

Défendre, détecter et récupérer :

Contrer la menace d'ingérence dans les infrastructures électorales

Tout au long de 2020, les signataires de l'Appel de Paris pour le principe « Défendre les processus électoraux », qui est codirigé par l'Alliance for Securing Democracy (ASD), le gouvernement du Canada et Microsoft dans le cadre de l'Appel de Paris pour la confiance et la sécurité dans le cyberspace, ont organisé une série d'ateliers multipartites qui portaient tous sur un sujet essentiel lié à la prévention de l'ingérence dans le processus électoral. Voici un premier aperçu des principales observations dégagées par les intervenants au cours de ces ateliers. Une vue d'ensemble plus détaillée des pratiques exemplaires qui en sont ressorties paraîtra au début de 2021.

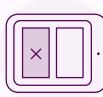
La protection des infrastructures électORALES est essentielle pour contrer l'ingérence électORALE.
Voici quelques-unes des pratiques exemplaires que nous avons entendues de la part des parties prenantes au sein du gouvernement, de l'industrie, des médias et de la société civile pour y parvenir avant, pendant et après les élections.

Protéger les systèmes d'inscription des électeurs



- Envisager des sauvegardes chiffrées, y compris des sites miroirs distants chiffrés, et des sauvegardes sur papier.
- Restreindre l'accès aux systèmes d'inscription des électeurs. Suivre le principe du droit d'accès minimal – une personne ne doit se voir accorder que les droits d'accès nécessaires à l'accomplissement d'une tâche dans un système technique.

Soutenir les registres électoraux électroniques et les systèmes de vote rapide sur papier



- Les registres électoraux électroniques et les systèmes de vote sur papier qui comptent rapidement les bulletins de vote (c'est-à-dire les scanners) et qui peuvent être contrôlés présentent des avantages.
- Les registres électoraux électroniques permettent un vote plus rapide et une synchronisation en temps réel pour aider à enregistrer de manière fiable qu'un électeur s'est inscrit, qu'il a déposé un bulletin de vote et qu'il n'a pas voté plus d'une fois.
- Mais les registres électoraux électroniques peuvent être défaillants, c'est pourquoi il faut stocker du matériel de secours comme des registres électoraux sur papier et des enveloppes pour que les électeurs puissent voter provisoirement.

Tenir à jour la technologie de vote



- Avoir des plans pour remplacer périodiquement la technologie de vote afin d'éviter l'utilisation de systèmes de vote obsolètes ou peu sûrs.

Effectuer des vérifications pour renforcer la confiance dans les résultats des élections



- Les vérifications de limitation des risques présentent des avantages par rapport aux vérifications traditionnelles. Elles sont plus efficientes, elles sont dynamiques et elles ne confirment que le vainqueur, et non la marge par laquelle le vainqueur a gagné, puisque ce type de vérification ne porte que sur un échantillon statistiquement significatif, au lieu de réaliser un comptage complet.

Permettre aux entreprises de cybersécurité de soutenir les campagnes électorales



- Les campagnes n'ont souvent pas l'expertise ou les capacités nécessaires pour traiter les questions de cybersécurité par elles-mêmes.