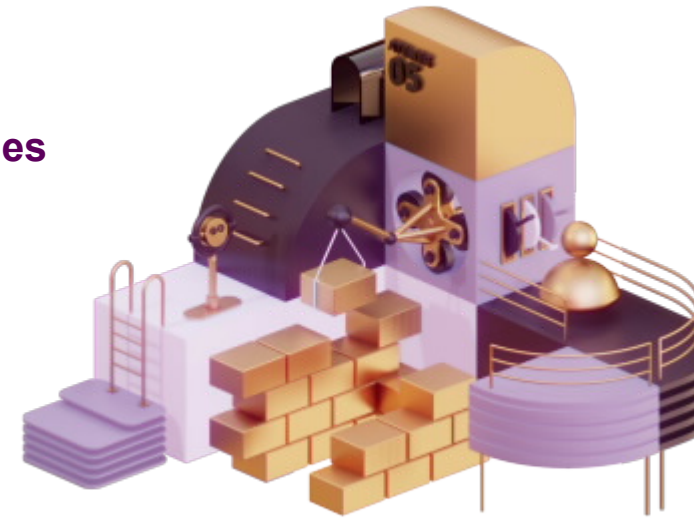
Le Protocole ne sert pas à arbitrer l'élection. Par conséquent, le seuil à atteindre avant de faire une annonce est très élevé et se limite aux circonstances exceptionnelles. Les considérations sont évaluées selon divers paramètres, y compris la portée et l'impact de l'incident. Le Protocole stipule que les incidents d'ingérence en cause sont ceux qui menacent l'intégrité d'une élection générale.



L'Annonce

La décision de faire une annonce publique doit susciter un consensus au sein du comité. En l'absence de considérations de sécurité nationale, les Canadiens sont informés de ce que l'on sait sur l'incident et des mesures qu'ils devraient prendre pour se protéger.

Atelier 5 : Défendre, détecter et récupérer : Contrer la menace d'ingérence dans les infrastructures électorales



La protection de l'infrastructure électorale est essentielle pour contrer l'ingérence étrangère au sein des processus démocratiques. La protection de l'infrastructure électorale va au-delà des événements qui surviennent le jour de l'élection. Des mesures cruciales doivent prises avant, pendant et après le jour du scrutin pour s'assurer que les systèmes électoraux sont protégés. Le cinquième atelier de la série destiné aux signataires de l'Appel de Paris était axé sur la délimitation de la gamme complète des infrastructures nécessaires aux élections, l'évaluation des vulnérabilités auxquelles elles font face et la proposition de solutions pour réduire ces vulnérabilités.

Infrastructure électorale et vulnérabilités clés

Les pays du monde entier mènent leurs élections différemment. Certains ont des systèmes basés sur le papier tandis que d'autres utilisent des machines à voter et d'autres outils numériques pour inscrire les électeurs, enregistrer les votes et compiler les résultats. Toutes les élections font désormais appel aux technologies et communications numériques, que ce soit pour la transmission des votes ou pour rapporter les résultats aux citoyens et aux organisations médiatiques. L'amélioration de l'infrastructure électorale nécessite d'abord une compréhension de la gamme d'infrastructures nécessaires aux processus électoraux, puis une évaluation soigneuse des risques auxquels elles font face.

Avant le jour du scrutin, plusieurs volets de l'infrastructure sont déjà utilisés, et chacun peut s'avérer vulnérable, notamment :

- **Les systèmes d'inscription en ligne des électeurs** peuvent faire l'objet de mystification par des malfaiteurs, qui créent une reproduction malveillante du site Web officiel pour saisir des renseignements sensibles ou donner aux électeurs l'impression que leurs renseignements ont été modifiés. Les coupures et refus de service ciblés pourraient empêcher l'inscription des électeurs.

- **Les systèmes de communication interne ou les comptes électoraux officiels de médias sociaux** peuvent être compromis par des malfaiteurs, qui utilisent des comptes légitimes provenant de ces systèmes pour envoyer de fausses informations, comme des dates électorales et des lieux de scrutin inexacts, aux fonctionnaires électoraux, au personnel des bureaux de scrutin, aux électeurs et à d'autres.

- **Les lieux d'entreposage** peuvent être vulnérables à l'altération physique ou à la destruction du matériel de scrutin par des acteurs malveillants.

L'attention et les ressources visant à protéger la sécurité de l'infrastructure électorale sont concentrées autour du jour de l'élection. Dans les pays comme les États-Unis, l'infrastructure électronique et numérique joue un rôle considérable dans le déroulement du scrutin. Dans d'autres, notamment l'Estonie et la Suisse, le vote a même eu lieu en ligne.

Dans des scénarios de scrutin plus traditionnel, les éléments d'infrastructure suivants sont une préoccupation majeure :

- **Les registres de scrutin électroniques (listes électroniques des électeurs)** pourraient être compromis par des malfaiteurs, qui pourraient y obtenir l'accès en utilisant une connexion sans fil ou en exploitant un appareil physique sécurisé de façon inadéquate. La compromission d'un registre de scrutin pourrait permettre aux électeurs de manipuler les listes électorales, en supprimant ou en modifiant les données d'inscription d'électeurs admissibles. Cela pourrait entraîner de la confusion pour ces électeurs le jour de l'élection.

- **Les systèmes d'inscription des électeurs** pourraient être bloqués. Les données et les copies de sécurité pourraient être chiffrées ou effacées à l'aide d'un logiciel rançonneur par des malfaiteurs jusqu'à ce qu'une rançon soit versée. Cela pourrait aussi causer le vol ou le chiffrement irréversible des bases de données d'inscription des électeurs et d'autres registres sensibles, causant de la perturbation aux activités électorales et le possible déclin de la confiance du public.

- **Les appareils de vote**, selon leur type, pourraient être vulnérables à l'altération physique à l'aide de médias amovibles ou à distance avec une connexion sans fil. Un appareil de vote pourrait permettre à un acteur malveillant de modifier un vote lors d'une élection.

- **La communication des résultats le soir de l'élection**, qui dépend aussi du flux d'information concernant les résultats de scrutin, est un élément crucial du processus électoral et comporte des éléments technologiques. La communication de résultats électoraux inexacts pourrait engendrer des tensions ou intensifier celles qui existent déjà.

Après l'élection, certaines vulnérabilités demeurent. Une attention doit être accordée aux systèmes de gestion électorale, aux sites Web officiels et aux processus de vérification.

- **Les systèmes de gestion électorale** pourraient être compromis par des logiciels commerciaux ou du matériel informatique qui comportent des faiblesses en matière de sécurité ou des erreurs de configuration dans les connexions du réseau. Une intrusion réussie pourrait conduire à la manipulation des résultats pendant la transmission électronique du total des votes.

- **Les sites Web officiels** pourraient être compromis par des malfaiteurs, qui peuvent reproduire des sites Web électoraux officiels et publier des résultats différents de ceux qui sont rapportés.

Pratiques efficaces

Pour protéger l'infrastructure électorale, il faut déployer des efforts soutenus tout au long du cycle électoral.

Certaines solutions réduisant la vulnérabilité s'appliquent à l'ensemble du cycle, tandis que d'autres sont pertinentes seulement à certaines étapes du processus électoral. Les solutions possibles ci-dessous s'inspirent des idées proposées par des participants à un atelier, qui proviennent des secteurs public et privé et de la société civile.

Bonnespratiquesgénérales

Le risque humain est présent tout au long du cycle électoral. Il est essentiel que toutes les personnes qui jouent un rôle dans une élection, tant les personnes qui l'organise que celles qui ont un emploi en lien avec cette élection (comme les médias la couvrant ou les partis politiques et les candidats), de pratiquer une bonne cyberhygiène.

Lesfournisseursde ressourceshumaineset matérielles jouant un rôle dans les élections peuvent présenter des points faibles. Les OGE et les institutions et fournisseurs connexes doivent veiller à ce que des protections adéquatessoient misesen place pour évaluer soigneusementle personnel et l'équipement.

Par exemple, le personnel électoral est souvent embauché temporairement, et il se peut que le processus d'évaluation du personnel ne soit pas assezrigoureux sur le plan de la sécurité. Des vérifications des antécédents plus approfondies réduiraient les risques. De même, les fournisseurs (ceux qui produisent et gèrent les machines à voter), les systèmes de gestion des élections et d'autres équipements, devraient faire l'objet d'une surveillanceétroite. Un mécanisme de certification pourrait être mis en place pour exiger des fournisseurs qu'ils démontrent qu'ils appliquent de bonnes pratiques de cybersécurité.

Pratiques efficaces en matière de cybersécurité

Maintenir la cybersécurité est un processus continu.

Il est important de comprendre que la réaction aux incidents (intervenir lors d'incidents de cybersécurité au sein d'un système technique) s'apparente à un « cycle de vie » qui doit être au cœur de la posture actuelle en matière de sécurité du système; et cette posture doit être continuellement améliorée grâce aux enseignements tirés. Une détection et une réaction rapides sont essentielles.

Voici quelques conseils en matière de cybersécurité :

- Observerles métadonnées, comme l'emplacement d'une cyberactivité donnée, qui peuvent faciliter la détection de comportements suspects.

- Utiliser de « conteneurs », c'est-à-dire des mécanismes qui permettraient aux individus d'ouvrir des pièces jointes potentiellement dommageables sans subir aucun dommage.

- Les infractions peuvent être décelées en vérifiant si des personnes au sein d'une organisation téléchargent des documents et les impriment, ainsi qu'en examinant les boîtes aux lettres électroniques pour vérifier s'il y a eu transfert externe.

- Pour les personnes participant aux processus électoraux, il est important de vérifier qui a accès aux boîtes aux lettres et de confirmer que la fonction d'audit est activée. Les acteurs malveillants la désactivent souvent.

Lesdécideurs politiques devraient permettre aux entreprises ayant une expertise en matière de cybersécurité de répondre aux besoins de cybersécurité des campagnes électorales si l'objectif de ces entreprises est de soutenir l'intégrité électorale. Aux États-Unis, cette pratique satisfait aux directives de la Commission électorale fédérale américaine. Ce type de soutien est essentiel, car les campagnes n'ont souvent pas l'expertise ou la capacité de traiter les questions de cybersécurité, ce qui met en péril l'intégrité électorale.

Pratiques efficaces en matière de systèmes d'inscription des électeurs

Pour protéger les systèmes d'inscription des électeurs, les OGE doivent disposer de robustes mécanismes de sauvegardes robustes. Les responsables devraient songer à mettre en place des sauvegardes cryptées, y compris des sites miroirs externes, ainsi que des sauvegardes sur papier.

Pour atténuer les failles inhérentes au personnel, les personnes travaillant sur les systèmes d'inscription des électeurs ne devraient avoir que les droits d'accès qui leur sont indispensables pour accomplir leur tâche. Le principe du droit d'accès minimal est essentiel. De même, les rôles des utilisateurs devraient être isolés au sein d'un système.

Enfin, il est important que les informations qui peuvent conduire à l'effacement des sauvegardes soient extrêmement sécurisées, car elles ont été la cible d'attaques de la part d'acteurs hostiles.

Pratiques efficaces en matière de registres de scrutin et des machines à voter

Les administrateurs électoraux devraient envisager d'utiliser des registres de scrutin électroniques tout en prenant des mesures pour atténuer les risques qu'ils créent. Parmi les avantages des registres de scrutin électroniques, citons un vote plus rapide et une synchronisation en temps réel avec d'autres registres de scrutin et avec les bases de données d'inscription des électeurs. Cela permet de consigner de manière fiable qu'un électeur s'est inscrit, a déposé un bulletin de vote et n'a pas voté plus d'une fois. Cependant, les registres de scrutin électroniques tombent souvent en panne, ce qui peut retarder le processus de vote, comme ce fut le cas lors de l'élection primaire dans le comté de Los Angeles en 2020.

Les cyberattaques représentent aussi une menace pour les registres de scrutin électroniques. En effet, il est possible qu'une cyberattaque modifie les informations figurant dans un registre de scrutin. Pour se prémunir contre ces risques, les responsables politiques devraient exiger des administrateurs électoraux qu'ils stockent de grandes quantités de matériel de secours, comme des cahiers de scrutin et des enveloppes pouvant permettre aux électeurs de voter provisoirement.

Des mesures de sauvegarde similaires sont également efficaces pour les machines à voter, car le stockage de grandes quantités de bulletins de vote papier peut être utile en cas de piratage des machines de vote.

Pratiques efficaces en matière de communications

Si l'infrastructure électorale a été piratée, les fonctionnaires électoraux doivent communiquer judicieusement avec toutes les parties concernées, y compris les électeurs et le grand public. Il est important de faire part de ce qui s'est passé, des dommages causés (par exemple, certaines intrusions n'entraînent pas de modifications des données) et de signaler où le public peut obtenir des informations précises.

Pratiques efficaces en matière d'audits et d'autres mesures de renforcement de la confiance

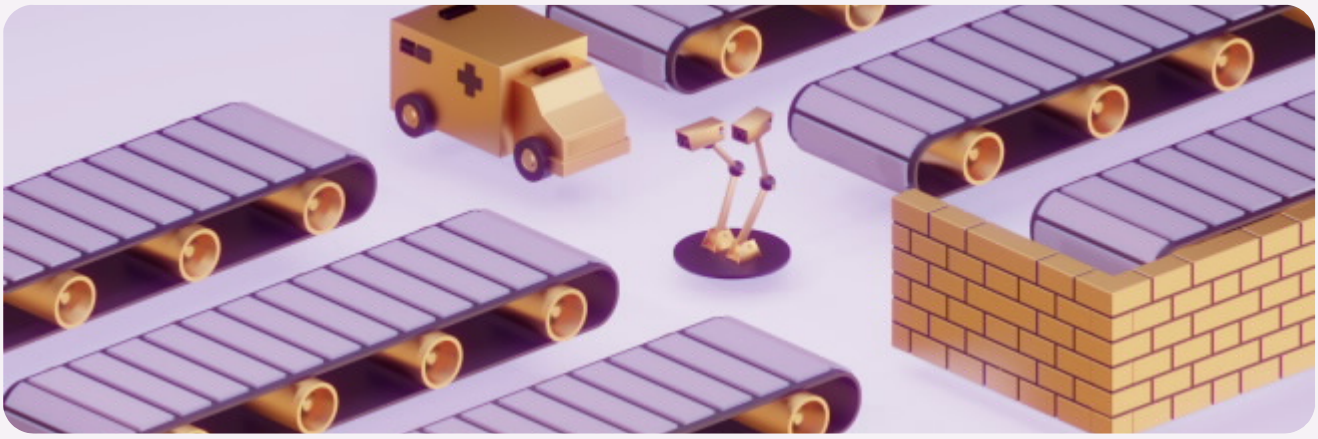
Les audits postélectoraux sont importants pour renforcer la confiance dans les résultats des élections. Les audits limitant les risques (ALR) offrent des avantages par rapport aux audits traditionnels. Ils sont plus efficaces : ils sont dynamiques, ils sont basés sur des échantillons et des audits, et ils ne confirment que le résultat de l'élection, et non la marge par laquelle le vainqueur a gagné.

D'autres mesures pouvant renforcer la confiance devraient être envisagées, notamment :

- Permettre au public de vérifier par lui-même que le dépouillement a été effectué correctement;
- Renseigner le public sur tous les aspects du processus de vote (surtout compte tenu des changements liés à la COVID-19);
- Améliorer la coopération entre tous les intervenants gouvernementaux et non gouvernementaux, et les intervenants au sein du gouvernement fédéral, étatique et local. Aux États-Unis, par exemple, ce processus a été facilité par la désignation de l'infrastructure électorale comme « infrastructure critique ».

Atelier 5

Protéger l'infrastructure électorale : Défendre, détecter et récupérer



- La prévention de l'ingérence malveillante par des acteurs étrangers visant à miner les processus électoraux par le biais de cyberactivités hostiles se résume largement à trois choses : défense, détection et récupération. Malheureusement, comme il n'existe aucun moyen de sécuriser entièrement une élection contre les acteurs malintentionnés, il faut s'assurer que le système électoral est assez résilient pour résister à une attaque.

- La défense d'un système électoral contre des acteurs étrangers exige des ressources suffisantes en matière de cybersécurité. Pour cela, il faut avoir assez d'employés capables de comprendre la menace de l'ingérence étrangère, détecter les vulnérabilités, faire des recommandations pour atténuer les vulnérabilités, mettre en œuvre ces recommandations et être en mesure de se remettre de tout compromis. Il faut également assurer une formation continue sur les meilleurs moyens de protéger les systèmes électoraux des cyberactivités et des stratégies malveillantes afin de communiquer rapidement les menaces et les incidents cybernétiques qui surviennent.

- La détection des problèmes potentiels au sein des systèmes électoraux nécessite de cartographier toutes les vulnérabilités possibles et de mettre sur pied des processus pour repérer les problèmes qui pourraient survenir si une vulnérabilité était exploitée. Par exemple, de robustes vérifications postélectorales, comme des vérifications de limitation des risques, contribuent à s'assurer que l'équipement de scrutin et les procédures de dépouillement des votes fonctionnent correctement et que l'élection produit un résultat exact.

- Finalement, pour chaque vulnérabilité détectée, il est important d'envisager ce qui pourrait arriver si la vulnérabilité était exploitée et de se préparer à prendre le meilleur moyen pour s'en remettre. Par exemple, si un appareil de vote par lecture optique tombe en panne, les fonctionnaires électoraux devraient avoir des procédures en place pour s'assurer que les électeurs peuvent continuer à voter.

David Levine
Intégrité des élections, Alliance for Securing Democracy

Atelier 5

Menaces et mesures de résilience concernant le vote le jour du scrutin aux États-Unis

Base de données d'inscription des électeurs et registres de scrutin électroniques

Les bases de données d'inscription contiennent les listes des électeurs inscrits et les renseignements d'identification qui déterminent à quelles courses un électeur peut voter. Elles contiennent les données qui sont utilisées pour produire les registres de scrutin pour le vote du jour de l'élection. Les registres de scrutin contiennent les listes électorales pour un bureau de scrutin donné et servent à vérifier l'admissibilité des électeurs qui viennent voter. Les registres de scrutin électroniques sont tout simplement une version électronique de ceux-ci, souvent sur une tablette comme un iPad.

Menaces

Des agents du gouvernement russe ont ciblé les bases de données d'inscription des électeurs aux États-Unis en 2016[19], rehaussant l'inquiétude selon laquelle l'accès aux bases de données et aux registres de scrutin électroniques ainsi que leur intégrité pouvaient être compromis, que ce soit par des malfaiteurs ou en raison d'erreurs survenant pendant le transfert des données et la mise à jour des logiciels. Une compromission pourrait entraîner la suppression d'électeurs dans une base de données ou un registre de scrutin, le cryptage des données par le biais d'un logiciel rançonneur, des informations inexactes quant aux électeurs qui ont demandé ou renvoyé des bulletins de vote d'électeurs absents, ainsi que des informations inexactes à savoir si les électeurs ont déjà voté. Cela pourrait causer de la confusion si on affirme aux électeurs qui se présentent le jour de l'élection qu'ils ne sont pas sur la liste des électeurs admissibles, qu'ils ont déjà voté ou qu'ils ont demandé un bulletin de vote d'électeur absent.

Mesures de résilience mises en œuvre par de nombreux fonctionnaires électoraux nationaux et locaux avant novembre 2020

- Faire une copie de sauvegarde des bases de données
- Laisser une copie de sauvegarde des registres de scrutin sur papier dans tous les bureaux de vote
- Conserver beaucoup de documents de vote provisoires à portée de main dans chaque bureau de vote

Instrumentsde vote

Les instruments de vote aux États-Unis incluent des scanneurs dans lesquels les électeurs placent leur bulletin de vote en papier pour la compilation, des appareils d'enregistrement électronique direct (DRE) sur lesquels les électeurs effectuent leurs sélections et qui enregistrent et compilent directement les choix, ainsi que des dispositifs servant à marquer les bulletins de vote (BMD) sur lesquels les électeurs effectuent leurs sélections, qui sont ensuite imprimés sur un bulletin papier et sont ultimement déposés.

19 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, no 116-290, vol. 1, p. 6. Select Committee On Intelligence (2020). **https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf**
*Exemple d'agents du gouvernement russe ciblant l'inscription des électeurs.

Menaces

Selon l'appareil, celui-ci pourrait être vulnérable à l'altération physique à l'aide de médias amovibles ou à distance avec une connexion sans fil. Il pourrait également être vulnérable aux erreurs de programmation. La compromission d'un instrument de vote pourrait permettre à un acteur malveillant de modifier un vote pendant une élection ou de rendre un appareil inutilisable, engendrant de longues files.

Mesures de résilience mises en œuvre par de nombreux fonctionnaires électoraux nationaux et locaux avant novembre 2020 :

- Vérification des compilations, en particulier des vérifications de limitation des risques
- Bulletins d'urgence en papier dans tous les bureaux de vote

Discussions : Les élections américaines sont-elles résilientes face aux menaces intérieures?

La décentralisation de l'administration électorale peut être une forme de résilience. La portée des dommages qu'une personne peut faire grâce un « travail interne » est limitée à une seule administration, habituellement un comté ou une municipalité. Toutefois, les fournisseurs électoraux ne sont pas aussi décentralisés que les administrateurs électoraux, puisqu'il n'existe que quelques fournisseurs principaux d'appareils de vote et d'autres formes d'infrastructure électorale aux États-Unis. Une façon d'améliorer ce domaine constituerait à certifier les fournisseurs qui suivent les bonnes pratiques en matière de cybersécurité et de personnel afin de contrer les menaces venant de l'intérieur.

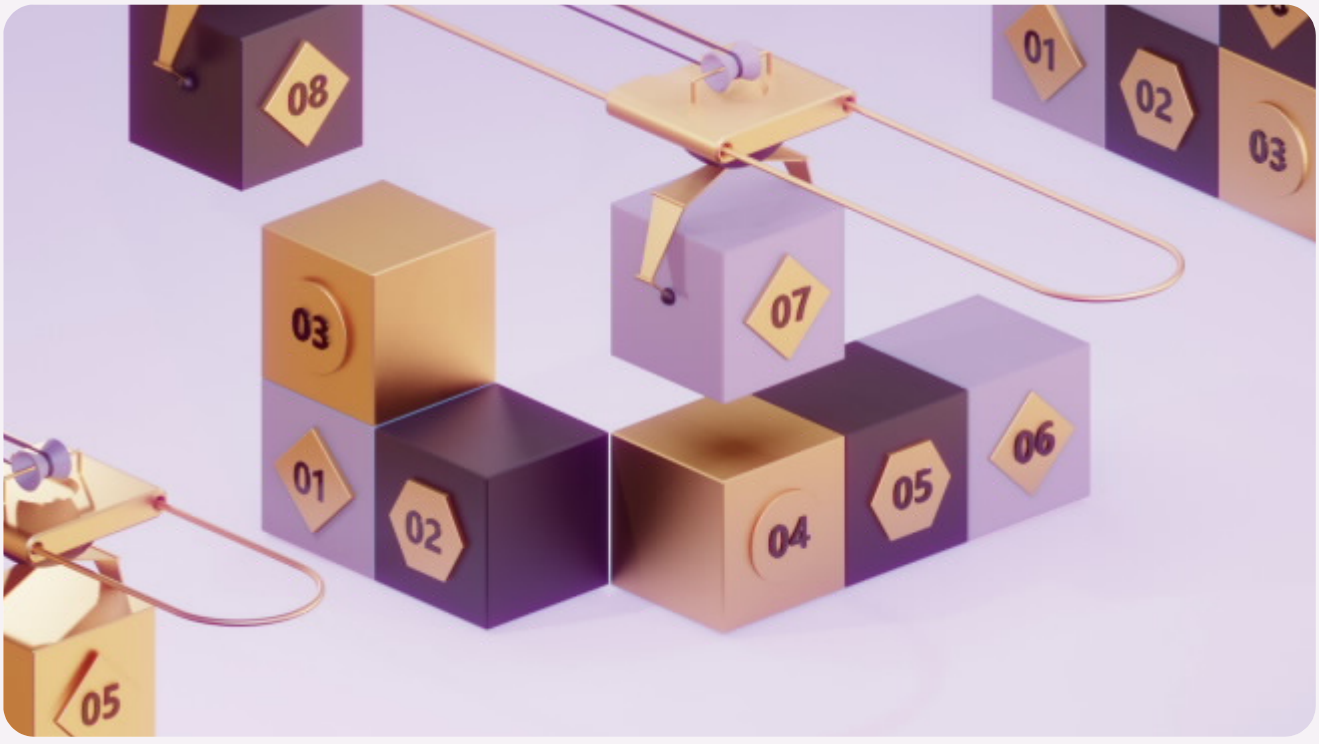
Gowri Ramachandran
Avocate-conseil – Démocratie, Brennan Center for Justice

Workshop 5

10 pratiques exemplaires qui s'appliquent à toutes les administrations chargées de tenir des élections

1. Créer une culture de sécurité proactive.
2. Traiter les élections comme un système interconnecté.
3. Tenir un registre des votes sur papier.
4. Utiliser des audits pour faire preuve de transparence et maintenir la confiance dans le processus électoral.
5. Mettre en place des mots de passe complexes et une authentification à deux facteurs.
6. Contrôler et gérer activement l'accès.
7. Prioriser et isoler les données et les systèmes sensibles.
8. Contrôler, enregistrer et sauvegarder les données.
9. Exiger des fournisseurs qu'ils fassent de la sécurité une priorité.
10. Accroître la confiance du public et se préparer aux opérations d'information.

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

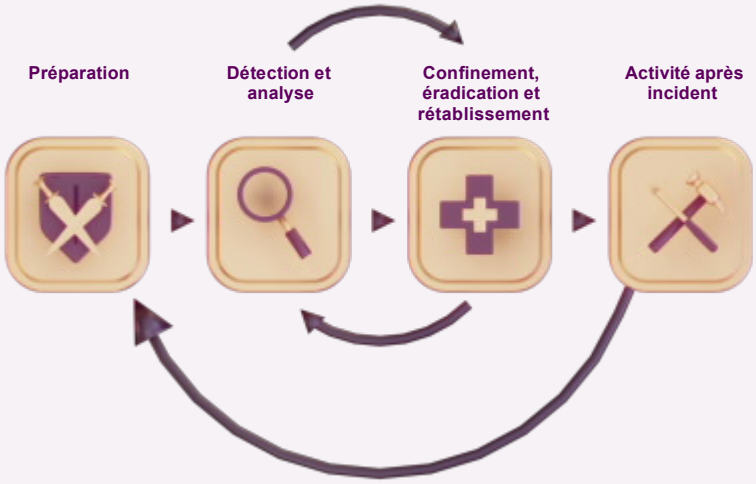


Atelier 5

Cybersécuritéproactive et réactive

L'identité est essentielle pour le fonctionnement interne d'une entreprise. Elle détermine à quoi les utilisateurs peuvent se connecter, permet la communication d'informations opérationnelles sensibles et protège l'environnement des acteurs externes. Cependant, c'est exactement la raison pour laquelle il s'agit d'une cible privilégiée pour les pirates. Une fois qu'un compte utilisateur a été compromis, un cyberpirate peut l'utiliser pour télécharger des boîtes de réception de courriels, se déplacer latéralement vers d'autres appareils du réseau, ou même vendre les identifiants en ligne pour réaliser un profit.

L'intervention en cas d'incidents ne se limite pas à la détection de ces événements et à la réparation des dommages. Microsoft voit le processus comme un cycle de vie continu où les connaissances sont réintégrées dans la chaîne pour que les gens en tirent des enseignements et évoluent. Chaque événement qui se produit dans un environnement crée une occasion de comprendre ce qui est « normal » et ce qui est « suspect ». Dans les meilleures stratégies d'intervention en cas d'incidents, on utilise ces données au fil du temps pour fournir une image complète d'une organisation.



Préparation

Quels outils et systèmes sont actuellement utilisés pour se préparer en cas d'incident? Ils peuvent inclure des logiciels qui protègent les utilisateurs et les mesures qui seront prises si un incident est décelé. Avoir une stratégie pour gérer un incident permettra de réagir plus rapidement et d'atténuer les dommages.

Outils:

- **Application Guard** pour les téléchargements conteneurisés afin de protéger les appareils contre les logiciels rançonneurs et autres fichiers malveillants.
- **O365 ImpersonationProtection** pour la sécurité des courriels contre les campagnes d'hameçonnage. Souvent, c'est d'abord au moyen de ces campagnes que les pirates accèdent à un système.

Processus:

- Établir une **configuration de base en matière de sécurité**, c'est-à-dire, déterminer qui a accès à quoi, quels systèmes peuvent accéder à d'autres, qu'est-ce qui est considéré comme sensible et quelles activités sont autorisées par ces systèmes.
- Mettre en œuvre la règle du droit d'accès minimal pour les comptes. Il est facile pour un pirate de deviner des mots de passe ou d'hameçonner un utilisateur. Mais si cet utilisateur ne peut pas fournir de valeur supplémentaire à un pirate, les dommages causés sont minimes malgré l'intrusion du pirate. Les niveaux d'accès et les utilisateurs/systèmes qui peuvent avoir un accès privilégié doivent être définis et considérés comme une norme.
- Authentification multifactorielle (AMF) pour tous les utilisateurs.
- Ne pas activer les boîtes aux lettres pour les rôles assortis de droits d'accès (administrateur de système, administrateur de base de données).
- Désactiver les anciennes méthodes d'authentification.
- Surveiller les dépôts de code pour les secrets de l'organisation et les clés d'interfaces de programmation (API). Il arrive souvent que des personnes utilisent accidentellement un code qui n'est pas sûr pour le stockage public. Les pirates informatiques parcourront GitHub et d'autres sources pour obtenir ces informations afin d'accéder à l'environnement.
- Maintenir à jour les systèmes destinés au public. Les pirates exploreront les appareils d'une organisation qui sont accessibles au public pour trouver des informations sur les versions des logiciels. Si un pirate voit qu'un serveur Web exécute une version vulnérable d'Apache, il peut utiliser des trousses d'exploitation publiées pour s'introduire facilement.

Détection et analyse

Il faut savoir ce qui est considéré comme « normal » dans l'environnement.

Établir des connaissances sur ce qui est attendu facilite la détection d'événements qui ne s'inscrivent pas dans un processus opérationnel habituel. Où pourrait se trouver les failles potentielles sur le plan de la sécurité? La stratégie de renforcement de la sécurité de toute organisation aura des failles, mais s'il y a des failles non décelées sur le plan de la sécurité, elles risquent d'être exploitées.

Outils:

- Utiliser des programmes comme **Degré de sécurisation Microsoft** pour connaître les recommandations relatives à l'environnement ainsi que la posture en matière de sécurité du groupe.
- Tirer parti d'applications, comme Power BI pour consulter les **données de connexion** afin de créer une image de l'endroit et de la manière dont les gens se connectent normalement.
- **Surveiller les applications** avec lesquelles les utilisateurs interagissent sur le plan de la programmation au moyen d'applications, comme Microsoft Cloud App Security afin de repérer les applications potentiellement suspectes.
- Créer des alertes pour informer les administrateurs du système de tout changement touchant les activités. Par exemple, une alerte pourrait être déclenchée si un fichier téléchargé est assorti d'un code de hachage qui n'a pas été vu auparavant dans l'environnement.

Confinement et éradication

Au cours d'une enquête, il y a itération entre la détection et le confinement à mesure que de nouveaux indicateurs de compromis apparaissent. Par exemple, si dans l'analyse des journaux d'ouverture de session, il y a une connexion suspecte à un seul appareil, il est possible de « pivoter » pour rechercher l'activité sur tous les appareils utilisant cette adresse IP. Cela pourrait élargir le champ des appareils compromis qui devront être corrigés, mais garder cela en tête permettra d'avoir l'esprit plus tranquille et ne rien manquer à l'avenir.

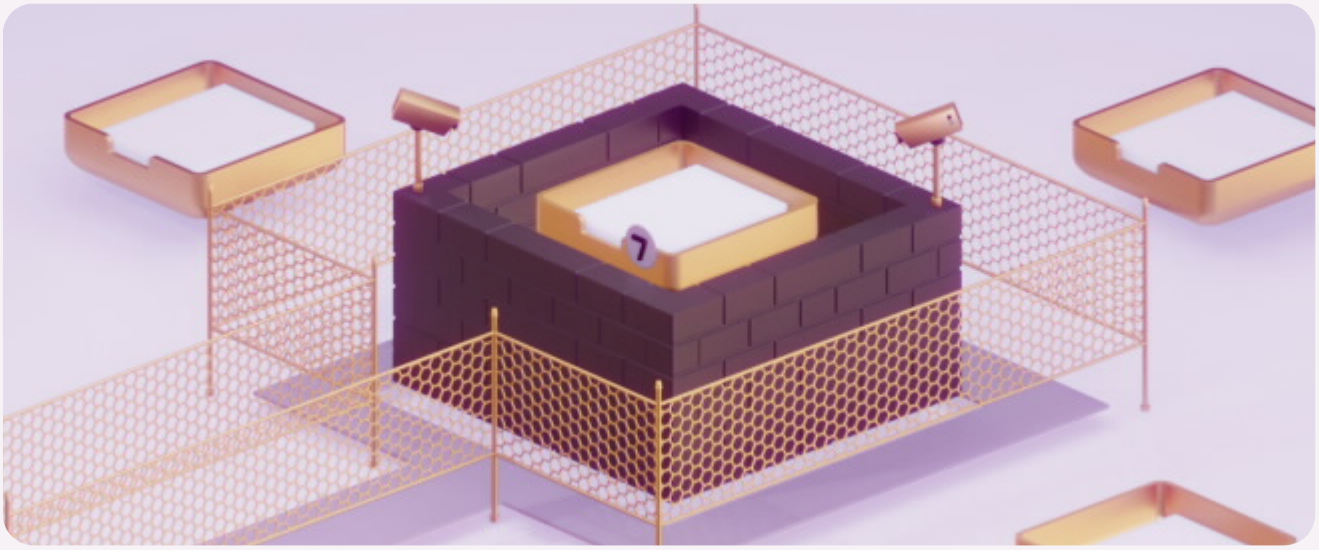
Outils:

- Utiliser des filtres spécialisés, comme la **réponse automatisée aux incidents dans Office 365** qui analysent de façon automatisée les courriels suspects et les retirent des boîtes aux lettres avant que le destinataire puisse les ouvrir.

Activité après incident

Noter les leçons apprises et revenir à l'étape de préparation afin de déterminer les mesures à prendre pour être prêt la prochaine fois

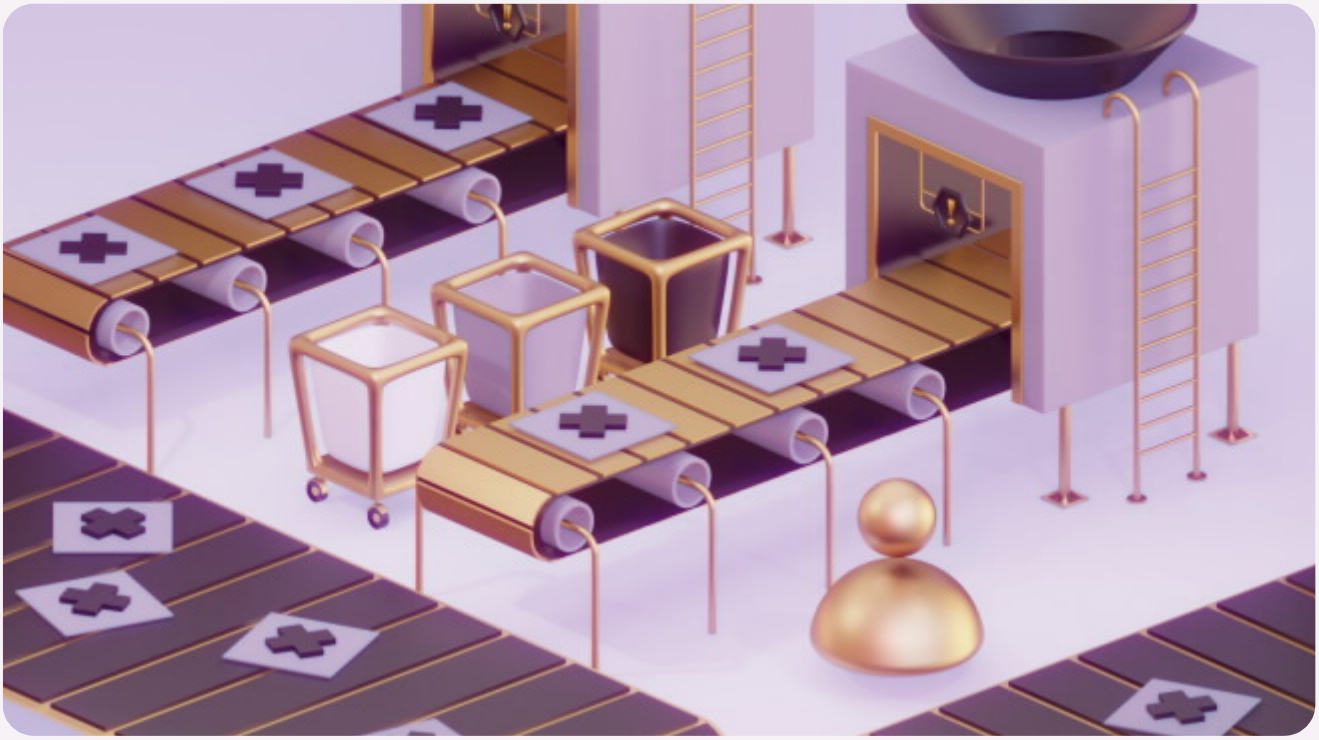
Si le pirate s'est introduit au moyen d'un courriel, quels outils permettraient de sécuriser la boîte de réception d'un utilisateur? C'est le moment de poser des questions sur ce qui a fonctionné et ce qui n'a pas fonctionné et d'actualiser la stratégie en conséquence.



Drew Robinson,
Équipe de détection et d'intervention de Microsoft

Atelier 5

Lesbasesdu protocole d'audit limitant lesrisques



Un bon audit est essentiel pour renforcer la confiance dans l'intégrité des élections. Plusieurs types d'audit peuvent être faits.

- Audits de conformité : dans le cadre de ces derniers, on inspecte les processus et les équipements électoraux afin d'évaluer les procédures utilisées lors de la tenue de l'élection.
- Audits administratifs : ils sont menés par les administrateurs électoraux – il s'agit idéalement d'audits publics – pour vérifier les bulletins de vote papier par rapport au dépouillement à la machine afin d'établir la confiance dans l'exactitude de ce type de dépouillement.
- Audits publics : ils permettent aux électeurs de vérifier directement que leurs votes ont été correctement consignés et comptés.

Généralement, lors d'un audit administratif, on choisit au hasard une partie des bulletins de vote papier et on les compare aux attentes. Cela se fait habituellement en appliquant des critères prédéfinis. Par exemple, avant une élection, on peut choisir au hasard 2 % des circonscriptions pour lesquelles les bulletins de vote seront comptés à la main afin de vérifier s'ils correspondent aux chiffres obtenus au moyen du dépouillement à la machine.

Cependant, dans un audit traditionnel, il y a préoccupation que les critères prédéfinis peuvent être insuffisants pour gagner la confiance des électeurs lors d'élections serrées tout en étant inutilement lourd pour des élections avec une grande marge de victoire.

Un audit limitant les risques (ALR) est une solution de rechange dynamique à un audit administratif traditionnel. La limite de risque est déterminée avant le début de l'audit et décrit la probabilité maximale qu'un dépouillement complet des voix produise un résultat différent (gagnant). Si l'on tient compte de la marge de victoire et que l'on effectue des calculs statistiques pendant l'audit, l'audit permet souvent d'atteindre un niveau de confiance élevé même si l'on examine beaucoup moins de bulletins de vote, sinon, on poursuit l'audit au-delà d'un point d'arrêt prédéterminé lorsque cela est nécessaire pour atteindre un niveau de confiance suffisant dans une élection serrée. Ce type d'audit est généralement beaucoup plus efficace, mais un des désavantages est que sa nature dynamique rend difficile l'allocation de temps et de ressources, car on ne sait pas l'avance combien de temps il durera.

Les principaux types d'ALR sont les audits de bulletins de vote et les audits de comparaison des bulletins de vote. Dans le cadre du premier, les bulletins papier sont choisis au hasard, et on procède au dépouillement des votes, le résultat devrait correspondre au résultat annoncé précédemment.

Dans le cadre de l'audit de comparaison des bulletins de vote, le contenu de chaque bulletin est consigné dans un registre électronique des votes exprimés. Les bulletins papier sont alors choisis au hasard et comparés au registre correspondant. Comme chaque correspondance devrait être parfaite, il n'est pas nécessaire d'attendre la confirmation et on peut donc atteindre la limite de risque en examinant beaucoup moins de bulletins.

L'une des difficultés des audits de comparaison des bulletins de vote est de savoir comment gérer la liste des registres. En effet, un électeur pourrait se faire dire de voter selon un mode très précis, et la personne qui exerce la coercition peut ensuite vérifier dans le registre public si un bulletin de vote présentant ce schéma se trouve dans le bureau de scrutin de l'électeur. En revanche, si les registres ne sont pas publiés, l'audit n'est pas convaincant. Un observateur pourrait être d'avis que les administrateurs se sont contentés de sélectionner des bulletins et ont affirmé sans preuve qu'ils correspondaient à la liste non divulguée des registres.

Cette difficulté peut être résolue en publiant un document chiffré de tous les registres ainsi que des preuves vérifiables par le public que ces registres correspondent aux résultats annoncés. Une fois l'audit terminé, les registres vérifiés peuvent être déchiffrés et il est possible de prouver qu'ils correspondent aux bulletins papier correspondants. Puisqu'on ne publie qu'une fraction des registres, les renseignements personnels des électeurs sont protégés. Cette façon de faire est pratique, car il est possible d'utiliser les outils d'audit public existants pour chiffrer les bulletins de vote et produire les preuves nécessaires.

Josh Benaloh,
Senior Cryptographer, Microsoft Research

Atelier 5

Des technologies électorales vérifiables de bout en bout pour améliorer la sécurité des modes de scrutin

Dans toutes les démocraties du monde, différents systèmes informatiques sont de plus en plus utilisés pour l'expression des suffrages et le dépouillement officiel des bulletins de vote lors d'une élection. Ces technologies – que ce soit les dispositifs de marquage des bulletins de vote, des lecteurs optiques pour lire les bulletins de vote en papier marqués à la main, ou des solutions expérimentales de vote en ligne/à distance – offrent des avantages considérables à l'administration des élections, notamment pour ce qui de l'échelle, de la réponse aux besoins d'accessibilité, de la rapidité et de la précision du dépouillement. Cependant, pour être efficaces, ces systèmes doivent être dignes de confiance et correctement sécurisés, et tous les composants électroniques doivent susciter une attention particulière en matière de cybersécurité.

La vérifiabilité de bout en bout est un ensemble de technologies et de solutions de cryptage qui visent à répondre à la question : « Comment puis-je avoir confiance dans l'exactitude du résultat d'une élection... si je crains que le logiciel, le matériel, l'infrastructure de transmission ou le personnel responsable de la conduite de l'élection ne soient pas dignes de confiance? » Contrairement aux logiciels bancaires ou à d'autres secteurs à haute sécurité, les élections à scrutin secret requièrent un ensemble unique d'exigences en matière de sécurité, car les données d'un particulier (vote) doivent toujours rester secrètes, et il ne peut y avoir de lien direct entre l'identité du particulier et son vote.

La vérifiabilité honore ce postulat en se concentrant sur deux principes primaires :

- **Confidentialité** – Personne d'autre que l'électeur ne doit connaître le contenu d'un vote particulier. Tous les votes sont cryptés immédiatement après avoir été émis et aucun vote n'est jamais décrypté.
- **Intégrité** – Les électeurs reçoivent un code de vérification unique pour s'assurer que leur vote a été inclus dans le dépouillement final, n'importe qui peut vérifier si les votes enregistrés ont été correctement comptés, et le logiciel ne peut pas « tricher » et annoncer un dépouillement incorrect sans qu'un tel événement ne soit clairement détectable.

Dans son rapport de 2018 intitulé « Securing the Vote » (Protéger le scrutin), l'Académie nationale des sciences aux États-Unis recommande aux autorités étatiques et locales de mener et d'évaluer des projets pilotes de systèmes électoraux vérifiables de bout en bout.

Microsoft a récemment lancé un kit de développement (SDK) gratuit et en source ouverte, appelé **ElectionGuard**, qui adopte les principes de la vérifiabilité de bout en bout. Ce kit est conçu pour fonctionner sur des systèmes de scrutin nouveaux ou existants pour rendre le vote plus sûr, plus auditable, plus vérifiable et plus digne de confiance. Au début de 2021, ElectionGuard avait été utilisé lors d'élections publiques et d'élections législatives à bulletin secret aux États-Unis, et son utilisation est actuellement étudiée sur plusieurs continents. Vous trouverez des informations sur ElectionGuard a**www.electionguard.vote**

ElectionGuard peut également être utilisé pour renforcer la sécurité et la confidentialité des audits postélectoraux, tels que les audits limitant les risques (ALR). Les audits publics et administratifs sont essentiels pour garantir que les élections ont été menées et comptabilisées correctement, mais ces audits compromettent parfois la vie privée des électeurs en révélant publiquement et en ouvrant les bulletins de vote scellés. ElectionGuard peut aider à protéger la vie privée des électeurs en cryptant les données pendant ces audits postélectoraux.

Ethan Chumley,
Stratège principal en sécurité, programme Defending Democracy, Microsoft

Atelier 5

Un regard sur les élections américaines de 2020 - amélioration des pratiques : la communication et la coordination sur la cybersécuritéet la sécurité des infrastructures électorales ont augmenté de manière considérable

En prévision de l'élection américaine de 2020, le gouvernement américain, le secteur privé et les organisations de la société civile ont fait d'importants progrès dans la coordination de l'infrastructure et la cybersécurité électorales. De nouveaux organismes et institutions ont joué un rôle important pour faciliter la communication et la coopération entre les responsables fédéraux, étatiques et locaux, ainsi qu'avec les campagnes politiques.

Après l'élection de 2016, le gouvernement fédéral et les partenaires de la société civile ont mis en place de nouveaux mécanismes pour combler les écarts entre les autorités fédérales et étatiques, notamment la Cybersecurity and Infrastructure Security Agency (CISA) et l'Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

En 2020, la coordination entre les responsables fédéraux, étatiques et locaux, ainsi qu'entre les intervenants intersectoriels, a augmenté considérablement. Le CISA et l'EI-ISAC ont noué et entretenu des relations profondes afin d'ouvrir des lignes de communication pour l'échange d'informations et de bonnes pratiques. L'EI-ISAC a organisé une « salle virtuelle de conscience situationnelle » commune qui a rassemblé des centaines de responsables électoraux, des membres du personnel de la CISA et de l'EI-ISAC, des employés d'entreprises de médias sociaux et des représentants de partis politiques afin d'échanger des informations, de surveiller les menaces et de fournir des conseils sur la sécurité des élections dans les heures précédant, pendant et après l'élection[20]. L'EI-ISAC a également géré une salle de crise le jour de l'élection, avec des équipes de réponse aux incidents, de renseignement et d'ingénierie prêtes à intervenir pour surveiller les menaces et apporter son appui aux représentants des États et des collectivités locales, au besoin[21].

Les agences fédérales et les partenaires de la société civile ont offert une multitude de ressources et d'assistance aux autorités étatiques et locales, ainsi qu'aux campagnes, pour les aider à sécuriser et à mener à bien l'élection, apportant un soutien que les responsables n'auraient peut-être pas eu autrement. Ces efforts méritent d'être salués, mais il est encore possible d'assurer une plus grande adoption et une plus grande sécurité. Par exemple, bien que près de 3 000 autorités électorales étatiques et locales aient joint l'EI-ISAC en novembre 2020, il y a plus de 10 000 autorités qui organisent des élections à l'échelle du pays[22].

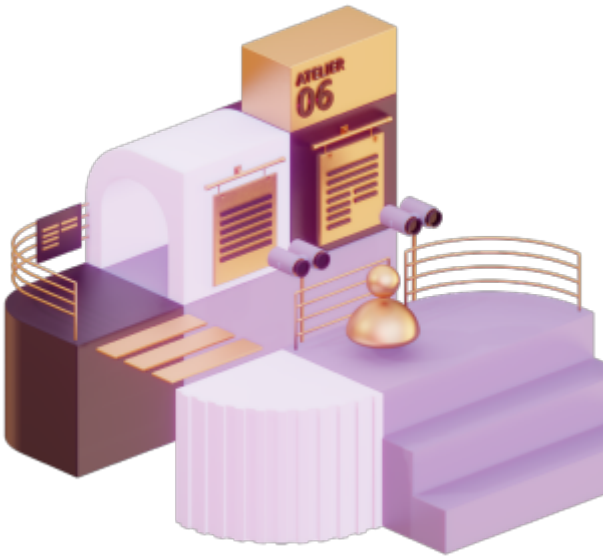
From the Alliance for Securing Democracy's assessment of the 2020 U.S. election, Brandt, J. and Hanlon, B. (2021, March 30). *Defending 2020: What Worked, What Didn't, and What's Next.*[23]

20 MS-ISAC hits 10,000 members, eyes continued growth with local governments. Freed, B. (le 14 décembre 2020) **https://statescoop.com/ms-isac-10000-members-cis-20th-anniversary/**; International Election Observation Mission. Assemblée parlementaire de l'OSCE (le 3 novembre 2020) **https://www.osce.org/files/f/documents/9/6/469437.pdf**; Election Administration at State and Local Levels. National Conference on State Legislatures (le 3 février 2020) **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. (le 5 novembre 2020) **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. (le 3 novembre 2020) **https://statescoop.com/election-infrastructure-prepares-election-day-2020/**; How US security officials are watching for threats ahead of Election Day. Lyngaas, S. (le 22 octobre 2020) **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. (le 3 novembre 2020) **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**



Atelier 6 : Habiliter les citoyens : Comprendre et renforcer la résilience des communautés pour contrer la menace d'ingérence électorale

Une démocratie stable qui fonctionne correctement ne peut se passer de citoyens bien informés et engagés

C'est pourquoi les citoyens doivent avoir accès à des sources d'information diverses et fiables afin de pouvoir se forger une opinion éclairée, prendre de bonnes décisions et exercer un jugement réfléchi. Malheureusement, les problèmes grandissants de la désinformation généralisée et de la publication de commentaires toxiques en réponse à des messages dans les médias sociaux minent la confiance des citoyens dans les sources d'information crédibles. Pratiquée par des acteurs tant étrangers que nationaux, la désinformation est donc une menace pour la démocratie elle-même, y compris les élections.

La méfiance à l'égard des grands médias est particulièrement préoccupante; de plus en plus de personnes obtiennent leurs informations en ligne, où il peut parfois être difficile de faire la distinction entre les sources fiables et non fiables. Exacerbant cette menace, les acteurs malveillants s'en prennent de plus en plus à des segments spécifiques de la société afin d'exploiter, d'amplifier et d'aggraver délibérément les divisions et les tensions actuelles. Combinés, ces phénomènes ont contribué à une polarisation accrue et à un débat public plus tendu sur des questions comme le changement climatique, l'immigration et, plus récemment, la santé publique et la réponse à la pandémie de COVID-19.

Lors du sixième atelier, on s'est penché sur la façon dont les gouvernements, l'industrie et les organisations de la société civile peuvent élaborer des politiques et des programmes pour aider les citoyens à évaluer de manière critique ce qu'ils lisent et diffusent afin de renforcer la résilience des communautés à l'égard de l'effet corrosif de la désinformation. Comme pour tous les défis de cette ampleur, une approche globale et collaborative est particulièrement importante pour sauvegarder l'intégrité des élections et des processus électoraux.

Bonnes pratiques et stratégies pour le gouvernement, littératie numérique et vérification des faits

Les initiatives communautaires sont efficaces, en partie, parce que les informations reçues d'une source communautaire crédible peuvent se poser en complément des communications du gouvernement. Les organisations et les dirigeants qui ont établi des réseaux sont les plus susceptibles de gagner la confiance des citoyens, en particulier au sein des groupes difficiles à joindre ou vulnérables.

Les gouvernements, les organisations de la société civile et les plateformes de médias traditionnels ou sociaux doivent tenir compte de considérations importantes lorsqu'ils établissent des partenariats avec les communautés :

- Savoir qu'une organisation peut ne pas représenter l'ensemble de la communauté;
- S'assurer que les personnes et les organisations qui s'attaquent aux menaces liées à l'information dans diverses communautés sont interconnectées, car elles peuvent échanger des outils et des informations;
- Comprendre ce que les partenaires communautaires font déjà et ce dont ils ont besoin pour poursuivre ou élargir leur action.

Soyez prêt et proactif – pré-discréditez. En adoptant des mesures proactives contre la désinformation, vous contribuerez à la résilience des citoyens. « Inondez » l'espace de l'information avec des informations précises et utiles, au moyen de conférences de presse fréquentes, de sites Web gouvernementaux et de comptes de médias sociaux fiables (p. ex., l'OGE ou autorités de santé publique). Concentrez-vous sur les questions de processus, en soulignant les mécanismes et les procédures liés aux élections. La désinformation se propageant très rapidement, une approche purement réactive augmente la probabilité qu'un faux récit entraîne un réel préjudice pour les individus, les groupes ou les organisations.

Élaborez des suggestions concrètes et alimentez un récit positif et courtois. Mettez l'accent sur les vertus de la démocratie, le renforcement de la souveraineté du pays, les valeurs communes et l'intérêt national. Cela doit être fait de manière à favoriser la cohésion sociale et s'appliquer à tous les pays, en se concentrant sur le contenu ou le comportement plutôt que sur l'acteur. Lorsque l'on s'attaque aux menaces liées à l'information, il est également nécessaire d'éviter les platitudes et les grandes généralisations.

Développez la culture civique et numérique.

Vous devez connaître votre public. Pour inculquer un sentiment clair de la démocratie et des institutions démocratiques, les programmes d'éducation et de littératie numérique devraient être adaptés à des groupes démographiques et des communautés spécifiques. Cela comprend les étudiants de l'école primaire à l'université, ainsi que les adultes de plus de 65 ans, et les programmes de formation pour les entreprises de médias, afin de les aider à repérer les campagnes d'influence de l'information.

Adaptez les programmes et les contenus à des communautés spécifiques. Adressez-vous aux communautés marginalisées en tenant compte de facteurs comme le revenu, l'accès aux technologies et le statut d'immigration, et veillez à ce que les efforts en matière d'éducation et de littératie numérique soient adaptés à ces populations. Il est également nécessaire de reconnaître quels outils éducatifs sont efficaces pour différentes populations. Par exemple, les médias sociaux ou les outils en ligne peuvent être efficaces pour mobiliser les jeunes, tandis que les ateliers en personne dans les centres communautaires et les bibliothèques peuvent être plus efficaces pour les populations plus âgées. Le contenu devrait être simple et ne pas porter de jugement. Il devrait encourager les gens à s'arrêter et à réfléchir à ce qu'ils voient en ligne avant de le croire ou de le diffuser.

Les outils numériques sont essentiels. Pour que les efforts en matière de littératie numérique soient efficaces, il faut davantage avoir accès accru à des outils numériques permettant de repérer les faux comptes de médias sociaux, les images et vidéos manipulées et la source initiale de l'information. Ces outils sont souvent gratuits, peu coûteux et à source ouverte. De plus, il est essentiel de veiller à ce que des recherches fiables et des contenus crédibles soient largement accessibles pour aider les citoyens à déceler la désinformation.

Atelier 6

L'importance de la vérification des faits

Le profil de la vérification des faits a considérablement augmenté au cours de la dernière décennie. Les vérificateurs de faits représentent maintenant une source fiable de renseignements pour des millions de gens partout dans le monde. On observe de plus en plus que la vérification des faits fonctionne. Des études ont démontré que si l'on soumet à un groupe de personnes un élément de désinformation, puis qu'on soumet dans un deuxième temps l'information correcte à un sous-groupe d'entre elles seulement, le pourcentage de personnes adhérant à l'élément de désinformation est considérablement plus faible au sein de ce sous-groupe.

L'écosystème d'information dans lequel les vérificateurs de faits travaillent est aujourd'hui complexe et en constante évolution. Depuis quelques années, on se soucie de plus en plus de la désinformation. La rapidité et l'importance d'Internet dans nos vies permettent au phénomène de se répandre comme jamais. En tant qu'organisme vérificateur de faits indépendant et sans but lucratif du Royaume-Uni, Full Fact a pu constater concrètement à quel point la désinformation favorise la haine, cause du tort à la santé et nuit à la démocratie.

Les vérificateurs de faits se situent aux premières lignes lorsqu'il s'agit de déterminer les faits et d'évaluer la qualité de l'information. Dans un rapport publié en 2020, nous avons établi que les difficultés se situent à différents niveaux. Par exemple, dans le cadre du processus de surveillance et de sélection, les vérificateurs de faits doivent composer avec de grands volumes d'affirmations potentiellement à vérifier, des questions sur la manière de définir la viralité, la nature opaque de certaines plateformes et à répondre à des volumes élevés de demandes du public.

Afin de pouvoir établir si une affirmation est vraie, les vérificateurs de faits font face à de nombreux défis, dont l'accessibilité de l'information et la transparence des autorités responsables, le caractère hautement répétitif des tâches liées à la vérification des affirmations et à la recherche ainsi que la modification ou la disparition des outils de recherche en ligne. Lorsqu'ils publient et distribuent le fruit de leur travail, les vérificateurs de faits font face à d'autres défis, comme d'essayer d'établir le juste équilibre entre la demande pour des vérifications de faits provenant d'entreprises basées en ligne et l'incidence des partenariats établis.

Si la technologie aide de nombreux vérificateurs de faits dans leur travail, son efficacité n'en est pas moins limitée. Elle ne peut à elle seule résoudre des difficultés comme la difficulté d'obtenir des renseignements auprès de certains gouvernements ou le manque de transparence et de facilité d'accès à l'information.

Mais s'y attaquer à l'échelle mondiale lorsque des vies sont en jeu et qu'il faut préserver la liberté d'expression est un défi nouveau. Il faut largement renforcer la collaboration entre toutes les parties prenantes du monde de l'information : les entreprises en ligne telles que Twitter, Facebook et Google, les vérificateurs de faits du monde entier, les organisations de la santé ainsi que les chercheurs et les organisations de la société civile. Si nous pouvions disposer de réponses déjà préparées d'après des recherches et des discussions, nous serions tous en mesure de répondre rapidement et de travailler beaucoup plus efficacement. Voilà pourquoi, grâce au soutien financier de Facebook, Full Fact travaille à l'élaboration d'un nouveau cadre pour gérer les incidents en lien avec l'information.

Les vérificateurs de faits jouent un rôle essentiel dans l'écosystème d'information, mais ils ne peuvent pas à eux seuls régler le problème. Nous devons tous jouer notre rôle afin de veiller à ce que l'information juste prévale.

Full Fact

Atelier 6

Le travail de Patrimoine canadien pour financer des projets en vue des élections de 2019

Avant les élections générales de 2019 au Canada, on se préoccupait que certains citoyens soient la cible de manœuvres de désinformation en ligne ayant le potentiel de se répercuter sur le résultat des élections ou de semer la discorde dans la société.

Le 30 janvier 2019, en réponse à cette préoccupation, la ministre des institutions démocratiques a annoncé l'approche du gouvernement du Canada pour défendre la démocratie au pays. Cela a permis au ministère du Patrimoine canadien (PCH) de créer l'Initiative de citoyenneté numérique (ICN) et d'investir 7 millions de dollars dans des activités citoyennes afin de soutenir la démocratie et la cohésion sociale au Canada, en prévision de l'élection fédérale de 2019. L'objectif stratégique de ces activités était de renforcer la résilience des citoyens face à la désinformation en ligne et d'établir des partenariats avec des organismes de la société civile afin de soutenir l'établissement d'un écosystème d'information fiable. Ainsi, plus de 20 projets sur la citoyenneté, les nouvelles et les médias numériques ont permis à des tiers d'offrir des activités et des programmes financés par PCH et l'ICN, dont des séances de sensibilisation et des ateliers et activités visant l'élaboration d'outils pédagogiques pour accroître les connaissances du public à l'égard des médias numériques et de la citoyenneté.

Les projets financés visaient en particulier à aider les Canadiens à avoir une pensée critique face à l'information en ligne, à comprendre le fonctionnement des algorithmes et la manière dont ils peuvent parfois définir l'expérience de l'utilisateur, à reconnaître quand et comment des intervenants mal intentionnés peuvent exploiter les plateformes numériques, et à acquérir les compétences nécessaires pour éviter de se faire manipuler.

Afin de maximiser l'efficacité et l'impact des projets en vue des élections fédérales de 2019, l'ICN a accordé la priorité à des initiatives de nature variée qui permettaient d'atteindre un vaste éventail de participants de différents groupes d'âge et de différentes régions; des candidats qui différaient aussi sur le plan des capacités, de l'emploi et de l'identité. Le financement accordé visait à permettre la tenue d'activités citoyennes à participation directe et indirecte.

Les participants « directs » sont ceux qui ont pris part à des ateliers ou à des activités de sensibilisation, à des activités de mobilisation sur les médias sociaux et à des groupes de travail, qui ont eu accès à du matériel éducatif et qui ont pris part à des défis ou à des concours. Les participants indirects sont les Canadiens qui ont été touchés par des activités financées par l'ICN par des voies moins directes, notamment des publicités sur les plateformes en ligne ou les médias sociaux, et des ateliers offerts par des gens qui ont eux-mêmes pris part à une activité ou un programme (approche « former les formateurs »). Les participants indirects sont aussi ceux qui ont eu accès à de l'information transmise de manière informelle par des jeunes, des éducateurs et des adultes.

Le budget fédéral de 2019 prévoyait 19,4 M$ sur quatre ans pour l'ICN afin de permettre la poursuite des activités et l'élargissement de leur portée en dehors du contexte des élections. À présent, l'ICN lance annuellement des appels d'offres pour financer des activités citoyennes au moyen d'un programme de contribution spécial. L'Initiative est une composante clé de l'écosystème d'acteurs qui cherchent à renforcer la résilience citoyenne au Canada.

Patrimoine canadien

Atelier 6

Un regard sur les élections américaines de 2020, ce qui a bien fonctionné : La société civile a mené des activités essentielles de renforcement de la résilience dans l'espace d'information

Tout au long du cycle électoral de 2020, les organisations de la société civile ont mené des activités de renforcement de la résilience qui ont comblé des lacunes importantes entre le gouvernement et le secteur privé – en surveillant l'espace d'information national, en informant publiquement les citoyens et en les préparant aux faux récits, et en facilitant l'échange d'informations et la coordination entre les différents secteurs. Ces activités ont été alimentées par un degré élevé d'intérêt public et un soutien philanthropique considérable. Il s'agit d'un modèle qui a généré une activité importante et percutante, mais qui n'est peut-être pas durable. Néanmoins, l'institutionnalisation de ces efforts pourrait poser des défis importants en soi, compte tenu des préoccupations liées aux droits à la vie privée et à la liberté d'expression.

Parmi les initiatives les plus marquantes de la société civile dans ce domaine figure l'Election Integrity Partnership (EIP), une coalition d'organismes de recherche visant à favoriser l'échange d'informations en temps réel entre les chercheurs, les organisations de la société civile, les plateformes de médias sociaux, les organismes gouvernementaux et les responsables électoraux[23]. L'EIP a servi d'important centre d'échange des informations entre le gouvernement, les plateformes et les chercheurs. Il a joué un rôle de premier plan en signalant les contenus préjudiciables aux entreprises. Et il a communiqué régulièrement avec le public, en produisant des analyses en temps réel des tactiques et des actualités de désinformation, et en organisant de fréquents points de presse[24].

Une myriade d'autres organisations de la société civile – d'Election SOS à la National Task Force on Election Crises et à la Disinfo Defense League – ont mis à la disposition des responsables électoraux, des journalistes et du public national des outils permettant de repérer et de contrer les fausses informations et la désinformation[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. (le 31 juillet 2020) **https://www.eipartnership.net/news/announcing-the-eip**

24 Election Delegitimization: Coming to you Live. Miller, C.M. et al. (le 18 novembre 2020). **https://www.eipartnership.net/rapid-response/election-delegitimization-coming-to-you-live;** Weaponizing projections as tools of election delegitimization. Bak-Coleman, J. (le 5 novembre 2020). **https://www.eipartnership.net/rapid-response/weaponizing-projections-as-tools-of-election-delegitimiz ation**

25 Meet the researchers and activists fighting misinformation. Birnbaum, E. (le 17 novembre 2020) **https://www.protocol.com/election-day-2020-misinfomation-disinformation;** The Fight Against Disinformation Requires the Right Tools. PEN America (le 3 décembre 2020). **https://pen.org/the-fight-against-disinformation-requires-the-right-tools/;** Resources. The National Task Force on Election Crises (sansdate). **https://www.electiontaskforce.org/resources;** Three New Ways Civil Society Is Protecting the U.S. Election. Quarcoo, A. (le 28 octobre 2020). **https://carnegieendowment.org/2020/10/28/three-new-ways-civil-societ y-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**

Bibliographie

Atelier 1

Beavers, O. (le 7 août 2020) *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 (le 10 août 2020) *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) (sans date) *Frequently Asked Questions.* Federal Bureau of Investigation, United States of America Department of Justice. https://www.ic3.gov/#

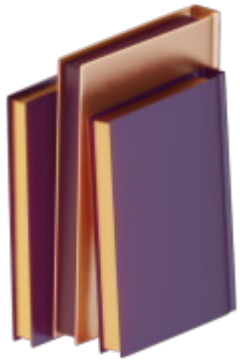
Nakashima, E. (le 3 novembre 2020) *U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election.* The Washington Post. https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html

Nakashima. E., et coll. (le 22 octobre 2020) *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. (le 22 octobre 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, J. (le 5 février 2021) *Hybrid CoE Paper 5: Improving cooperation with social media companies to counter electoral interference.* Centre européen d'excellence pour la lutte contre les menaces hybrides. 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 (le 10 septembre 2020) *Treasury Sanctions Russia-Linked Election Interference Actors.* Gouvernement des États-Unis. https://home.treasury.gov/news/press-releases/sm1118



Atelier 2

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

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

Dictionnaire Larousse (sans date). *S'ingérer*. Dictionnaire Larousse. https://www.larousse.fr/dictionnaires/francais/s_ingérer/43067

Ministère de l'Intérieur de l'Australie (sans date). *National Security: Countering Foreign Interference*. Gouvernement australien. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Facebook (2021). *Standards de la communauté : 20. Comportement trompeur*. Facebook, Inc. https://fr-fr.facebook.com/communitystandards/inauthentic_behavior

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

Pamment, J., et coll. (1er juillet 2018). *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. (février 2019). *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 (janvier 2021). *Politique en matière d'intégrité civique*. Twitter, Inc. https://help.twitter.com/fr/rules-and-policies/election-integrity-policy

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

Atelier 3

COVID Working Group by the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council (sans date). *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

Corte, E., et coll. (5 juin 2020). *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 coll. (19 mars 2020). *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

Atelier 4

Centre canadien pour la cybersécurité (le 5 avril 2019). *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019* Gouvernement du Canada. https://cyber.gc.ca/fr/orientation/le-point-sur-les-cybermenaces-contre-le-processus-democratique-du-canada-en-2019

Centre canadien pour la cybersécurité (le 5 avril 2019). *Le point sur les cybermenaces contre le processus démocratique du Canada* Gouvernement du Canada. https://cyber.gc.ca/fr/orientation/le-point-sur-les-cybermenaces-contre-le-processus-democratique-du-canada

Institutions démocratiques (le 9 juillet 2019). *Directive du Cabinet sur le Protocole public en cas d'incident électoral majeur* Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/protocole-public--incident-critique-elections/cabinet.html

Institutions démocratiques (le 9 juillet 2019). *Protocole public en cas d'incident électoral majeur.* Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/protocole-public--incident-critique-elections.html

Institutions démocratiques (le 20 novembre 2019). *Protocole public en cas d'incident électoral majeur : Document d'information.* Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/nouvelles/2020/10/protocole-public-en-cas-dincident-electoral-majeur.html

Institutions démocratiques (le 9 juillet 2019). *Protocole public en cas d'incident électoral majeur : Graphique*. Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/protocole-public.html

Institutions démocratiques (le 19 mars 2020). *Compter sur les plateformes de médias sociaux pour qu'elles agissent : Document d'information*. Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/nouvelles/2019/01/encourager-les-plateformes-de-medias-sociaux-a-agir.html

Institutions démocratiques (le 19 mars 2020). *Protection de la démocratie – Sauvegarder nos élections et nos institutions démocratiques*. Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie.html

Institutions démocratiques (le 7 février 2019). *Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections : Graphique*. Gouvernement du Canada. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/groupe-travail-securite.html

Journalism Trust Initiative. (sans date). *Le problème. La solution. Le procédé*. Journalism Trust Initiative. https://jti-rsf.org/fr/

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

Atelier 5

Berger, M., et coll. (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 coll. (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. (le 9 septembre 2019). *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 (sans date). *Election Infrastructure Cyber Risk Assessment and Infographic.* United States of America. https://www.cisa.gov/publication/election-cyber-risk

Cybersecurity and Infrastructure Security Agency (sans date). *Mail-in Voting Risk: Infrastructure and Process.* États-Unis d'Amérique. https://www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-infographic_508.pdf

Department of Homeland Security (le 14 juillet 2020). *US Electoral Process.* United States of America. https://www.dhs.gov/topic/election-security

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

Freed, B. (le 5 novembre 2020). *'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. (le 3 novembre 2020). *'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. (le 22 octobre 2020). *How US security officials are watching for threats ahead of Election Day.* https://www.cyberscoop.com/2020-election-cybersecurity-chris-krebs/

Microsoft (sans date). *Stratégies anti-hameçonnage dans Microsoft 365.* https://docs.microsoft.com/fr-ca/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide

Microsoft (le 5 octobre 2020). *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 (sans date). *Meilleures pratiques en matière de sécurité du contrôle d'accès et de la gestion des identités Azure.* https://docs.microsoft.com/fr-ca/azure/security/fundamentals/identity-management-best-practices

Microsoft (sans date). *Tutoriel : Examiner des applications OAuth à risque.* https://docs.microsoft.com/fr-ca/cloud-app-security/investigate-risky-oauth

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

Microsoft (sans date). *Vue d'ensemble de Microsoft Defender Application Guard*. https://docs.microsoft.com/fr-ca/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 (sans date). *Rapports d'activité de connexion dans le portail Azure Active Directory*. https://docs.microsoft.com/fr-ca/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 (le 3 février 2020). *Election Administration at State and Local Levels*. https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx

Assemblée parlementaire de l'organisation pour la sécurité et la coopération en Europe (le 3 novembre 2020). *International Election Observation Mission*. https://www.osce.org/files/f/documents/9/6/469437.pdf

Select Committee On Intelligence (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, No. 116-290, Vol. 1, at 6*. United States Senate https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

Atelier 6

Bak-Coleman, J. (le 5 novembre 2020) *Weaponizing projections as tools of election delegitimization*. https://www.eipartnership.net/rapid-response/weaponizing-projections-as-tools-of-election-delegitimization

Birnbaum, E. (le 17 novembre 2020). *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

Patrimoine canadien (le 2 juillet 2019). *Aider les citoyens à renforcer leur pensée critique et leur résilience face aux dangers de la désinformation en ligne*. Gouvernement du Canada. https://www.canada.ca/fr/patrimoine-canadien/nouvelles/2019/07/aider-les-citoyens-a-renforcer-leur-pensee-critique-et-leur-resilience-face-aux-dangers-de-la-desinformation-en-ligne.html

Centre de la sécurité des télécommunications. (sans date). *Pratiques exemplaires en cybersécurité*. Gouvernement du Canada. https://www.cse-cst.gc.ca/fr/cyberhygiene-pratiques-cybersecurite

Cybersecurity and Infrastructure Security Agency (sans date). *#protect2020 Rumor vs. Reality*. États-Unis d'Amérique. https://www.cisa.gov/rumorcontrol

Cybersecurity and Infrastructure Security Agency (sans date). *Resilience Series Graphic Novels*. États-Unis d'Amérique. https://www.cisa.gov/cfi-resilience-series-graphic-novels

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

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

Full Fact (le 17 décembre 2020). *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 (le 17 décembre 2020). *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/

Gouvernement du Canada (le 17 octobre 2020). *Désinformation en ligne - Initiative de citoyenneté numérique*. Gouvernement du Canada. https://www.canada.ca/fr/patrimoine-canadien/services/desinformation-en-ligne.html

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

PEN America (le 3 décembre 2020). *The Fight Against Disinformation Requires the Right Tools*. https://pen.org/the-fight-against-disinformation-requires-the-right-tools/

Quarcoo, A. (le 28 octobre 2020). *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. (le 31 juillet 2020). *Announcing the EIP*. https://www.eipartnership.net/news/announcing-the-eip

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