INTERNATIONAL IDEA
INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

La sécurité informatique des processus électoraux

Modèles de collaboration entre organismes

La sécurité informatique des processus électoraux

Modèles de collaboration entre organismes

Sam van der Staak et Peter Wolf

IDEA International
Strömsborg
SE–103 34 Stockholm
Suède
Téléphone : +46 8 698 37 00
Courriel : info@idea.int
Site Internet : ‹https://www.idea.int›

Traduction : Strategic Agenda Ltd
Révision : Anne Marsaleix
Graphisme : IDEA International
Illustration de la couverture : ID 125793633 © Blackboard373 | Dreamstime.com
DOI : ‹https://doi.org/10.31752/idea.2020.50›

ISBN: 978-91-7671-329-7 (PDF)

Créé avec Booktype: ‹https://www.booktype.pro›

Table des matières

Préface

Les technologies de l'information et de la communication ont un poids grandissant dans les procédures de gestion électorale et les processus démocratiques. Si ces technologies offrent de nouvelles possibilités, elles entraînent également de nouvelles menaces dans leur sillage. La sécurité informatique représente, à l'heure actuelle, un enjeu électoral majeur, même dans les pays exempts de toute forme de vote électronique. La sécurité informatique implique nombre d'intervenants, à commencer par les organismes de gestion des élections, les entités spécialisées en cybersécurité et les agences de sécurité.

Dans de nombreux pays, il s'est dégagé un consensus autour du caractère essentiel de la collaboration entre organismes afin de préserver les processus électoraux des menaces numériques. Ces dernières années, cette coopération s'est structurée et intensifiée, tant au niveau national qu'international.

Le présent document se propose de dresser un état des lieux sur les progrès enregistrés en matière de sécurité informatique en contexte électoral dans différents pays. Regroupant une vingtaine d'études de cas menées dans le monde entier, ce document constitue une mine d'informations pour quiconque souhaite se prémunir contre les attaques informatiques.

Alors que les technologies numériques font de plus en plus partie intégrante de nos sociétés, l'ensemble des pays devront orienter leurs investissements de façon à garantir l'intégrité des élections face aux menaces informatiques. Nous espérons que ce guide apportera un éclairage sur la sécurité informatique et trouvera un écho au-delà des pays qui ont fait l'objet de nos recherches.

IDEA International

Remerciements

Le présent guide a été rédigé avec le concours du programme régional Europe et du programme mondial d'IDEA International.

Les précieuses données qui y figurent, ainsi que les analyses et entretiens menés dans le cadre des études de cas sont à porter au crédit de nombreuses personnes travaillant pour le compte de différentes institutions, parmi lesquelles : la Commission électorale indépendante d'Afrique du Sud, la Commission électorale australienne, le ministère fédéral autrichien de l'Intérieur, la Commission électorale centrale de la République de Bulgarie, Élection Canada, le ministère de l'Économie et de l'Intérieur du Danemark, le bureau électoral de l'Estonie, la branche Sécurité informatique de l'Agence estonienne des systèmes informatiques, la Commission d'assistance électorale des États-Unis, le centre finlandais du registre juridique, la Commission électorale centrale géorgienne, la chancellerie d'État de Lettonie, la Commission électorale centrale de Lettonie, la Commission électorale centrale de Lituanie, l'Institut national électoral du Mexique, la Commission électorale centrale de la République de Moldavie, le Conseil électoral néerlandais, l'Autorité électorale permanente de Roumanie, l'Autorité électorale suédoise et l'Agence suédoise pour les contingences civiles, la Commission électorale du Royaume-Uni, le Centre national de sécurité informatique du Royaume-Uni et les services de sécurité d'Ukraine.

Au sein même d'IDEA International, les apports et suggestions inestimables de nos collègues ont façonné la rédaction de ce guide. Mentionnons à ce propos Therese Pearce Laanela et Adina Trunk. Alyssa Bittner-Gibbs, Oliver Joseph, Dominika Michalak et Maryam Safi ont grandement contribué par leurs travaux de révision et prises de notes assidus.

Enfin, nous remercions le Réseau des compétences électorales (RECEF), Élections Québec et tout particulièrement Marie-Christine Ross et Simon Mélançon qui ont contribué à réviser la version française de cette publication.

Abréviations

AEP	Autorité électorale permanente (Roumanie)
CAE	Commission d'assistance électorale (États-Unis)
CEC	Commission électorale centrale
CEI	Commission électorale indépendante (Afrique du Sud)
CERT	Équipe d'intervention d'urgence informatique
CST	Centre de la sécurité des télécommunications (Canada)
DDoS	Déni de service distribué
DHS	Département de la Sécurité intérieure (États-Unis)
DoS	Déni de service
INE	Institut national électoral du Mexique
NCSC	Centre national de sécurité informatique
OGE	Organisme de gestion des élections
ONG	Organisation non gouvernementale

SE	Section des élections (Danemark)
SSSCIP	Service d'État chargé des communications spéciales et de la protection de l'information de l'Ukraine
TIC	Technologies de l'information et de la communication

Définitions et thématiques couvertes

Les *risques de sécurité informatique (cyber-risques)* ont trait aux menaces de pertes financières, de perturbations ou d'atteintes à la réputation d'une organisation en raison de défaillances concernant ses systèmes informatiques. Cette expression englobe aux fins du présent document les risques liés aux pratiques de désinformation – portant sur les autorités électorales ou les technologies électorales – susceptibles de se manifester même en l'absence de défaillances techniques.

La *sécurité informatique (cybersécurité)* consiste à protéger les systèmes, les réseaux, les logiciels et les données connectés à Internet de tout accès ou usage non autorisé. Dans le présent document, cette expression désigne également la sécurité des technologies hors ligne utilisées dans le cadre d'élections ainsi que la protection de l'intégrité du processus électoral contre les opérations de désinformation et les guerres d'influence.

Les *menaces informatiques* en contexte électoral comprennent les menaces contre tout type de technologie à des fins hostiles et/ou illégales en vue de nuire à l'intégrité du processus électoral.

La *collaboration entre organismes* se rapporte ici aux initiatives de coopération visant à prévenir et réduire les risques de sécurité informatique tout en réagissant aux incidents informatiques en période d'élections. Cette collaboration ne se limite pas nécessairement aux organismes gouvernementaux ; elle inclut un large éventail d'acteurs parmi lesquels les organismes de gestion des élections (OGE), les médias et plates-formes de médias sociaux, les partis politiques, les candidats aux élections, la société civile et d'autres parties prenantes électorales, ainsi que des

entités privées telles que les consultants et les fournisseurs de technologies électorales.

Les *vulnérabilités* sont des failles dans le processus électoral qui exposent ce dernier à des attaques présumées ou avérées. Ces failles peuvent être aussi bien technologiques (appareils, logiciels ou réseaux défectueux) que liées à des procédures inadaptées ou à des facteurs humains (formation du personnel insuffisante notamment).

Le présent document s'intéresse essentiellement aux risques et menaces en matière de sécurité informatique dans le cadre des processus électoraux, lesquels relèvent de la responsabilité des OGE. Parmi les différents risques, mentionnons les attaques menaçant la confidentialité, l'intégrité et l'accessibilité des données et des technologies liées aux élections. Un autre risque important consiste en la diffusion de fausses informations concernant les processus électoraux sur les médias sociaux et d'autres supports de publication en ligne.

1. Introduction

Certains pays, à l'instar de l'Estonie, la Géorgie et l'Ukraine, ont déjà été exposés à des menaces informatiques visant leurs processus électoraux, et ce, depuis au moins dix ans. Cependant, les incidents informatiques largement débattus et soupçonnés d'avoir influencé les élections présidentielles américaines de 2016 ont été l'un des éléments déclencheurs d'une plus grande attention et sensibilisation face à ces enjeux. Au bout de quelques mois, les discussions se sont multipliées sur les moyens à mettre en œuvre pour faire face aux risques croissants d'attaques informatiques en contexte électoral, aussi bien dans les jeunes démocraties que dans celles plus établies.

La tenue d'élections repose sur des combinaisons variées de processus manuels et technologiques. Il n'existe aucune technologie à l'abri des piratages ni aucune procédure manuelle entièrement viable. À partir de ce constat, il importe de gérer les élections en maîtrisant et en limitant les risques de manipulation grâce à l'adoption d'un certain nombre de mesures d'intégrité, d'audit et de contrôle. Si, aux quatre coins de la planète, les pays s'appuient depuis longtemps sur de bonnes pratiques pour veiller à l'intégrité des processus manuels avec bulletins papier, les récents événements mettent en lumière la nécessité de faire face aux risques de l'utilisation croissante des technologies en contexte électoral.

Il est souvent considéré à tort que seuls les pays dotés de systèmes de vote électronique et d'autres technologies de vote sophistiquées sont potentiellement exposés à des attaques informatiques. Rappelons toutefois que tous les processus électoraux reposent sur les outils des technologies de l'information et de la communication (TIC), qu'il s'agisse de l'enregistrement des électeurs ou encore du site Internet d'un OGE. Ainsi, bien que les risques de sécurité informatique, les moyens utilisés pour mener ces attaques et leurs auteurs varient selon les pays, les OGE – mais aussi les hauts fonctionnaires concernés, les agences de sécurité et les organismes d'assistance démocratique – s'accordent sur un point : il est

impératif d'accroître les investissements afin de mieux cerner, prévenir et limiter les risques que les nouvelles technologies font peser sur les processus démocratiques et électoraux.

Une autre idée préconçue voudrait que les OGE soient les principales – voire les seules – agences responsables des questions de sécurité informatique pendant les élections. Or, les menaces informatiques s'attaquant aux processus électoraux et démocratiques surgissent sous des formes diverses, sous la responsabilité de différents acteurs :

- les attaques informatiques menées contre les infrastructures électorales, visant à porter atteinte à la confidentialité, l'intégrité et l'accessibilité des technologies et données électorales ;
- les campagnes de désinformation menées dans le but de saper la crédibilité du processus électoral et des institutions démocratiques ;
- les attaques informatiques ciblant les parties prenantes électorales, les partis, les candidats, les médias et les campagnes ;
- les campagnes de désinformation visant à influencer le débat politique.

La simple application de mesures techniques d'atténuation par un OGE, ou toute autre entité, ne peut, de façon générale, suffire pour affronter ces menaces.

Les OGE se trouvent généralement responsables de la préservation de l'intégrité de leurs propres systèmes et à maintenir intactes la réputation et la crédibilité de leur institution. Le piratage informatique ciblant les parties prenantes électorales (partis politiques et candidats notamment) ainsi que les guerres d'influence accaparant le débat politique constituent généralement une zone grise relevant de la responsabilité gouvernementale. Dans certains cas, il n'existe pas de législation ou de mandat clairement défini pour la mise en place de contre-mesures.

Les gestionnaires d'élections et les parties prenantes concernées disposent rarement des ressources ou de l'expertise pour se prémunir face aux menaces informatiques sophistiquées. Les experts en sécurité informatique sont généralement peu au fait des questions électorales *stricto sensu*, et n'accorderont pas nécessairement le degré de priorité dû en matière de lutte contre les menaces visant le champ électoral. Ils auront plutôt tendance à se concentrer sur la protection informatique des infrastructures stratégiques, à savoir : les institutions militaires, les services publics ou encore, les acteurs économiques majeurs.

Une collaboration entre les organismes est nécessaire en vue de mettre en commun les ressources et l'expertise requises pour i) favoriser une compréhension mutuelle des sphères de responsabilité, des domaines de rencontre, des lacunes ou encore des points de contact ; et ii) bâtir un système de défense holistique contre

les attaques informatiques, aussi bien sur le plan national qu'international, visant les élections et les fondements mêmes de la démocratie.

La présente publication décrit les modèles de collaboration émergents entre les organismes, à la demande de nombreux acteurs des processus électoraux qui ont émis le souhait de bénéficier de telles données. Elle s'inscrit dans le sillon de divers événements et échanges organisés par IDEA International en lien avec la sécurité informatique en contexte électoral. Ces derniers se sont tenus à la suite d'une table ronde inaugurale autour de cette problématique (Wolf 2017), au cours de laquelle les représentants des commissions électorales et des agences de sécurité ainsi que des experts parlementaires et indépendants se sont penchés sur les moyens de faire face aux risques de piratage – perçus ou réels – en contexte électoral.

Le document aborde des problématiques soulevées dans le cadre d'un exercice plus général d'évaluation des besoins.

- Quelles sont les technologies utilisées dans le cycle électoral susceptibles d'être exposées aux menaces informatiques ?
- Pourquoi les menaces informatiques constituent-elles un enjeu sérieux même pour les pays ne recourant pas au vote électronique ou à des technologies électorales avancées comparables ?
- Quelles instances gouvernementales et entreprises privées faut-il impliquer ?
- Comment articuler la collaboration entre les différents acteurs ? Quelles doivent être leurs fonctions et responsabilités respectives ?
- Quels sont les cadres officiels (législation ou entente) requis pour favoriser, encourager ou faciliter la collaboration entre organisations ?
- Quelles mesures faut-il prendre ? À quel stade du cycle électoral ?

Les élections représentent une infrastructure nationale critique (ou essentielle) : quelles sont les implications pour les OGE et leur mission ? La publication s'appuie sur 20 études de cas menées auprès d'OGE et d'agences gouvernementales concernées par les questions électorales. Elle expose également la teneur d'une table ronde organisée en 2018 au cours de laquelle différents pays ont échangé sur leurs expériences en la matière, à commencer par l'Afrique du Sud, l'Autriche, l'Australie, la Belgique, la Bulgarie, le Canada, le Danemark, l'Estonie, les États-Unis, la Finlande, la Géorgie, la Lettonie, la Lituanie, le Mexique, la Norvège, les Pays-Bas, la République de Moldavie, la Roumanie, le Royaume-Uni, la Suède et l'Ukraine.

2. Les menaces informatiques au cours du cycle électoral

Les menaces informatiques peuvent mettre à mal l'intégrité électorale en exploitant des vulnérabilités techniques ou en créant un climat de suspicion autour desdites vulnérabilités. Les menaces informatiques se manifestent généralement de deux façons : a) attaques ciblant les technologies utilisées pendant le cycle électoral ; ou b) campagnes de désinformation sapant l'intégrité du processus électoral.

2.1. Attaques ciblant les technologies utilisées pendant le cycle électoral

Parmi les principales cibles du piratage informatique en contexte électoral, figurent : les dispositifs technologiques d'enregistrement des électeurs, les équipements destinés aux scrutins, les technologies utilisées pour le dépouillement des votes, les technologies d'agrégation et de transmission des résultats, les sites Internet publiant les résultats des élections et d'autres services en ligne liés aux élections, les messageries électroniques et les systèmes de communication institutionnels et privés, ainsi que les infrastructures nationales au sens large, notamment les systèmes d'administration en ligne ou encore les réseaux d'électricité et de communications.

Le piratage électoral peut s'exercer de façon indiscriminée ou ciblée. Ainsi, les parties prenantes peuvent être les cibles d'attaques délibérées ou les victimes du hasard. Les attaques indiscriminées ne nécessitent généralement pas un degré de sophistication technologique élevé et s'accommodent de ressources limitées. Il s'agit notamment d'attaques par déni de service (DoS), d'attaques de sites Internet

ou encore d'attaques de logiciels malveillants, éventuellement avec demande de rançon.

Les attaques DoS se manifestent notamment par la saturation des ressources en ligne moyennant des envois massifs de requêtes ralentissant ou rendant le service complètement inopérationnel. Ce type d'attaque ne s'introduit pas dans les systèmes visés et n'altère pas les données ; de même qu'il ne permet pas d'accéder aux informations confidentielles. Les dommages se traduisent par une impossibilité à accéder aux systèmes, entachant ainsi la réputation de l'institution attaquée. Les attaques DoS visent les sites Internet afin de les rendre inaccessibles, ou les systèmes de communication afin d'encombrer ou d'empêcher l'accès des utilisateurs aux communications. Dans certains cas, elles entraînent le blocage ou la saturation des téléphones mobiles, canaux de communication et dispositifs utilisés par le personnel responsable des processus électoraux (voir l'encadré 2.1). Si les attaques DoS proviennent d'une source unique, il est généralement aisé de bloquer cette dernière. Il est plus difficile de se prémunir contre les attaques par déni de service distribué (DDoS) : dans la mesure où elles proviennent de différentes sources, elles ne peuvent être repoussées que moyennant des ressources informatiques substantielles combinées à une coopération entre les partenaires technologiques et les fournisseurs de services Internet. Relativement simples à exécuter, les attaques DDoS, lancées avec succès ou non, sont incontestablement les offensives informatiques les plus courantes : rares sont les OGE qui n'en ont pas subi à ce jour. C'est ainsi que nombre d'OGE ont récemment mis en place des garde-fous pour se prémunir contre les attaques et y répondre.

Encadré 2.1. Indonésie : attaques informatiques ciblant le personnel de la commission électorale

Pendant les élections régionales indonésiennes de 2018, des attaques ont été lancées pour tenter de pirater la page des résultats de la Commission des élections générales et infiltrer les comptes Telegram et WhatsApp des hauts responsables de l'administration électorale en exploitant les failles des systèmes SMS sur mobile. Les auteurs ont tenté d'accéder à ces services et de bloquer leur utilisation afin d'influer sur le cours du processus électoral.

Les attaques de sites Internet peuvent se traduire par la modification de leur apparence ou la manipulation de leurs contenus. Les altérations visuelles sont souvent flagrantes et destinées à entacher la réputation des instances ciblées. Les manipulations de contenus sont quant à elles plus subtiles, visant à semer la confusion ; elles peuvent aboutir à la publication d'informations mensongères ou de faux résultats électoraux. Ces menaces profitent de vulnérabilités de sites Internet publics en vue d'accéder aux serveurs publics, mais atteignent rarement

les systèmes informatiques internes et ne se traduisent pas, en principe, par une manipulation des données internes de l'institution visée. Cela dit, quand elles aboutissent, les attaques sèment le doute et compromettent la crédibilité de l'entité. Les actes malveillants contre les sites Internet peuvent également conduire à des fuites de données personnelles lorsque les registres d'électeurs en ligne sont exposés.

Encadré 2.2. Ukraine : l'infrastructure en ligne de la Commission électorale centrale en proie à une longue série d'attaques

Les élections présidentielles et législatives ukrainiennes de 2014 ont été marquées par une salve d'attaques informatiques. Ces actions – notamment le lancement d'attaques DDoS et l'altération du site publiant les résultats électoraux – ont perturbé la transmission des résultats par les commissions électorales de districts. On a également observé des envois de logiciels malveillants et des attaques par hameçonnage. Une attaque DDoS similaire a été lancée contre la Commission électorale centrale et des candidats quelques semaines avant la tenue des élections présidentielles de 2019. Mais ces actes malveillants n'ont pas atteint leur objectif, à savoir influer sur les résultats, la Commission électorale ayant mis en place les mécanismes de défense appropriés.

Les logiciels malveillants et attaques avec demande de rançon ont des répercussions préjudiciables sur les élections en rendant inaccessibles des systèmes et des données essentiels (voir l'encadré 2.3). Leurs visées ne sont pas nécessairement politiques. Il arrive que les parties prenantes électorales soient les victimes fortuites de formes de piratage criminel ou financier. Au cours des dernières années, 12 % des menaces informatiques perpétrées dans le monde contre des processus démocratiques étaient de nature criminelle, sans réelle visée politique (CST 2019).

Encadré 2.3. Macédoine du Nord : la Commission électorale d'État de Macédoine du Nord victime d'attaques avec demande de rançon

Environ un mois avant la tenue des élections présidentielles de 2019 en Macédoine du Nord, les principaux systèmes TIC de la Commission électorale d'État ne fonctionnaient pas correctement. Ceci a compromis l'accès en temps voulu à l'information, la publication des comptes-rendus, des instructions et des décisions de séances, la vérification en ligne des données des électeurs dans le registre électoral, ou encore le registre en ligne des plaintes. Ces événements ont soulevé des questions quant à la sécurité des TIC au sein de la Commission. Aux dires de celle-ci, parmi les systèmes ciblés par la demande de rançon GEFEST 3.0, figuraient les serveurs de fichiers et de messagerie électronique, compromettant ainsi l'accès au registre des électeurs et à la base de données des fonctionnaires utilisée pour la désignation des comités électoraux (OSCE/BIDDH 2019).

Certaines attaques plus sophistiquées ciblent explicitement les systèmes internes ainsi que les données et les informations privées. La manipulation de telles données est généralement plus complexe qu'une offensive ciblant des ressources publiques en ligne. Et pour cause, les systèmes internes bénéficient souvent d'un degré de protection bien supérieur et ne sont pas directement accessibles depuis le réseau Internet. Le succès de telles attaques est le résultat de lacunes importantes en matière de sécurité des TIC ou de menaces persistantes sophistiquées, à la fois bien planifiées (en plusieurs étapes) et menées par des auteurs bien équipés, souvent des États-nations. Ces attaques peuvent se solder par des dommages particulièrement étendus et sévères. Leurs auteurs se concentrent sur une cible très précise, souvent individuelle, et utilisent les technologies avancées les plus récentes pour perpétrer leurs méfaits, à l'image des vulnérabilités *zero-day*, sans correctif connu au moment de leur emploi. Les menaces sophistiquées persistantes sont exécutées sur de longues périodes, jusqu'à ce qu'elles soient concluantes. Elles peuvent même cibler des systèmes non reliés au réseau Internet, en empruntant d'autres canaux (clés ou dispositifs USB infectés notamment).

Dans les organisations dont les vulnérabilités techniques sont faibles, l'obtention d'identifiants par le biais de l'ingénierie sociale est un mode d'attaque privilégié, de par sa simplicité et son taux de réussite. L'ingénierie sociale désigne notamment des procédés de manipulation psychologique visant à soutirer aux utilisateurs un accès aux systèmes et données ainsi que des mots de passe et autres identifiants. Cette pratique s'exerce en face-à-face ou plus généralement par voie téléphonique, ou encore via des procédés d'hameçonnage et de harponnage électroniques amenant insidieusement les destinataires à révéler leurs informations confidentielles ou à cliquer sur des liens les redirigeant vers des sites frauduleux, lesquels constituent le terreau du piratage et des attaques malveillantes.

Enfin, les attaques d'initiés incluent l'exploitation par des usagers ayant accès aux systèmes d'information électorale et ciblant délibérément les failles de ces systèmes. En général, ces attaques avancées ciblées se limitent à la manipulation des dispositifs suivants : i) systèmes de transfert et d'agrégation des résultats et services en ligne connexes (par exemple, registres des électeurs, partis ou candidats), et ii) dispositifs électoraux accessibles publiquement dont la technologie est utilisée dans les centres de vote (machines de vote et systèmes d'identification des électeurs notamment).

2.2. Les failles du système électoral

Les attaques informatiques communes exploitent les vulnérabilités découlant, entre autres, d'un manque d' « hygiène informatique ». Ce terme englobe a) le degré de formation et de sensibilisation des utilisateurs concernant les façons de préserver le bon fonctionnement du système et la sécurité informatique ; b) le degré d'obsolescence des technologies utilisées par les organisations, notamment selon la fréquence des contrôles et des opérations de maintenance effectués ; c) la mesure dans laquelle les procédures et principes existants sont adaptés à la gestion de nouvelles menaces informatiques et de leur évolution ; d) l'absence ou l'existence de frontières suffisamment marquées entre les systèmes internes et les systèmes reliés en ligne ; e) le degré de surveillance des membres du personnel ayant accès à des systèmes confidentiels, dans le but de réduire le risque d'attaques provenant de l'intérieur ; et f) l'efficacité des mesures de protection informatique des organisations face aux ressources et aux stratégies tenaces des pirates informatiques (voir l'encadré 2.4).

Encadré 2.4. Roumanie : formation à l'« hygiène informatique » pour les partis politiques

L'Autorité électorale permanente de la Roumanie a mis en place des programmes de formation en matière d'hygiène informatique destinés aux partis politiques du pays afin de protéger les informations confidentielles de ces derniers ainsi que les données relatives aux élections que la commission leur fournit. Toute attaque informatique ou fuite de données subie par un parti donnerait en effet l'impression que la commission électorale a également été touchée.

Certaines vulnérabilités propres aux processus électoraux entraînent des risques de sécurité informatiques inexistants dans le cadre d'autres fonctions gouvernementales. En raison de la nature périodique des élections, les bases de données et les technologies électorales sont régulièrement utilisées, réactivées et renforcées aux alentours des jours de vote. C'est pourquoi le suivi continu et la

gestion des risques posent beaucoup plus de difficultés dans ce domaine que dans d'autres. Le jour du vote constitue le « point critique de vulnérabilité » des technologies électorales. De nombreux systèmes, en particulier les systèmes informatiques des gouvernements, sont conçus de façon à demeurer inaccessibles durant quelques heures, voire quelques jours en cas d'attaque grave. Le jour du vote, les technologies doivent être opérationnelles : un maximum de dégâts peut être causé simplement en interrompant les systèmes et en créant la confusion durant ces heures critiques d'une élection.

Il est nécessaire de garantir non seulement la facilité d'accès, mais aussi la sécurité des technologies électorales, qui ne sont utilisées qu'à quelques années d'intervalle par des millions de citoyens. Bien que ces deux principes entrent souvent en contradiction, ils doivent être respectés afin de maintenir un certain équilibre. Il arrive que de multiples organismes gouvernementaux soient chargés de la mise en œuvre de processus électoraux complexes, tels que l'inscription sur les listes électorales, ce qui peut créer des failles exploitables par les pirates. Si les rôles et les responsabilités de chaque organisme ne sont pas clairement définis, la responsabilité finale en matière de sécurité informatique ne revient à aucun d'entre eux. Dans le cas d'OGE disposant de ressources financières et humaines ainsi que de compétences en informatique limitées pour élaborer et garantir le fonctionnement des technologies électorales, les systèmes et procédures établis peuvent être mal conçus ou peu sûrs.

La chaîne d'approvisionnement utilisée pour les technologies électorales est également susceptible de constituer une faiblesse du point de vue de la sécurité informatique. Enfin, les technologies électorales qui ont été mises au point sur mesure, parfois par des fournisseurs étrangers, peuvent comporter de manière intentionnelle ou accidentelle des logiciels malveillants ou des vulnérabilités.

2.3. Perception de l'intégrité des processus électoraux et désinformation

La désinformation consiste à faire circuler, de façon délibérée et souvent clandestine, des informations fausses, trompeuses ou inexactes dans le but d'influencer l'opinion publique à des fins malveillantes. Dans le cadre des élections, la désinformation peut être l'œuvre d'acteurs nationaux ou internationaux. Les acteurs étrangers peuvent s'en servir en tant qu'outil d'influence (renseignements), procédé traditionnellement militaire qui est de plus en plus souvent appliqué dans le contexte d'élections. Les opérations de désinformation fournissent souvent une représentation exagérée ou erronée de sujets de débat publics. Conformément à leur mandat, les OGE ne peuvent prendre des mesures de lutte contre les campagnes de désinformation que dans les cas où celles-ci concernent spécifiquement les processus électoraux et leur gestion.

La désinformation en tant qu'outil de campagne électorale ne sera pas étudiée dans ce document, car elle échappe généralement au champ d'action des OGE (voir l'encadré 2.5). L'étendue de la réglementation, de la législation, des mesures d'autoréglementation et des codes de conduite qui devraient s'appliquer dans ce cas fait encore débat, un équilibre prudent devant être assuré entre la prévention de la désinformation et la protection de la liberté d'expression. Il est également nécessaire de distinguer ce qui est illégal de ce qui relève de campagnes légitimes dans les activités menées en ligne. En 2019, seuls quelques pays avaient légiféré au sujet des fausses informations ou envisagé l'adoption de lois y étant liées (Poynter Institute, 2018).

Encadré 2.5. Lettonie : piratage d'un média social et rôle de l'équipe spéciale de lutte contre la désinformation

Le 6 octobre 2018, jour des élections législatives, un réseau social letton populaire appelé Draugiem a été piraté. Une déclaration en russe proclamant « Camarades lettons, ce message vous est adressé. Les frontières de la Russie ne connaissent pas de limites » et accompagnée d'images montrant des soldats russes en Crimée et des parades militaires russes à Moscou a été publiée. L'origine du piratage n'a pas été clairement identifiée.

Draugiem étant une entreprise privée, les institutions gouvernementales n'étaient pas dans l'obligation de fournir une réponse formelle. Cependant, l'équipe spéciale de lutte contre la désinformation du pays a jugé important de s'assurer que les médias rendent compte de l'incident de manière nuancée afin d'éviter de donner une mauvaise image du processus électoral au public. Elle a donc agi sur trois fronts en : a) demandant à l'équipe d'intervention de l'agence responsable de la cybersécurité de procéder immédiatement à une enquête sur le piratage ; b) annonçant publiquement que le piratage n'avait eu aucun impact sur les élections ; et c) sensibilisant les décideurs politiques de plus haut niveau à l'importance des risques encourus afin de garantir une réponse politique appropriée. Par conséquent, la réaction des médias traditionnels et du public a été mesurée, et il a généralement été jugé que le système électoral du pays était sûr.

Deux types d'activités de désinformation sont d'intérêt pour les OGE, parce qu'elles visent à influencer le déroulement des élections. Ces opérations recourent souvent à des outils en ligne et aux médias sociaux pour cibler les électeurs. Premièrement, elles peuvent viser à réduire le taux de participation, par exemple en prétendant que les bureaux de vote sont fermés ou que les élections ont été reportées en raison du mauvais temps, de violences ou d'autres facteurs, ou en affirmant qu'il est possible de voter en ligne ou par téléphone lorsque ce n'est pas le cas (voir l'encadré 2.6).

Encadré 2.6. Canada : menaces intérieures

En 2011, le Canada a été secoué par le scandale des appels automatisés (scandale Robocall), au cours duquel des milliers d'électeurs de presque toutes les 250 circonscriptions du pays ont signalé avoir reçu des appels automatisés affirmant à tort qu'un autre lieu de vote leur avait été assigné. Cette opération de désinformation avait pour objectif de limiter le taux de participation aux élections. Les enquêtes conduites par Élections Canada ont conclu que des acteurs politiques nationaux étaient à l'origine de cette attaque. L'organisme a ainsi décidé de mettre en place un Bureau de l'intégrité électorale afin d'identifier les menaces informatiques nationales et internationales, d'évaluer les risques et de concevoir des systèmes de prévention et de suivi des attaques provenant d'acteurs étrangers, d'agents politiques ou d'individus cherchant à perturber les élections ou à en trafiquer les résultats.

Deuxièmement, les opérations de désinformation peuvent viser à éroder la confiance du public dans les institutions, les technologies électorales et les processus électoraux en faisant circuler des rumeurs de manipulation et d'activités malveillantes. Dans les cas où le niveau de confiance envers l'intégrité des processus électoraux est traditionnellement élevé, le simple fait de souligner des défauts mineurs peut suffire à entraîner une grave détérioration de cette perception (voir l'encadré 2.7).

Encadré 2.7. Mexique : campagne de désinformation sur le processus électoral

Verificado, une initiative de vérification des informations mise en place pour les élections de 2018 au Mexique, a permis de repérer différentes fausses affirmations à propos de la gestion de l'élection et du processus électoral (Verificado, 2018). Celles-ci comprenaient notamment des instructions pour marquer les bulletins de vote erronées, visant à rendre les votes nuls, ainsi que des rumeurs à propos de règles qui permettraient de voter à la place de parents décédés et de défauts ou de violations concernant la sécurité des bulletins. Les accords conclus par l'institution électorale nationale avec des fournisseurs de technologies pour protéger le système électoral contre les tentatives de piratage ont même été faussement perçus comme cédant la responsabilité de contrôler les résultats officiels aux entreprises privées et à leurs propriétaires.

Les technologies électorales peuvent facilement constituer la cible de campagnes de désinformation lorsque leurs particularités sont mal connues du public et des autres parties prenantes électorales. Ce type de désinformation peut consister à répandre des rumeurs proclamant que les technologies électorales sont mal protégées et peuvent être piratées (ou l'ont été), dépeignant de manière

exagérée des défauts et atteintes à la sécurité techniques mineurs ou fournissant des informations délibérément trompeuses. Donner l'impression que la sécurité informatique est menacée peut causer des dégâts aussi importants que les opérations qui s'attaquent au système en lui-même (voir l'encadré 2.8).

Encadré 2.8. Pays-Bas : chercher à nouer une collaboration entre organismes sous l'œil du public

Quelques semaines avant les élections générales de 2006, les Pays-Bas ont été forcés d'abandonner le vote électronique après qu'un groupe néerlandais de pirates à « chapeau blanc » défavorables à ce procédé a démontré les risques de sécurité auxquels les machines de vote du pays étaient exposées. Depuis, les autorités électorales des Pays-Bas font face à une lutte difficile concernant l'usage d'outils électroniques dans les processus électoraux, et ce même après avoir réinstitué le vote et le dépouillement manuels. En 2017, des pirates à « chapeau blanc » ont de nouveau affirmé que le logiciel utilisé par les municipalités pour compiler et calculer les résultats des élections ne bénéficiait pas d'un niveau de protection suffisant. Le ministère de l'Intérieur a par conséquent interdit l'emploi de ce logiciel deux semaines avant les élections, malgré les protestations de la commission électorale et des municipalités. Ces épisodes illustrent à quel point il est difficile d'assurer une collaboration continue entre différents organismes sur le devant de la scène publique.

Les technologies trop ambitieuses ou impossibles à mettre en place demandées par des parties prenantes électorales peuvent créer des attentes démesurées dans l'opinion publique. Cela peut mener les partis à se livrer une guerre de l'information concernant l'efficacité réelle ou perçue des mesures de sécurité informatique du pays. Un manque de compréhension ou des défauts de fonctionnement peuvent entraîner l'instrumentalisation des technologies électorales dans le but de saper la crédibilité des élections, ou rendre impossible leur organisation dans les délais appropriés en raison de contraintes financières, techniques ou de temps.

Les attaques visant à divulguer des informations confidentielles au sujet des parties prenantes électorales consistent à la fois en des piratages informatiques et des opérations d'influence. Les OGE doivent être particulièrement conscients des risques de fuite de données pesant sur les parties prenantes qui disposent d'un accès privilégié aux informations relatives aux élections, telles que les listes électorales et les résultats provisoires. La protection contre ce type de fuites de données représente l'un des domaines potentiels de coopération entre organismes et de prise de mesures conjointes entre les OGE, les autres organes gouvernementaux et les parties prenantes électorales.

Tableau 2.1. Classification des menaces informatiques liées aux élections

Attaques informatiques générales (dont les élections peuvent être une cible parmi d'autres)	Attaques informatiques visant spécifiquement les processus électoraux	Failles propres aux processus électoraux	Désinformation et opérations visant à influencer la perception de l'intégrité électorale
Attaques par déni de service (DoS)	Attaques exploitant des vulnérabilités *zero-day*	Nature périodique des élections	Divulgation de données confidentielles
Altération de sites Internet, manipulation de leur contenu	Ingénierie sociale, hameçonnage	Jours d'élections, en tant que point critique de vulnérabilité	Désinformation visant les technologies électorales
Opérations générales de piratage menées pour des raisons criminelles ou financières	Saisie et manipulation de données électorales	Technologies utilisées à quelques années d'intervalle seulement, mais par des millions de personnes	Désinformation concernant le processus électoral
Exploitation d'un manque d'hygiène informatique, par exemple, piratage de mots de passe trop faibles	Piratage des technologies électorales	Ressources limitées pour le maintien du bon fonctionnement des technologies électorales	Projets de technologies électorales impossibles à mettre en œuvre
	Attaques provenant de l'intérieur	Processus complexes, souvent partagés entre différents organismes	Désinformation dans le cadre de campagnes électorales

2.4. Les entités adverses

Depuis les élections présidentielles de 2016 aux États-Unis, de nombreux pays considèrent que la principale menace planant sur la sécurité informatique de leurs élections provient d'autres États qui tenteraient d'influencer leurs processus électoraux nationaux. Le droit international s'applique également à l'espace numérique : au regard de la loi, le piratage d'élections constitue un « fait internationalement illicite » et une violation de la souveraineté qui requiert une réponse de la part de l'État touché. Cependant, il est très difficile d'identifier la provenance des piratages et de prouver que des organismes d'États étrangers en sont à l'origine. D'autres types d'adversaires cherchent à employer des technologies afin d'influencer les résultats d'une élection, qu'il s'agisse d'acteurs politiques nationaux œuvrant dans le cadre d'une campagne électorale, de hacktivistes dont les actions visent à promouvoir un programme politique ou des changements sociaux (y compris en démontrant leur manque de confiance en des technologies électorales existantes) ou de terroristes recourant à des opérations cybernétiques.

Hormis les acteurs politiques, les entités adverses peuvent comprendre des groupes criminels organisés cherchant à influencer les élections, des cybercriminels s'attaquant aux systèmes pour en retirer des gains financiers ainsi que des individus ou des groupes dont le piratage vise à faire étalage de leurs talents ou à les faire gagner en popularité et en notoriété.

Les pirates sont souvent classés en trois catégories, selon leurs raisons d'agir et leur propension à recourir à des méthodes illégales. Les pirates à chapeau noir (*black hat hackers*) sont mal intentionnés et conduisent des opérations dans leur propre intérêt et dans le but de nuire à leurs cibles. Les pirates à chapeau blanc (*white hat hackers*) sont bienveillants et motivés par des raisons éthiques ; ils agissent au moyen de méthodes légales et se voient souvent attribuer des contrats pour tester des systèmes afin de détecter des failles de sécurité qui pourront ensuite être corrigées. Ces pirates n'exploitent ni ne dévoilent au grand jour les faiblesses qu'ils découvrent avant que les institutions n'y remédient. Les pirates à chapeau gris (*grey hat hackers*) peuvent parfois enfreindre la loi, mais n'exploitent pas les failles qu'ils décèlent.

N'importe quel type de pirate peut avoir une incidence négative sur l'intégrité des processus électoraux. Malgré leurs bonnes intentions, même les pirates bienveillants peuvent considérablement détériorer l'intégrité d'un processus électoral s'ils rendent leurs découvertes publiques de façon imprudente et irresponsable, par exemple peu avant une élection, dans un délai insuffisant pour que les autorités puissent corriger les défauts soulignés, ou en exagérant la gravité d'une faille pour attirer davantage d'attention. Certains événements, tels que le DefCon Voting Village aux États-Unis (DefCon, 2017 ; DefCon, 2018), fournissent l'occasion de promouvoir l'amélioration des technologies électorales, mais sont aussi susceptibles de mettre à mal la crédibilité des élections.

Tableau 2.2. Entités adverses pouvant avoir une incidence négative sur l'intégrité des processus électoraux

Visée politique	Visée non politique
États étrangers	Groupes criminels organisés
Acteurs politiques nationaux	Criminels recherchant des gains financiers
Hacktivistes	Individus
Terroristes	

2.5. Les mesures d'atténuation

Bien que ce document ne vise pas à fournir une liste détaillée des mesures potentielles d'atténuation des risques de sécurité informatique, les aspects communément abordés dans ces dernières comprennent :

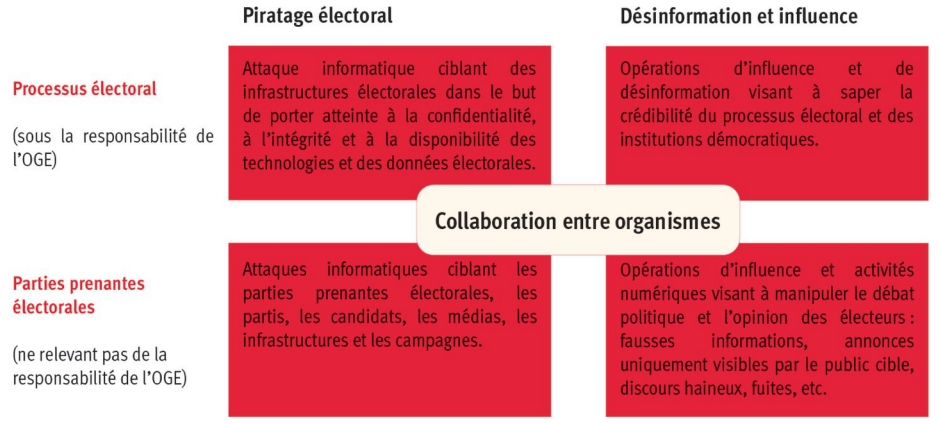
- *Assurer la sécurité des technologies* en procédant régulièrement à des contrôles, à des audits et à des mises à jour des technologies et des procédures, en plus de les renforcer au moyen de copies et de systèmes de sauvegarde. Il peut notamment s'agir d'instaurer des canaux de transfert d'informations de secours, de concevoir des systèmes de cryptage et d'identification de pointe, de créer des « zones tampons » (*air gapping*) en établissant la séparation la plus stricte possible entre les technologies essentielles et le réseau Internet, et de surveiller en permanence toutes les infrastructures critiques.
- *Contrôler et évaluer la qualité* des procédures électorales à différents niveaux, en incluant une copie des composantes essentielles, notamment par la double saisie des données et leur vérification d'après des documents manuscrits ou par téléphone. Surveiller la bonne mise en œuvre de ce type de mesures.
- *Veiller à garantir la sécurité informatique tout au long de la chaîne d'approvisionnement*, notamment par l'évaluation et la sélection minutieuse de fournisseurs et de vendeurs de confiance.
- *Investir dans les ressources humaines,* la formation du personnel et l'hygiène informatique, en définissant des rôles et des responsabilités claires pour chacun, en adoptant un principe de « double vérification » visant à ce qu'aucune procédure essentielle ne soit conduite par un seul membre du personnel et en examinant les antécédents des membres clés des institutions électorales ayant accès aux données administratives.
- *Surveiller les échanges en ligne* sur les médias sociaux publics, mais aussi sur le dark Web, sur les forums d'hacktivistes et sur d'autres plates-formes afin de détecter des signes de fuites de données ou de planification d'attaques coordonnées.
- *Définir une responsabilité pénale* en cas de fraude ou de manipulation électorales, et poursuivre en justice les contrevenants à la loi reconnus comme tels.

- *Entretenir une collaboration continue* au moyen d'échanges continus avec une multitude d'acteurs et de structures de communication interne et publique établie bien avant l'apparition de crises.

2.6. Les raisons d'être de la collaboration entre organismes

Alors que les entités adverses sont libres de choisir n'importe quel angle d'attaque, la mise en œuvre de stratégies de défense est bien plus complexe et fragmentée. Selon le contexte national, certaines menaces informatiques se trouvent sous l'autorité des différents niveaux de l'administration électorale ou d'autres agences gouvernementales, tandis que dans d'autres cas, ce sont le secteur privé et les partis politiques qui interviennent. Dans d'autres cas encore, ce sont les mesures d'autorégulation de l'industrie qui entrent en jeu. Dans les cas où les progrès techniques sont rapides et où la liberté d'expression est en jeu, aucune forme de régulation n'existe. C'est l'enchevêtrement de compétences et de responsabilités découlant de ces situations qui rend essentielle l'adoption d'une approche gouvernementale et d'une collaboration entre organismes en matière de sécurité informatique dans les processus électoraux.

Figure 2.1. Risques de sécurité informatique pesant sur les élections et champ d'action des OGE



3. Les modèles de collaboration entre organismes

Le présent document analyse les cas de collaboration entre organismes selon quatre facteurs principaux : a) le nombre et le type d'organismes impliqués ; b) les plates-formes de collaboration entre organismes ; c) la coopération entre les différents niveaux des OGE ; et d) la collaboration avec des organismes non étatiques. Le présent chapitre étudie chacun de ces facteurs l'un après l'autre.

3.1. Nombre et type d'organismes impliqués

Dans certains pays, la collaboration est assurée par un nombre réduit d'organismes. Les études de cas réalisées ont cependant permis de recenser un grand nombre d'organismes constituant des partenaires potentiels (voir le tableau 3.1). La collaboration peut se limiter aux organismes gouvernementaux, mais inclut souvent des agents non étatiques ou provenant de la société civile, des médias ou des partis politiques, ainsi que des candidats aux élections et des acteurs du secteur privé (voir l'encadré 3.1). Selon le contexte national, l'OGE peut remplir des fonctions de médiation ou servir de moteur à la collaboration.

Encadré 3.1. République de Moldavie : collaboration étroite avec les agences de sécurité en cas d'incidents informatiques

En 2014, la République de Moldavie a instauré, comme mécanisme de vérification supplémentaire, des listes électorales électroniques permettant d'enregistrer la venue des électeurs aux bureaux de vote. Au cours de sa première utilisation pour les élections générales de 2014, le système a cessé de fonctionner de manière inattendue pendant plusieurs heures. Bien que cette interruption ait été causée par un manque de serveurs de secours, des rumeurs affirmant qu'une attaque était survenue ont commencé à circuler peu après l'incident. La collaboration nouvellement établie entre la commission électorale centrale et les services de sécurité a toutefois rapidement porté ses fruits. Ces derniers ont promptement livré des serveurs supplémentaires au siège de la commission électorale, et les rumeurs d'attaque ont été publiquement démenties. Non seulement ces mesures ont permis à la commission de reprendre rapidement le contrôle des élections, mais elles ont également posé les fondations d'une relation de confiance entre ces organismes.

Tableau 3.1. Organismes susceptibles de participer à une collaboration en matière de sécurité informatique

Acteurs gouvernementaux	Acteurs non gouvernementaux
Membres de l'exécutif (cabinet ministériel, bureau du Premier ministre ou du président)	Presse écrite et audiovisuelle
Institutions de gestion des élections à différents niveaux	Fournisseurs de médias sociaux
Équipes chargées de la sécurité informatique au sein des institutions de gestion des élections	Partis politiques et candidats aux élections
Organismes administratifs responsables de l'inscription sur les listes électorales (si distincts des OGE)	Milieu universitaire
Organismes experts en sécurité informatique (par exemple, équipe d'intervention d'urgence informatique, centre pour la sécurité informatique, autorités responsables des systèmes d'information)	Entreprises privées du secteur des TIC
Organismes publics d'administration en ligne	Entreprises privées du secteur de la sécurité
Entreprises publiques fournissant des technologies électorales	Fournisseurs de logiciels utilitaires et d'infrastructures
Fournisseurs de certificats électroniques pour l'identification numérique	Pirates à chapeau blanc, hackers éthiques ou experts en sécurité numérique

Tableau 3.1. Organismes susceptibles de participer à une collaboration en matière de sécurité informatique (suite)

Acteurs gouvernementaux	Acteurs non gouvernementaux
Ministères : de l'Intérieur, de la Justice, de la Communication, de la Défense, des Affaires étrangères	
Organismes de sécurité publique	
Forces de police de différents niveaux	
Organismes de renseignement et de sécurité nationale	
Ministère public	

3.2. Les plates-formes et organes administratifs dédiés

Certains pays organisent la collaboration au moyen de plates-formes dédiées telles que des équipes spéciales, des groupes de travail, des projets spécifiques ou des organes administratifs (voir le tableau 3.2). Certaines équipes spéciales se réunissent selon les besoins, tandis que d'autres organisent régulièrement des forums afin d'échanger des informations. De nombreux pays disposent d'une seule équipe spéciale chargée de la sécurité informatique des élections. Cependant, l'Estonie a conclu qu'un modèle comprenant plusieurs petits groupes avec des objectifs spécifiques était plus efficace. Les États-Unis utilisent deux plates-formes, l'une pour la collaboration entre organismes gouvernementaux, et l'autre pour la collaboration avec le secteur privé.

Tableau 3.2. Exemples de plates-formes de collaboration entre organismes en matière de sécurité informatique

Pays	Plate-forme pour la sécurité informatique des élections
Australie	Équipe spéciale de protection de l'intégrité électorale
Bulgarie	Groupe interservices, sous la direction du Premier ministre Équipes spéciales conjointes de la commission électorale centrale (CEC) et du ministère de l'Intérieur pour la lutte contre les délits relatifs aux élections
Canada	Bureau de l'intégrité électorale
Danemark	Équipe spéciale interministérielle

Tableau 3.2. Exemples de plates-formes de collaboration entre organismes en matière de sécurité informatique (suite)

Pays	Plate-forme pour la sécurité informatique des élections
Estonie	Groupe de travail hebdomadaire sur les TIC Groupe de travail hebdomadaire chargé des relations publiques Groupes de travail sur les registres, les cartes d'électeur et les listes électorales Équipe spéciale pour le vote à l'étranger Équipe spéciale pour le vote par Internet
États-Unis	Conseil gouvernemental de coordination sectorielle pour les élections Conseil de coordination sectoriel
Géorgie	Groupe de travail conjoint de la CEC
Lettonie	Groupe de travail sur la sécurité informatique des processus électoraux Équipe spéciale de lutte contre la désinformation
Moldavie	Groupe de travail sur les services conjoints
Suède	Projet de lutte contre les opérations d'influence, coordonné par l'agence pour la protection civile
Ukraine	Commission conjointe de l'OGE et des services de sécurité sur la sécurité informatique

3.3. La coopération entre les différents niveaux des OGE

Les pays qui disposent d'un OGE central chargé de l'organisation à tous les niveaux des élections, y compris des opérations de vote dans les bureaux de vote, rencontrent généralement moins de difficultés dans l'application homogène de mesures de sécurité informatique sur l'ensemble de leur territoire. Dans les pays qui ont recours à un modèle décentralisé, des OGE indépendants et locaux administrent directement les opérations électorales sur le terrain. Cependant, l'opinion publique (voire certains responsables politiques) a tendance à imputer la responsabilité finale à l'autorité électorale centrale en cas d'incident à l'échelle locale. L'autorité centrale est donc régulièrement blâmée pour les erreurs survenant dans le cadre des processus électoraux, ce qui écorne chaque fois un peu plus son image.

Les modèles d'OGE décentralisés requièrent donc d'instaurer ou de renforcer des mesures de coopération et de soutien entre les différents organismes. Il peut également être nécessaire d'atténuer les appréhensions que la supervision nationale d'activités locales peut susciter. Dans le cas d'un modèle décentralisé, la collaboration entre organismes vise, le plus souvent, à assurer la coordination et le développement d'une relation de confiance entre les autorités locales de gestion des élections et différents organismes d'envergure nationale, des OGE nationaux aux agences de sécurité.

3.4. La coopération avec des acteurs non gouvernementaux

Le secteur privé, qui comprend les fournisseurs de technologies électorales et les prestataires de services de télécommunications ou d'analyse des risques, constitue un partenaire important pour la plupart des OGE dans le cadre de l'entretien des technologies, de la conduite d'audits de sécurité ainsi que de la proposition et du soutien à la mise en œuvre de contre-mesures. Dans certains pays, la collaboration entre organismes inclut des fournisseurs de logiciels utilitaires dans le but de minimiser les risques d'interruption de fonctionnement des services en amont et en aval du vote.

Afin de garantir l'exécution des plans de communication, même en cas d'attaque, il est essentiel d'échanger avec les médias et, également, avec les fournisseurs de médias sociaux. Les entretiens conduits lors des études de cas réalisées dans le cadre du présent document révèlent que le degré de collaboration avec les fournisseurs de médias sociaux varie grandement d'un pays à l'autre. Alors que plusieurs pays, par exemple le Mexique, ont conclu des mémorandums d'entente formels, certains OGE se tiennent largement à l'écart des médias sociaux. Les grands pays dotés de mécanismes de collaboration et de services solidement établis font preuve de bonne volonté et disposent de meilleures capacités de coopération avec les fournisseurs de médias sociaux. De leur côté, les pays plus petits ou les marchés moins importants n'ont pas les mêmes capacités à établir des ententes avec les fournisseurs de médias sociaux.

Les partis politiques et les candidats font l'objet de piratages relatifs aux élections non seulement en raison de leur rôle central dans la vie politique, mais aussi parce qu'ils constituent souvent les acteurs les plus vulnérables du système électoral. Ce constat est d'autant plus vrai dans les cas où il existe un grand nombre de partis politiques et où les ressources investies dans la sécurité des technologies sont insuffisantes. Il est possible et bienvenu pour les OGE, ou d'autres organismes gouvernementaux, de conseiller les partis politiques en matière de sécurité informatique. Cette capacité varie grandement d'un pays à un autre. Il est recommandé prévenir les partis politiques des ravages potentiels des attaques informatiques tout comme de les informer du soutien que les OGE et les autres organismes gouvernementaux pourraient leur fournir s'ils devaient être la cible d'une attaque informatique. L'accès privilégié aux données électorales dont les partis peuvent être dotés, notamment aux listes électorales ou aux résultats préliminaires, requiert également d'être assorti de conditions et d'instructions concernant la protection de ces données.

Le milieu universitaire joue un rôle important dans le cadre de la sécurité informatique des élections. Par exemple, des experts en technologie ou des hacktivistes peuvent alerter les parties prenantes au sujet des risques posés par le manque de prise au sérieux de la sécurité des TIC en contexte électoral. Ces

acteurs sont la source de nombreuses contributions, notamment en formulant des suggestions concernant les façons d'améliorer les systèmes informatiques, ainsi qu'en réalisant des démonstrations publiques de failles existantes dans les processus électoraux en place. Établir des relations constructives avec ces experts, à condition que leurs intentions et leurs modes opératoires soient transparents, peut contribuer à renforcer les systèmes et à limiter les risques de détérioration de la réputation des organismes responsables des processus électoraux. Certaines institutions universitaires ont pris l'initiative de nouer des partenariats en matière de sécurité informatique avec les administrateurs électoraux et apportent leur soutien aux parties prenantes électorales en fonction des résultats de leurs recherches. Par exemple, le Centre Belfer pour la science et les affaires internationales de la Harvard Kennedy School est à l'origine du rapport *The Cybersecurity Campaign Playbook* (2018a, 2018b). Dans le même ordre d'idées, la DefCon, une convention annuelle consacrée au piratage, basée aux États-Unis, s'est intéressée à la sécurité informatique des élections et a publié le rapport *Voting Machine Hacking Village Report on Cyber Vulnerabilities in the U.S.* (DefCon 2017 ; DefCon 2018). Dans des pays d'Amérique latine tels que le Mexique et le Venezuela, des institutions universitaires font partie d'un organisme indépendant de contrôle et d'évaluation des technologies électorales qui favorise leur amélioration et renforce la confiance de la population en ces technologies. Enfin, en Indonésie, des acteurs du milieu universitaire jouent un rôle essentiel dans la conception de technologies électorales.

4. La mise en œuvre de la collaboration entre organismes

Dans le cadre d'une approche gouvernementale exhaustive en matière de sécurité informatique des processus électoraux, la collaboration entre organismes vise généralement à atteindre les objectifs principaux suivants : protéger les données confidentielles relatives aux élections, telles que les listes électorales, les courriels et les documents internes ; préserver l'accessibilité et l'intégrité des technologies électorales ; défendre l'intégrité des élections contre les campagnes de désinformation ; obtenir les ressources, les contributions d'experts, les financements et l'appui institutionnel et juridique requis pour l'instauration des mesures nécessaires ; et renforcer la sécurité informatique des parties prenantes électorales.

4.1. Les domaines de collaboration

Les organismes peuvent notamment collaborer pour :

1. *Organiser la communication entre organismes*, en commençant par l'élaboration d'un répertoire d'interlocuteurs et de personnes à contacter en cas d'urgence pour chaque entité participante, suivie de la conclusion d'accords généraux concernant l'attribution des rôles, le fonctionnement de la coordination et la prise de décisions. Afin de renforcer ces partenariats, les organismes devraient maintenir des échanges réguliers au moyen de canaux de communication, notamment en établissant des équipes spéciales, des groupes de travail et d'autres plates-formes de collaboration similaires. Il est tout aussi important de nouer des relations

professionnelles et de confiance entre les organismes participants et de surmonter les différences de culture organisationnelle que d'assurer la collaboration en elle-même.

2. *Évaluer conjointement les risques et prendre conscience de la situation* au moyen de procédures menées par de multiples organismes comprenant des échanges d'informations, l'élaboration de rapports de situation et la construction d'une expertise partagée au sujet des sources de vulnérabilité et de leur évolution pendant et entre les périodes d'élections (voir l'encadré 4.1). Le suivi coordonné des médias et des médias sociaux, ainsi que le partage de renseignements entre organismes compétents peuvent également constituer de précieuses contributions.

Encadré 4.1. Finlande : partage d'informations et conscience de la situation

En Finlande, le centre du registre juridique organise des réunions avec différents organismes à intervalle irrégulier. La sécurité informatique ne constitue que l'un des sujets abordés au cours de ces réunions de coordination relatives aux élections, qui assurent un suivi en temps réel des risques et définissent des mesures d'atténuation fondées sur l'évaluation des menaces, ainsi que sur les informations existantes. Les risques de sécurité informatique sont évalués de façon continue et à l'occasion de chaque processus électoral, en tenant compte de l'évolution récente du contexte international.

3. *Coordonner la communication publique et informer les électeurs*, ce qui constitue une composante essentielle visant à prévenir les menaces informatiques. Les menaces réelles étant tout aussi importantes que les menaces perçues, il est nécessaire de mettre en place une stratégie de communication publique cohérente et coordonnée. Les plans de communication publique doivent chercher à informer les électeurs en amont des élections, notamment en cas d'incident, en leur transmettant des informations vérifiées en continu.
Les méthodes adoptées par les organismes participant à ces plans de communication varient grandement. Certains pays préfèrent ne pas mettre en avant le sujet de la sécurité informatique afin d'éviter d'inquiéter leurs citoyens, tandis que d'autres considèrent qu'une population sensibilisée et instruite représente la meilleure défense contre une attaque. Quelle que soit l'étendue des activités de communication publique, tous les organismes concernés devraient élaborer une stratégie conjointe en la matière et communiquer d'une seule voix au sujet des menaces et des contre-mesures adoptées avant (ou pendant) d'éventuelles crises.

Il convient d'établir des canaux de communication efficaces avec les médias afin de transmettre les informations importantes dans les délais appropriés. Cet aspect requiert de plus en plus souvent de conclure des accords formels avec les principaux fournisseurs de médias sociaux afin d'informer les électeurs et de s'assurer que les fausses informations concernant les processus électoraux sont rapidement rectifiées. À titre d'exemple, les OGE peuvent effectuer des annonces à forte visibilité afin de rétablir la vérité. Par exemple, l'OGE du Mexique a signé en 2018 un mémorandum d'entente avec Twitter et Facebook (INE, 2018 ; *El Universal,* 2018).

4. *Créer des mécanismes de prévention et de réponse* fondés sur les risques identifiés. Il est possible de soutenir et de conseiller les parties prenantes électorales concernant les mesures de prévention et d'atténuation de ces risques, ainsi que de les aider à mettre en place des plans d'urgence en cas d'attaque informatique. À cette fin, des protocoles prévoyant les circonstances dans lesquelles un OGE doit transmettre la gestion d'un incident aux organismes de sécurité ou aux décideurs politiques peuvent être mis en place. La gestion efficace des problèmes émergents est essentielle pour préserver la confiance de la population.

Encadré 4.2. Estonie : préserver la confiance au sein d'une société numérique

Bien que l'Estonie fasse partie des démocraties qui utilisent le plus de technologies numériques au monde, les attaques informatiques ne représentent pas une menace importante aux yeux de son OGE. La petite taille du pays constitue un avantage : avec seulement 1,3 million d'habitants, le personnel de l'OGE peut trouver, avec une certaine facilité, des partenaires dans d'autres organismes pour l'aider à assurer la sécurité des technologies électorales. L'OGE estonien cherche donc davantage à maintenir sa stricte impartialité politique afin de s'assurer le soutien des partis et la confiance de l'électorat concernant le vote électronique. Il vise également à aider les candidats et les jeunes électeurs à faire un usage responsable des technologies. Dans une société largement numérique, la confiance de la population forme le socle de la sécurité informatique.

5. *Acquérir et partager des connaissances, des outils et des ressources* en matière de sécurité informatique, y compris des programmes de formation et des directives telles que le >recueil de l'Union européenne sur la cybersécurité des technologies électorales (groupe de coopération en matière de SRI, 2018) ou les ressources en matière d'organisation de la sécurité des

élections de la commission d'assistance électorale des États-Unis (U.S. CAE, s.d.).

6. *Effectuer des évaluations et délivrer des certificats* concernant les mesures de sécurité adoptées par l'OGE au moyen d'un autre organisme gouvernemental indépendant (voir l'encadré 4.3).

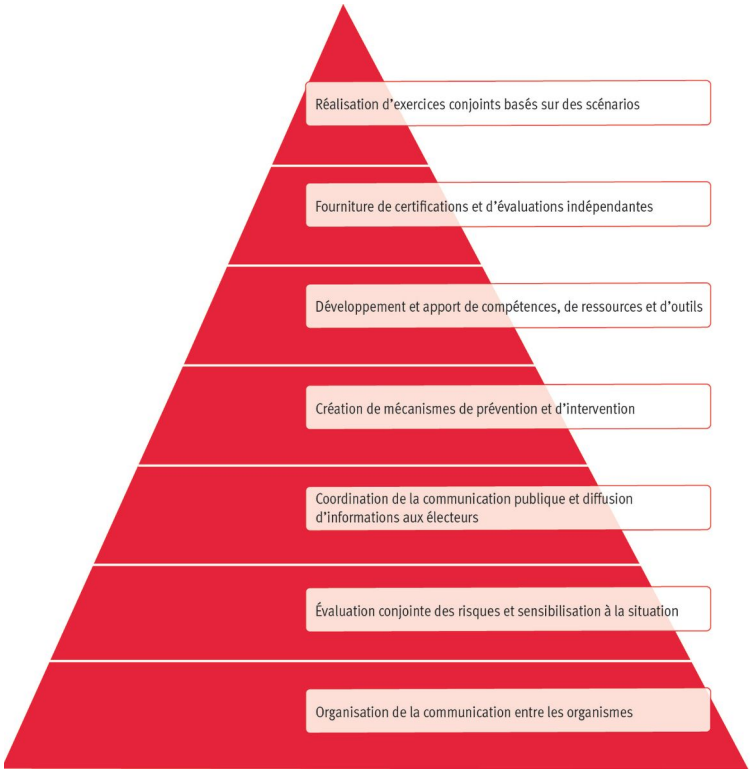
Encadré 4.3. Ukraine : collaboration entre la commission électorale centrale et d'autres autorités en matière de certification et de suivi des technologies de l'information et de la communication électorales

En Ukraine, tous les systèmes d'information relatifs aux élections doivent être évalués par le gouvernement afin de recevoir un certificat de conformité avant leur utilisation par la commission électorale centrale. Le service national des communications spéciales et de la protection des données soumet les systèmes à des tests et évalue leur conformité aux termes de référence ainsi qu'aux exigences en matière de protection des informations. Des experts de ce service surveillent également les systèmes et les défendent contre d'éventuelles attaques au cours de leur utilisation.

7. *Effectuer des exercices conjoints fondés sur l'élaboration de scénarios*, ce qui constitue une forme plus avancée de collaboration entre organismes que seuls certains des pays étudiés ont mise en place. Ces simulations basées sur des scénarios de crise sont effectuées afin de tester l'efficacité des mécanismes d'intervention d'un pays. Elles sont conçues de manière à ce que les différents organismes concernés collaborent afin d'organiser les réponses aux crises potentielles, d'identifier les lacunes en matière de planification et de procédures, et de recueillir des retours d'information en vue d'améliorer les processus. Les exercices de simulation en salle, au cours desquels les participants discutent de leurs rôles et de leurs responsabilités dans le cadre de différents scénarios, présentent un rapport coût-efficacité plus intéressant et sont donc plus courants que les simulations d'incidents en conditions réelles.

Les différents stades de la collaboration entre organismes sont interdépendants, leur mise en œuvre progressive mène à l'adoption d'une approche plus exhaustive (voir la figure 4.1).

Figure 4.1. Les stades de la collaboration entre organismes



4.2. Préparer et faciliter la collaboration entre organismes

D'après les entretiens conduits dans le cadre des études de cas réalisées pour le présent document, les mesures de protection des élections contre les menaces informatiques sont encore en cours d'élaboration dans de nombreux pays. Bien que l'importance de la collaboration entre organismes soit de plus en plus reconnue, la conception et la mise en œuvre des mécanismes qui lui sont nécessaires ne font souvent que débuter.

4.2.1. Défis et limites

La collaboration entre organismes se heurte régulièrement à des défis, au nombre desquels figure le manque de compatibilité des cultures institutionnelles, en particulier entre les OGE et les services de sécurité, qui constitue un frein à la volonté de collaborer (voir l'encadré 4.4).

Encadré 4.4. Finlande : surmonter les divergences culturelles entre les organismes

Collaborer avec des organismes non conventionnels peut nécessiter d'opérer des changements aussi bien organisationnels que culturels, voire linguistiques. En Finlande, les organismes militaires et les services de sécurité considèrent que seules les cibles militaires peuvent être qualifiées d'« infrastructures essentielles » et donc nécessiter leur intervention en cas d'attaque. Lorsque le pays a renoncé à recourir au vote électronique en 2017 pour des raisons de sécurité, ces organismes ont décidé que les élections ne relevaient plus de leur responsabilité. Malgré ces divergences culturelles intrinsèques, le centre du registre juridique, organe technique de l'OGE finlandais, s'est adressé aux agences du secteur de la sécurité afin qu'elles contribuent à assurer la protection d'autres processus informatiques, tels que la gestion des listes électorales et le calcul des résultats. L'agence pour la sécurité informatique et la police judiciaire se sont montrées particulièrement réceptives. Depuis lors, l'OGE a conclu que, même sans la désignation officielle « infrastructures essentielles », la mise à disposition des fonds nécessaires et le fait d'encourager les institutions à s'impliquer davantage pouvaient produire des résultats positifs.

Les pays disposant d'un modèle de gestion des élections indépendant peuvent éprouver des difficultés à préserver l'indépendance de leur OGE, qu'elle soit réelle ou perçue, dans le cadre d'une étroite collaboration avec des organismes de sécurité (voir l'encadré 4.5). Plus particulièrement, doter d'autres agences gouvernementales d'un accès aux infrastructures technologiques des élections pour en évaluer la sécurité ou exiger des habilitations pour le personnel des services électoraux peut déclencher des controverses. En effet, cela accroît le risque que les agences responsables de ces vérifications acquièrent une influence indue sur la composition de l'administration électorale et un accès inapproprié aux données et systèmes électoraux.

Encadré 4.5. Roumanie : la solidité d'une collaboration étroite en matière d'audit face aux débats suscités par la coopération avec les services de renseignement

L'autorité électorale permanente de la Roumanie bénéficie d'une collaboration complète et éprouvée avec d'autres agences gouvernementales et le secteur privé. Elle a par exemple travaillé en étroite collaboration avec l'équipe d'intervention d'urgence informatique dans le cadre d'audits de sécurité, ainsi qu'avec les institutions du ministère de la Défense responsables de fournir des infrastructures sûres pour les télécommunications et les serveurs. Les services de renseignement roumains sont chargés de veiller à la sécurité informatique de toutes les infrastructures d'État, y compris celles relatives aux élections. Cependant, les abus de pouvoir dont ils ont fait preuve par le passé rendent leur coopération avec d'autres organismes gouvernementaux controversée.

Les limites des mandats et des compétences des organismes peuvent également être un obstacle au renforcement de leur collaboration. Lorsque les ressources à disposition sont restreintes ou les risques de retombées politiques trop élevés, les organismes qui ne sont pas directement affectés à la gestion des élections peuvent se montrer particulièrement réticents à faire de la sécurité électorale leur priorité.

4.2.2. Les approches horizontales et verticales

L'adoption d'approches tant horizontales que verticales peut favoriser la collaboration entre organismes et contribuer à surmonter les difficultés qu'elle entraîne.

Encadré 4.6. Danemark : petits moyens, grandes ambitions – la collaboration informelle comme point de départ

À ses débuts, la collaboration entre organismes au Danemark a bénéficié à la fois de l'absence de pression médiatique forte et d'une récente augmentation de budget qui ont favorisé l'instauration d'un climat de confiance. La forme de collaboration intersectorielle et en partie informelle qui a été adoptée par la suite a depuis démontré son efficacité. Les structures hiérarchiques sont demeurées simples et de nombreuses initiatives ont été prises sur le terrain. Cette approche a permis aux informations qui en provenaient d'être rapidement transmises aux décideurs concernés. Le fait que le personnel d'encadrement se réunisse au besoin, plutôt que dans le cadre de procédures formelles ou d'organismes nouvellement établis, a garanti un sentiment d'appropriation ainsi qu'une forte volonté de collaborer.

Les approches horizontales signifient que les organismes prennent eux-mêmes l'initiative de collaborer, ce qui peut stimuler l'adoption de solutions efficaces, pragmatiques et requérant peu de ressources. Les premières interactions, dont les OGE sont le plus souvent à l'origine, naissent de besoins spécifiques. Par la suite, les organismes échangent leurs coordonnées, organisent des réunions, facilitent l'établissement de relations de confiance et visent à remédier aux divergences institutionnelles. En fonction du contexte national, la collaboration informelle peut cependant nuire à la transparence des processus et avoir des répercussions négatives sur l'indépendance perçue de l'OGE.

Les approches verticales découlent quant à elles de décisions prises à haut niveau et sont régies par des cadres juridiques et des politiques. Elles peuvent renforcer la coopération existante et permettre de dépasser les limites des formes de collaboration moins formelles, notamment dans les cas où d'éventuels partenaires ne feraient pas de la mise en commun de leurs forces une priorité ou ne disposeraient pas des compétences nécessaires à cet effet. Un soutien officiel émanant de l'ensemble du gouvernement, par le biais de politiques de sécurité informatique et en reconnaissant les élections comme une infrastructure essentielle, peut permettre de débloquer des ressources supplémentaires et de définir des normes minimales applicables aux administrations électorales hautement décentralisées. Les approches verticales peuvent toutefois présenter l'inconvénient de susciter des inquiétudes et des résistances au sujet de la « mainmise du gouvernement » dans des pays au système très décentralisé, tels que les États-Unis.

Qu'il soit préférable d'adopter une approche horizontale, verticale ou mixte dépend de nombreux facteurs, notamment de la taille de la population, de la nature des relations personnelles et professionnelles existantes, du niveau de confiance entre les organismes concernés, du degré d'indépendance perçue de l'OGE et de la mesure dans laquelle le cadre réglementaire est favorable ou défavorable à la collaboration.

Encadré 4.7. Royaume-Uni : parvenir à collaborer dans un contexte unique

Bien souvent, la collaboration entre organismes n'est pas le fruit du hasard. Au Royaume-Uni, la commission électorale collabore avec trois agences, qui existaient déjà lorsque les menaces informatiques des élections ont émergé :

1. le bureau du commissaire à l'information, la principale agence de protection des données du pays ;
2. le Centre national de sécurité informatique (l'un des premiers organismes de ce type au monde), qui fournit conseils et assistance aux secteurs public et privé en matière de protection contre les menaces informatiques ;
3. le groupe constitutionnel du Bureau du Cabinet, qui assume l'entière responsabilité des politiques, de la législation et des financements dans le cadre des élections nationales et d'autres votes.

Cette collaboration plurielle, unique au monde, ne suit pas des modèles internationaux, mais se développe naturellement et est renforcée au cours de chaque processus électoral.

Parmi les pays étudiés, peu ont officiellement défini les élections comme des infrastructures essentielles. De plus, selon les cas, ce terme n'existe pas ou revêt des significations très différentes. La Finlande, par exemple, le réserve au secteur militaire. La Géorgie, elle, a déclaré que les élections constituaient des infrastructures essentielles et a exigé de son OGE qu'il réalise une importante mise à jour de ses défenses contre les menaces informatiques, sans toutefois lui accorder des fonds ou un soutien supplémentaire (voir l'encadré 4.8). Aux États-Unis, cependant, cette désignation a joué un rôle décisif en faveur d'une collaboration plus étroite entre les administrateurs des élections locales, la commission d'assistance électorale et le département de la Sécurité intérieure en permettant à ce dernier de soutenir les organismes responsables de l'organisation des élections. Si certains pays ne reconnaissent pas officiellement les élections comme des infrastructures essentielles, comme la Roumanie, la plupart de leurs parties prenantes électorales les considèrent néanmoins comme telles. D'autres pays, y compris l'Australie, envisagent actuellement de définir les élections comme des infrastructures essentielles.

Encadré 4.8. Géorgie : infrastructures essentielles et normes ISO

La Géorgie a désigné les élections comme des infrastructures essentielles, ce qui signifie que son système de gestion de la sécurité informatique doit être mis en œuvre par la commission électorale centrale et d'autres organismes, conformément à la norme ISO 27001, qui requiert l'établissement de mécanismes de contrôle poussés. L'équipe d'intervention d'urgence informatique du pays a travaillé en étroite collaboration avec la commission électorale et aidé la Commission électorale centrale à mettre en place son système de gestion de la sécurité informatique. Cette équipe est également préparée à intervenir en cas d'urgence informatique relative à une élection.

5. Conclusions et recommandations

1. La sécurité informatique des élections représente un engagement à long terme qui nécessite la mise en œuvre de mesures tout au long du processus électoral. Les technologies utilisées peuvent varier d'un processus électoral à l'autre, tout comme les entités adverses et leurs moyens d'action. Garantir la complète sécurité informatique des élections requiert donc un engagement et des ressources continus.
2. Même dans les pays où le recours aux technologies électorales est limité, l'intégrité des élections est exposée à des menaces informatiques qui doivent être prises au sérieux. Encore récemment, les débats concernant la sécurité informatique des élections concernaient principalement le vote électronique. Les pays utilisant un système de vote manuscrit se considéraient donc comme largement à l'abri des attaques informatiques. Cependant, il est désormais amplement reconnu que presque tous les processus électoraux font un usage plus ou moins extensif des technologies, y compris pour l'inscription des électeurs, pour l'enregistrement des partis et des candidats ainsi que pour le calcul et la publication des résultats. Chacun de ces procédés peut constituer la cible d'attaques, à moins de faire l'objet d'une évaluation des vulnérabilités et d'une protection appropriées.
3. La collaboration entre organismes est essentielle à l'amélioration de la sécurité informatique des élections. Les menaces informatiques dépassent le cadre des mandats institutionnels. Leur gestion requiert souvent la mise en commun de ressources, de données, d'informations contextuelles et de l'expertise de différents organismes. Les OGE et les autres autorités électorales devraient donc étudier les différents modèles de collaboration

entre organismes en matière de sécurité informatique des élections, tels que ceux décrits dans le présent document.

4. Il est tout aussi important de gérer la perception qu'a la population d'un processus électoral que de se protéger contre des menaces avérées. L'intégrité électorale est entièrement tributaire de la confiance et du soutien de la population. Coordonner la communication publique fait donc partie intégrante de la lutte contre toutes les opérations de désinformation visant le processus électoral, afin de préparer correctement la population et de fournir une réponse homogène en cas d'incident. Le présent document contient des exemples de modèles de gestion de cette communication ayant fait leurs preuves.
5. La collaboration entre organismes devrait être transparente et clairement définie. Afin de préserver l'indépendance réelle et perçue de l'OGE, la collaboration entre organismes devrait être expliquée à la population. Le rôle joué par des organismes traditionnellement non concernés par les élections, tels que les services de sécurité, doit être clairement délimité. À cette fin, il peut être nécessaire de réglementer la portée et les limites de la collaboration.
6. Une collaboration internationale est nécessaire. La sécurité informatique des processus électoraux est trop complexe et évolue trop rapidement pour ne faire l'objet que d'une gestion nationale. Les pays devraient donc investir dans des échanges bilatéraux et internationaux de connaissances et d'informations aux échelles régionale, interrégionale et intercontinentale. Il a été démontré dans ce document que différentes régions progressent actuellement à un rythme similaire en matière de sécurité informatique. Cependant, la diversité de leurs expériences offre de nombreuses possibilités d'enrichissement mutuel.
7. La collaboration entre organismes ne devrait pas se limiter aux agences gouvernementales. Le secteur privé, les partis politiques, le milieu universitaire, la société civile et les médias peuvent tous jouer un rôle important dans l'amélioration de la sécurité informatique des processus électoraux et de sa perception par la population. En revanche, certains acteurs, dont les intérêts sont liés à cette question, peuvent représenter une menace supplémentaire à la réputation des organismes électoraux. En effet, s'ils ont le sentiment de n'avoir aucun moyen de faire part de leurs inquiétudes, ces acteurs sont susceptibles de divulguer des données ou d'exagérer les rumeurs de vulnérabilité. Les organismes gouvernementaux devraient donc étendre leur champ d'action et collaborer avec une grande variété de parties prenantes non gouvernementales.

8. Il convient de sensibiliser les partis politiques aux effets dévastateurs potentiels des attaques informatiques. Les candidats et les partis politiques (en particulier les petits partis) disposant de ressources limitées sont probablement les acteurs électoraux les plus vulnérables en matière de sécurité informatique. Dans certains pays, des organismes gouvernementaux peuvent fournir des conseils et une assistance de base dans ce domaine. Les partis devraient au moins être informés de leurs responsabilités, comme la protection de leurs infrastructures est de leur ressort. Il convient en outre de souligner que le gouvernement ne dispose pas des capacités nécessaires pour contenir les répercussions négatives d'une attaque informatique visant les partis et leurs campagnes électorales.
9. Lorsque les organismes ne collaborent pas spontanément, les responsables politiques devraient envisager de définir les élections comme des infrastructures essentielles ou d'adopter d'autres approches verticales. Certains pays sont parvenus à susciter une collaboration efficace entre organismes à partir d'une approche essentiellement informelle et horizontale, sur l'initiative d'une ou plusieurs des agences concernées. En particulier (mais sans s'y limiter) dans les cas où les organismes ne collaborent pas naturellement ou ne parviennent qu'à des résultats limités, il peut être nécessaire d'adopter une approche plus verticale. Elle devrait permettre de surmonter les obstacles institutionnels, culturels et administratifs rencontrés, garantir la disponibilité de financements et garantir la transparence requise. Faire des élections une infrastructure essentielle relève d'une approche verticale.
10. Des observateurs électoraux devraient évaluer la collaboration entre organismes. Afin d'assurer le suivi de la sécurité informatique des processus électoraux, il convient d'évaluer le niveau de collaboration entre les organismes ainsi que son degré d'efficacité ; ces critères doivent également être évalués chez les acteurs concernés. Les responsabilités des organismes et les mesures adoptées afin de préserver l'indépendance de l'administration électorale ne doivent pas être négligées dans le cadre de cette évaluation.

Annexe A : Études de cas

Des OGE et des agences de sécurité du monde entier ont été sollicitées pour les besoins du présent document. Certains entretiens sont mentionnés dans les études de cas suivantes, tandis que d'autres ont été utilisés pour fournir des informations contextuelles et des détails supplémentaires.

Ils se sont articulés autour des thèmes suivants :

- présentation de l'organisme et de son usage des TIC ;
- identification des risques de sécurité informatique pesant sur les élections ;
- vue d'ensemble des risques de sécurité informatique pesant sur les systèmes et processus électoraux ;
- acteurs chargés de la protection des élections contre les attaques informatiques ;
- organisation de la collaboration entre les parties prenantes concernées.

Afrique du Sud

Structure de l'OGE

La Commission électorale indépendante (CEI) d'Afrique du Sud est un organisme permanent créé en vertu de la constitution du pays pour organiser des élections libres et justes au niveau des administrations nationales, provinciales et municipales. Si elle est financée par des fonds publics et rend compte au parlement, la CEI est néanmoins indépendante du gouvernement.

Ses bureaux provinciaux sont responsables des activités réalisées dans les neuf provinces du pays, et comptent, chacun, un responsable électoral provincial et un

personnel d'appui. Les bureaux provinciaux supervisent 213 bureaux électoraux municipaux et 70 sous-bureaux, et gèrent les projets électoraux, dont les élections.

La CEI prend en main l'ensemble du processus électoral, allant de la planification à la communication des résultats. Les médias sociaux ne relèvent pas du mandat de la CEI.

Usage des TIC

Les votes, le décompte des voix et le dépouillement du scrutin à l'échelle locale sont tous des processus manuels. Un système centralisé assure une double saisie des résultats, indépendantes l'une de l'autre, afin de vérifier qu'il n'y a pas pas d'erreur de saisie ou encore de fraude, grâce à la comparaison des chiffres résultant des deux saisies différentes. Le système centralisé permet aussi la compilation des résultats, l'attribution des sièges, et l'audit des résultats. Les résultats sont publiés en temps réel, les données brutes et compilées étant mises à la disposition des médias et des partis politiques. Les fiches de résultats scannées sont également disponibles.

La technologie est également utilisée à des fins d'appui opérationnel et de gestion, à savoir :

- l'inscription sur les listes électorales, et l'enregistrement des partis politiques et des candidats, ainsi que le portail des citoyens et les outils en ligne en libre-service (désignation des candidats, statut d'enregistrement, votes spéciaux, etc.) ;
- la présence de la CEI sur Internet, dont le registre électoral en ligne ;
- les processus administratifs d'arrière-guichet, les systèmes de collaboration, l'informatique décisionnelle, et le suivi des problèmes, des biens et du personnel.

La sécurité des TIC englobe tous les niveaux, y compris la segmentation multiple du réseau, la conception et le développement d'applications axées sur la sécurité, la gestion des comptes d'utilisateur et le contrôle d'accès, le filtrage du trafic pour détecter les logiciels malveillants, le contrôle permanent de la sécurité et le partage d'informations sur toute infraction en temps voulu.

Risques

La protection de ces systèmes contre le piratage informatique représente une part importante du suivi quotidien assurant la sécurité des élections et s'inscrit dans les obligations et les devoirs de la CEI, qui doit « développer et promouvoir le développement des compétences et des technologies électorales à tous les échelons de l'administration ».

L'ouverture et la transparence sont les deux piliers de la CEI en matière de sécurité. En d'autres termes, elle veille à l'exactitude des informations qu'elle partage. En 2011 et en 2014, elle a détecté et mis fin à des tentatives de piratage contre son site Internet ; le premier incident a été considéré comme suffisamment grave pour justifier une enquête de l'Agence de sécurité de l'État. Depuis, la sécurité informatique de la CEI n'a plus fait l'objet d'attaques graves.

Collaboration entre organismes

La CEI a rarement recours aux autres institutions publiques, dans le cadre strict de leurs rôles constitutionnels, à savoir les forces de l'ordre, les services de sécurité, etc. Elle fait appel aux services spécialisés de sociétés privées. En Afrique du Sud, le suivi de la sécurité des élections et l'évaluation de l'état de préparation interviennent à de multiples niveaux :

- La CEI confie à des sociétés privées indépendantes l'évaluation de la sécurité et leur fournit différents niveaux d'accès à ses systèmes internes dans le cadre de la préparation des élections.
- Le Bureau du contrôleur général de la République effectue les audits de sécurité et bénéficie de tous les droits d'accès nécessaires.
- Le service informatique et le service des élections de la CEI vérifient la légalité du système des résultats, le contrôle d'accès et la sécurité.
- L'Agence de sécurité de l'État effectue une analyse des menaces pour le compte de la CEI, met en avant les domaines qui nécessitent une attention particulière (la sécurité informatique n'en fait généralement pas partie) et est habilitée à enquêter sur les incidents selon les besoins.
- La coopération de longue date avec la police sur les questions générales de sécurité exclut cependant tout ce qui a trait à Internet.

Chaque année électorale, la CEI commissionne un audit de sécurité indépendant de l'ensemble de son infrastructure de TIC. Cet audit comprend des tests de pénétration externe basés sur les contrôles de sécurité interne et la mise en œuvre des politiques, et des correctifs de logiciel pour identifier tout risque ou vulnérabilité possible en matière de sécurité. L'auditeur externe remet un rapport de certification à la direction de la CEI et aux parties prenantes, et fournit des instructions sur la résolution des problèmes aux équipes d'assistance technique. Par ailleurs, les partis politiques sont invités à vérifier de manière indépendante le système des résultats et à s'assurer ainsi que le système fonctionne tel qu'il se doit et qu'il est conforme à la loi.

Les partis politiques ayant demandé des conseils à la CEI en matière de sécurité informatique, ces échanges ont donné lieu à des réunions mensuelles du Comité

de liaison des partis (cette fréquence s'accentue pendant la période précédant les élections). Les petits partis possédant moins de ressources, ils sont plus exposés aux risques et nécessitent un soutien supplémentaire. Mais la sécurité informatique des partis ne relève pas du mandat de la CEI, qui peut simplement inciter les agences de sécurité à fournir davantage d'informations aux acteurs politiques. Dans l'ensemble, la CEI compte redoubler d'efforts pour contribuer à approfondir la compréhension commune des parties prenantes électorales en matière de menaces informatiques émergentes.

Australie

Structure de l'OGE

La commission électorale australienne est responsable de l'organisation des élections fédérales et des référendums ainsi que de la gestion de la liste électorale australienne du Commonwealth. Chaque membre de la Chambre des représentants d'Australie représente l'une des 151 circonscriptions électorales du pays. Les bureaux de circonscription sont chargés des listes électorales, de l'organisation de campagnes de sensibilisation et de la gestion des élections.

Usage des TIC

Par le passé, la commission électorale australienne a su s'adapter de façon efficace aux amendements rendant obligatoire l'usage des technologies informatiques, tout en préservant l'intégrité du système électoral. Au cours des élections fédérales de 2007, le vote électronique a été testé auprès de certains groupes de citoyens, au nombre desquels figuraient les électeurs aveugles ou malvoyants. Ces essais ont conduit à l'adoption de la méthode de vote par téléphone actuellement employée pour ces personnes.

À l'heure actuelle, la commission électorale australienne utilise aussi bien des ordinateurs centraux vieux de 20 ans que des outils modernes d'informatique en nuage. La commission est responsable :

- d'un site Internet à la capacité hautement évolutive (de 20 visites par jour en dehors des périodes électorales à 20 millions le jour du vote) ;
- du décompte des bulletins au moyen de lecteurs optiques, dont le fonctionnement est assuré par des fournisseurs tiers dans le centre de dépouillement de chaque État. Ces lecteurs servent à procéder au calcul complexe des résultats des votes préférentiels ;
- d'un système de transfert et de tabulation des données ;

- d'un système d'inscription sur les listes électorales (hébergé par un fournisseur tiers), utilisé pour élaborer les listes électorales et partager les données sur les électeurs avec les partis politiques ;
- de listes électroniques certifiées à certains endroits afin d'identifier les électeurs et d'inscrire sur la liste électorale qu'ils ont déjà voté.

Risques

L'une des priorités de la commission électorale australienne est de protéger ses systèmes informatiques (en particulier les systèmes utilisés pour le décompte des voix et le transfert de données) ainsi que l'ensemble des processus électoraux contre les menaces à leur intégrité. Des procédures manuelles, y compris un dépouillement sur support papier, restent possibles et disponibles en dernier recours.

Collaboration entre organismes

Le gouvernement australien attache une grande importance à sa politique de sécurité informatique. Son cadre politique pour la sécurité préventive contient des normes ainsi qu'un manuel de sécurité pour la protection de la confidentialité, de l'intégrité et de l'accessibilité des données et systèmes informatiques gouvernementaux (Département de l'Attorney-General du gouvernement australien, s.d.).

Ces normes exigeantes ne s'appliquent pas qu'aux élections, elles concernent également la sécurité informatique des copies numériques et papier ainsi que la sécurité physique et personnelle. Conformément à ces normes, la commission électorale australienne gère les risques de sécurité informatique de la même façon que les autres entités gouvernementales. Son unité pour la gouvernance et la sécurité informatiques comprend donc un conseiller affecté à la sécurité informatique.

En mai 2018, dans un contexte d'inquiétude croissante de la communauté internationale, l'Australie a créé une équipe spéciale de protection de l'intégrité électorale, chargée de renforcer ses processus pour les prochaines élections partielles et de contribuer à l'organisation des futures élections fédérales. L'équipe spéciale réunit un panel d'organismes, notamment la commission électorale australienne, les OGE des États fédérés et des territoires, le ministère de l'Intérieur, le centre australien pour la sécurité informatique, le ministère des Communications et les organismes de sécurité. Elle a évalué les failles auxquelles les élections et les processus électoraux sont exposés, et vise à :

- parvenir à une compréhension commune des vulnérabilités et de leur évolution d'une élection à l'autre ;

- évaluer les risques et proposer des contre-mesures adaptées ;
- clarifier la répartition des rôles ainsi que les mécanismes de coordination et de leadership entre les organismes participants ;
- conseiller la commission électorale australienne et les OGE des États fédérés et des territoires en matière d'atténuation des risques ;
- coordonner le suivi des médias sociaux ;
- élaborer une stratégie de communication commune.

Le Conseil des gouvernements australiens a également exigé que toutes les commissions électorales du pays soient soumises à une évaluation de leur santé informatique. Le Comité mixte permanent pour les questions électorales a fait de la désignation des systèmes électoraux australiens en tant qu'infrastructures nationales essentielles un sujet de débat fondamental (Parlement du Commonwealth d'Australie, 2019).

La commission électorale australienne maintient également des échanges continus avec des entreprises propriétaires de médias sociaux telles que Facebook, Twitter et Google afin d'améliorer sa gestion de la communication électorale.

Autriche

Structure de l'OGE

En Autriche, la gestion des élections est partagée : une commission électorale fédérale indépendante collabore avec le ministère fédéral de l'Intérieur. Les différents organismes de gestion des élections incluent la commission électorale fédérale, les conseils électoraux provinciaux, les conseils électoraux de districts, les conseils électoraux municipaux et un conseil électoral spécial. Les administrations locales sont responsables de tous les processus électoraux.

Usage des TIC

Le vote se fait à l'aide de bulletins en papier, avec un décompte manuel des voix et la rédaction de rapports manuscrits. Dès la fermeture des bureaux de vote, les rapports préliminaires sont transmis par téléphone, par courriel ou par SMS. Ces données préliminaires sont stockées sur un serveur du ministère de l'Intérieur. Elles n'ont aucune valeur juridiquement contraignante, mais doivent être protégées de toute divulgation tant que le scrutin n'a pas été clos dans tous les bureaux de vote. Les données numériques sont ensuite comparées à celles des rapports provinciaux, puis les résultats préliminaires sont publiés en ligne et annoncés par le ministère. Tous les logiciels utilisés sont continuellement révisés et mis à jour, et le système est testé avant chaque élection.

En 2018, un nouveau système centralisé de listes électorales numériques a été lancé. Il facilite l'amélioration de la qualité des données ainsi que l'augmentation du taux d'utilisation des outils en ligne et du nombre de signatures en faveur d'initiatives publiques. Bien que les municipalités soient toujours responsables de la gestion des listes électorales locales, toutes les données sont stockées dans un système centralisé. La convivialité accrue du système de participation en ligne a suscité l'intérêt des citoyens et un volume sans précédent de signatures en faveur d'initiatives publiques.

Risques

La transmission électronique des résultats consiste en des rapports rédigés selon les besoins qui n'ont pas de valeur juridiquement contraignante. La Cour constitutionnelle a statué que seuls les rapports manuscrits pouvaient servir de base légale au calcul des résultats finaux. Cependant, même la gestion des résultats préliminaires peut soulever des questions. Par exemple, la publication de données d'essai sur le site public de consultation des résultats provisoires, avant le jour de vote et à la suite de problèmes techniques, a fait débat.

Quelques jours après son lancement, la plate-forme en ligne pour les initiatives publiques est devenue inaccessible à de nombreux utilisateurs. Bien que ce problème ait été rapidement résolu, il a mené à une enquête parlementaire qui a conclu qu'il n'existait aucun risque d'attaque (informatique) externe. Ce sont plutôt l'engouement et le taux d'utilisation inattendus qui ont causé la lenteur de ce nouveau système en ligne, sans jamais en entraîner l'effondrement total.

Collaboration entre organismes

La collaboration entre les différents organismes s'articule autour du réseau électoral national, créé en novembre 2018. Ce réseau inclut les organismes compétents en matière d'élections (par le biais du ministère de l'Intérieur, de la commission électorale fédérale et du ministère des Affaires étrangères) ; de sécurité informatique et des réseaux (par le biais de la chancellerie fédérale et du ministère de l'Intérieur) ; de défense informatique (par le biais du ministère de la Défense) ; de droit des médias, de campagnes électorales et de partis politiques (par le biais de la chancellerie fédérale) ; de registres et d'infractions en ligne (par le biais du ministère de l'Intérieur) ; de services en ligne et de problèmes informatiques (par le biais du ministère des Affaires informatiques) ; de protection des données et de droit pénal (par le biais du ministère de la Constitution, des Réformes et de la Justice) ; et de droit européen et d'affaires institutionnelles (par le biais du ministère des Affaires étrangères). Le ministère de l'Intérieur représente le réseau national auprès de l'Union européenne.

Bulgarie

Structure de l'OGE

En Bulgarie, les OGE de gestion des élections sont répartis en trois niveaux : la commission électorale centrale (CEC), 31 commissions électorales de district et environ 12 000 commissions électorales de circonscription.

Usage des TIC

Les listes électorales sont constituées à partir du registre national de la population, qui est géré par le département des services d'état civil et d'administration du ministère du Développement régional et des Travaux publics.

La CEC conçoit et administre des sites Internet et différents registres, en plus de garantir le fonctionnement du système de messagerie électronique utilisé par les différents organismes de gestion des élections et d'un système de dépôt de demandes électroniques pour le vote à l'étranger. Elle rend également possibles les échanges de données numériques sur les électeurs et les candidats entre la Bulgarie et les autres États membres de l'Union européenne. Enfin, la CEC est chargée de la gestion d'un système électronique pour l'approbation de modèles préimprimés de bulletins papier, utilisés pour le décompte électronique des voix et les transferts nécessaires en cas de vote à l'étranger.

La législation électorale prévoit des dispositions concernant le vote manuscrit et électronique. Au cours de l'élection présidentielle de 2016, le vote électronique a été mis en place pour la première fois dans 500 bureaux de vote, et les résultats ont été inclus dans le total officiel. Un prototype de décompte des votes électroniques a également été testé. Le 1er janvier 2018, un projet pilote de vote électronique à distance (par Internet), placé sous la responsabilité de la CEC, a été lancé. Les listes électorales préliminaires doivent être soumises à l'examen du public par leur publication dans les bureaux de vote et sur les sites des municipalités au moins 40 jours avant toute élection. Pour finir, les transactions bancaires relatives aux campagnes électorales sont rendues publiques et accessibles sur le site du bureau national d'audit.

Risques

Après avoir réalisé un inventaire des TIC relatives aux élections, la CEC a adopté une approche de gestion des risques de sécurité informatique permettant de définir leurs répercussions potentielles sur les processus électoraux, leur probabilité ainsi que les mesures d'atténuation possibles. Ces informations sont mises à jour immédiatement avant les élections. Les principaux risques techniques traités dans le cadre de cette approche comprennent :

- les attaques DDoS – en 2013 et en 2015, les infrastructures publiques de la commission ont subi des attaques d'une ampleur sans précédent ;
- les fuites de données personnelles des électeurs ou des candidats (menace potentielle) ;
- les compétences insuffisantes des organismes de gestion des élections de différents niveaux ;
- la modification de données ou de contenus par des utilisateurs disposant d'un accès aux systèmes administratifs, accidentelle ou intentionnelle ;
- la désinformation (menace potentielle) ;
- les atteintes à la sécurité de l'information des ressources publiquement accessibles consistant en la modification ou le remplacement de contenus, y compris les risques de piratage de machines individuelles, d'attaques entraînant des défaillances de l'équipement ainsi que de manipulation des données au cours de leur transfert et du calcul des résultats, en particulier après l'instauration du vote électronique à distance et de machines à voter.

Collaboration entre organismes

Pour protéger les processus électoraux, la CEC collabore avec une grande variété de partenaires de l'administration publique et d'entreprises du secteur des technologies. Les activités gouvernementales en ligne et celles relatives à la sécurité de l'information relèvent du mandat de l'agence pour l'administration en ligne et dépendent des ressources du ministère de l'Intérieur, de l'agence du gouvernement pour la sécurité nationale et d'autres organismes.

Le principal partenaire technologique de la CEC est l'entreprise publique Information Services JSC. Des experts de JSC sont chargés de gérer les infrastructures essentielles de la CEC ainsi que d'élaborer et de mettre en œuvre des processus électroniques de calcul des résultats et du taux de participation en ligne dans le cadre des élections.

La CEC est responsable de la coordination de tous les acteurs concernés, y compris en cas d'incident. À l'échelle nationale, un groupe réunissant différents

services présidé par le vice-Premier ministre planifie et coordonne les activités avant, pendant, et après le jour de vote.

En amont de chaque élection, le procureur général et le ministère de l'Intérieur créent un quartier général commun (équipes) pour l'organisation d'activités de lutte contre les infractions relatives aux élections, y compris informatiques. Ces équipes sont opérationnelles tout au long de la période de campagne précédant l'élection ainsi que le jour du vote.

La CEC et son partenaire technologique travaillent continuellement à l'amélioration des méthodes et outils de protection informatique. Les centres de TIC utilisés pour le calcul des résultats électoraux sont situés dans des environnements physiquement indépendants, ce qui leur permet de fonctionner sans ingérence externe. Les infrastructures publiques disposent de plusieurs systèmes de secours et sont équipées de technologies de protection informatique modernes. Elles font également l'objet d'une surveillance permanente par des experts de la sécurité informatique. Les mesures de prévention des attaques informatiques adoptées par l'OGE protègent les partis participant directement à une élection et d'autres parties prenantes pertinentes, telles que les fournisseurs nationaux d'accès à Internet ainsi que les opérateurs de télécommunications et de systèmes de transfert, etc.

Au cours de la période précédant chaque élection, une vaste campagne de communication publique est organisée. Des séances d'information sont régulièrement organisées, et une collaboration étroite avec les médias est assurée afin de lutter contre les campagnes de désinformation.

Canada

Structure de l'OGE

Présidé par le directeur général des élections, Élections Canada est un organisme parlementaire indépendant impartial chargé de l'application de la loi électorale du Canada. Son mandat consiste à :

- se tenir prêt à organiser des élections générales et partielles ainsi que des référendums fédéraux à tout moment ;
- administrer la mise en œuvre des dispositions en matière de financement politique de la loi électorale du Canada ;
- veiller au respect des lois électorales ;
- mener des campagnes d'information publiques concernant l'inscription sur les listes électorales ainsi que les procédures de vote et de candidature ;
- mettre en œuvre des programmes d'éducation destinés aux étudiants concernant les processus électoraux ;

- soutenir les commissions indépendantes responsables du redécoupage des circonscriptions fédérales à la suite de chaque recensement décennal ;
- conduire des évaluations de nouvelles méthodes de vote et, avec l'approbation des parlementaires, mettre à l'essai de nouveaux processus de vote dans le but de les utiliser au cours de prochaines élections ;
- fournir des services d'aide et de coordination en matière d'élections aux organismes électoraux d'autres pays ou à des organisations internationales.

Usage des TIC

Pour les élections fédérales, le Canada recourt à des bulletins de vote papier remplis à la main par les électeurs et dépouillés manuellement par des fonctionnaires au sein des quelque 25 000 bureaux de vote du pays. Des observateurs provenant de chacun des principaux partis politiques surveillent le déroulement du processus. La gestion des élections est largement décentralisée et les données sont enregistrées en format papier afin de pouvoir être vérifiées après chaque élection. Le pays utilise également des systèmes de vote électronique. Élections Canada emploie les nouvelles technologies pour :

- gérer les réseaux numériques et intranets au sein des organismes et en situation réelle pour garantir le fonctionnement des communications ;
- tenir à jour et améliorer les logiciels utilisés pour le Registre national des électeurs et la Base de données de la géographie électorale, ainsi que d'autres outils de suivi (et d'élaboration de rapports) en temps réel concernant les activités électorales ;
- établir et renforcer sa présence sur les médias sociaux ;
- créer des applications sur mesure pour des services essentiels, tels que le Service d'information à l'électeur, la publication en temps réel des résultats électoraux et la soumission de rapports en ligne pour les entités politiques ;
- concevoir et gérer des applications sur mesure permettant aux partis politiques, aux associations de circonscription, aux candidats, aux candidats à l'investiture ou à la direction de remplir et de soumettre les rapports financiers requis par la Loi électorale du Canada ;
- administrer le Service d'inscription en ligne des électeurs, lancé en 2012, qui offre un autre moyen aux citoyens de vérifier et de mettre à jour leur statut d'électeur.

Risques

En cas d'erreur de transfert ou d'attaque visant leurs sites de publication, les résultats des élections fédérales peuvent toujours être vérifiés au moyen des documents papier, que même les attaques informatiques les plus sophistiquées ne peuvent manipuler. Cependant, les élections locales sont plus exposées aux menaces informatiques en raison de leur usage plus important d'outils technologiques tels que des lecteurs de bulletin, des tabulatrices de vote et des systèmes de vote en ligne.

Le Canada n'est pas à l'abri d'attaques cherchant à réduire le taux de participation ou à influencer le vote des électeurs. Jusqu'ici, la seule attaque recensée est celle du scandale Robocall de 2011, au cours duquel des milliers d'électeurs de presque toutes les 250 circonscriptions du pays ont signalé avoir reçu des appels automatisés affirmant à tort qu'un autre lieu de vote leur avait été assigné. À la suite de ses enquêtes, Élections Canada a attribué cette attaque à des acteurs politiques nationaux.

Le gouvernement canadien a chargé le Centre de la sécurité des télécommunications (CST) d'évaluer les menaces informatiques pesant sur les processus démocratiques du pays (CST, 2017) et de conseiller les partis sur les meilleures pratiques à adopter pour leur protection contre les attaques informatiques et la sauvegarde de leurs bases de données personnelles sur les électeurs.

Le CST identifie trois menaces informatiques majeures :

- pour l'inscription des électeurs, les attaques visant les systèmes de détermination des personnes en droit de voter ;
- pour les processus de vote, les attaques ciblant les systèmes de réception, de dépouillement et d'enregistrement des votes ;
- pour la publication des résultats, les attaques dirigées vers les systèmes utilisés pour informer la population de l'issue des élections.

Concernant les élections passées, l'évaluation du CST a mis au jour des attaques d'une complexité et d'une envergure majoritairement réduites, et a établi que les partis politiques, les politiques individuellement et les médias constituaient les parties prenantes les plus vulnérables. Le centre s'attend toutefois à des attaques plus nombreuses et plus sophistiquées à l'avenir. Son évaluation conclut que de multiples groupes emploieront probablement des outils liés aux technologies dans le but d'influencer les processus démocratiques du pays au cours des élections fédérales de 2019. Ce constat a poussé Élections Canada à renforcer la sécurité de ses systèmes en améliorant la protection de son réseau informatique et en mettant sur pied un nouveau service d'hébergement des

données qui offrira une série de mesures de défense supplémentaires, le tout en collaboration avec le CST.

Collaboration entre organismes

Le ministère des Institutions démocratiques est responsable de coordonner les efforts du gouvernement en matière de protection du processus démocratique contre les menaces informatiques, en coopération avec le CST, le Service canadien du renseignement de sécurité, Sécurité publique Canada et d'autres organismes.

En juin 2018, le gouvernement a annoncé la création du Centre canadien pour la cybersécurité, qui vise à proposer une approche globale de gestion de la sécurité informatique et à permettre la mise en œuvre de réponses gouvernementales plus rapides, mieux coordonnées et plus ciblées concernant les menaces informatiques (qu'elles soient relatives aux élections ou non). Élections Canada collabore avec ces partenaires en matière de sécurité pour se tenir à jour au sujet des menaces existantes. De plus, le Bureau de l'intégrité électorale, qui a été créé suite au scandale Robocall de 2011, évalue les menaces informatiques nationales et internationales et vise à les prévenir.

Élections Canada coopère également avec d'autres organismes gouvernementaux, dont les mandats ont trait à la sécurité des élections : le Commissaire aux élections fédérales, le Centre canadien pour la cybersécurité, le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada, Sécurité publique Canada et le Conseiller à la sécurité nationale.

L'organisation de processus électoraux sûrs et bénéficiant de la confiance de la population constitue un exercice conjoint incluant la participation d'Élections Canada, d'organismes de sécurité, de responsables politiques, des médias, d'entreprises privées et de la société civile. Les efforts d'organisation et de collaboration de ces organismes couvrent les quatre domaines complémentaires suivants :

1. La sécurité nationale et la gestion des urgences, notamment la défense du Canada contre une série de menaces à sa sécurité et d'autres risques tels que des ingérences ou des interventions étrangères. Les principales activités conduites à cette fin consistent en :
    - le transfert d'informations aux partis politiques et aux responsables électoraux fédéraux et provinciaux à propos des menaces pesant sur les processus électoraux du pays ;
    - des réunions avec des partenaires chargés de la sécurité internationale et des renseignements concernant leurs travaux et leur expérience ;

- l'établissement de relations avec les entreprises propriétaires de médias sociaux ;
- des collectes d'informations aux fins d'évaluation, telles que le rapport de 2017 du CST *Cybermenaces contre le processus démocratique du Canada* ;
- différents exercices de planification et de simulation.

2. Les institutions démocratiques, notamment le renforcement de leur capacité à faire face aux menaces émergentes afin de garantir la coordination de l'ensemble des activités du gouvernement. La principale action menée à cet effet a été l'adoption de la Loi sur la modernisation des élections (projet de loi C-76) en 2018. Cette loi comprend des dispositions qui visent à améliorer la sécurité des processus électoraux, en partie par :
   - le renforcement du système appliqué aux tiers ;
   - la promulgation d'interdictions supplémentaires concernant l'utilisation de fonds étrangers ;
   - l'accord de compétences supplémentaires au Commissaire aux élections fédérales ;
   - l'élargissement de la portée de dispositions relatives à certains types d'usurpation d'identité en ligne et de fausses déclarations ;
   - l'obligation pour les propriétaires ou exploitants de médias sociaux de publier et de conserver un registre des messages de publicité partisane et de publicité électorale.
3. La sécurité électorale, notamment des processus électoraux. L'indépendance de l'OGE dépend de diverses collaborations et activités principales :
   - des réunions mensuelles du comité directeur conjoint (OGE et agences de sécurité majeures) ;
   - la clarification des mandats ;
   - l'instauration d'une collaboration entre organismes/d'un soutien mutuel ;
   - le renforcement de la protection des infrastructures électorales ;
   - des échanges continus avec les partis politiques et les propriétaires de médias sociaux.

Les activités prévues comprennent :

- la finalisation et la mise à l'essai du Plan de gestion des incidents ;
- la conduite de différents exercices de planification et de formation ;
- la finalisation d'une stratégie en matière de communication ;
- le renforcement des sources d'information fiables.

4. La sécurité de l'OGE, au moyen de la coopération avec des partenaires en matière de sécurité pour renforcer ses infrastructures et ses mécanismes de protection. Les principales activités conduites à cette fin consistent notamment en :

    - le maintien d'une équipe chargée de l'intégrité électorale et la désinformation ;
    - le renforcement de la sécurité et du suivi des systèmes ;
    - des actions de sensibilisation à la sécurité, notamment sur le terrain ;
    - l'amélioration de la gouvernance et de la planification en matière de sécurité ;
    - le recensement et le partage des meilleures pratiques au profit des OGE ;
    - des réunions avec les partis politiques ;
    - la participation des propriétaires et exploitants de médias sociaux et l'établissement de canaux de communication pour apporter des réponses rapides en cas d'incident.

    Les activités prévues comprennent :

    - le renforcement continu de la position d'Élections Canada en tant que source d'informations fiables concernant quand, comment et où s'inscrire sur les listes électorales et voter ;
    - la finalisation d'exercices de planification et de formation, y compris de simulation de processus électoraux ;
    - le suivi des médias sociaux.

L'objectif final est de :

- préserver la simplicité et la facilité d'accès des processus de vote et d'assurer un accès pour tous à l'hygiène informatique de base.
- maintenir des échanges avec les partis politiques et la société civile, en reconnaissance du caractère politique de la sécurité informatique et dans le but d'éviter l'instrumentalisation de la sécurité électorale, en plus de gérer les attentes de la population et des acteurs politiques ;
- faciliter les activités de communication au moyen d'une source suscitant la confiance, de porte-parole publics qui tiennent compte de l'évolution du contexte médiatique et qui assurent un soutien cohérent et continu aux citoyens.

Au début de l'année 2019, le gouvernement canadien a dévoilé son plan en matière de lutte contre la désinformation et l'ingérence étrangère dans le cadre d'une approche multipartite incluant la participation des ministères des Institutions démocratiques, de la Défense nationale ainsi que de la Sécurité publique et de la Protection civile. Ce plan est fondé sur les quatre piliers suivants : a) améliorer l'état de préparation des citoyens en leur fournissant des informations ; b) renforcer la préparation organisationnelle en améliorant la coordination ; c) lutter contre l'ingérence étrangère au moyen des organismes chargés de la sécurité ; et d) compter sur les plates-formes de médias sociaux pour qu'elles contribuent à la sécurité des élections.

Conformément au Protocole public en cas de l'incident électoral majeur, cinq hauts fonctionnaires sont responsables de déterminer si la gravité d'un incident nécessite d'informer le public au cours de la période de campagne officielle. Pour leur décision, ces fonctionnaires se fondent sur les informations fournies par les organismes nationaux chargés de la sécurité.

Danemark

Structure de l'OGE

Au Danemark, la gestion des élections est la responsabilité d'organismes de trois niveaux : la section des élections du ministère de l'Économie et de l'Intérieur, 92 commissions électorales de districts et quelque 1 400 commissions électorales de circonscriptions. La section des élections est un organe permanent chargé de l'organisation des processus électoraux. Certains de ses fonctionnaires sont choisis par le ministère de l'Économie et de l'Intérieur pour faire partie d'une entité distincte, le conseil électoral. Ce dernier remplit des fonctions spécifiques telles que l'enregistrement des partis politiques non représentés au parlement qui

souhaitent contester les élections, le maintien d'un répertoire des noms de partis et la prise de décision quant à l'éligibilité d'électeurs ayant résidé à l'étranger pendant plus de quatre ans. Le système national d'enregistrement de l'état civil, qui contient des données personnelles élémentaires sur tous les résidents dotés d'un numéro d'état civil, sert de base à son personnel pour la constitution des listes électorales. Le ministère de l'Économie et de l'Intérieur est chargé de la gestion de ce système.

Les élections parlementaires nationales du Danemark ne sont pas à date fixe. Le mandat des membres du parlement est d'une durée maximale de quatre ans. Les élections se tiennent généralement trois semaines après avoir été convoquées par le Premier ministre. En pratique, l'enregistrement des partis doit être terminé avant la convocation d'une élection.

Les processus électoraux en eux-mêmes sont à la charge du ministère de l'Économie et de l'Intérieur. Les ministères de la Justice et de la Défense sont chargés de la gestion à plus grande échelle de l'intégrité électorale, qui concerne notamment les activités illégales sur les médias sociaux, la sécurité informatique et la coopération avec les partis politiques.

Usage des TIC

Tous les bulletins sont dépouillés manuellement le soir du vote, puis font l'objet d'un nouveau décompte manuel centralisé le lendemain. Les résultats des dépouillements effectués par district sont enregistrés dans le système de gestion des élections (conçu par un fournisseur privé) avant d'être transférés à l'office statistique danois. En tant que mesure de sécurité supplémentaire, celui-ci reçoit également par téléphone les résultats de tous les dépouillements par district le soir du vote. L'OGE dispose d'une méthode de calcul de la répartition des sièges doublement vérifiée et entièrement fonctionnelle. Un indicateur d'évolution des écarts de répartition des voix sert également de modèle statistique permettant d'évaluer la probabilité que ces écarts soient réels et d'aiguiller la recherche d'opérations de manipulation ou d'erreurs potentielles.

La section des élections collabore avec trois types d'acteurs qui ont recours à des systèmes informatiques :

- le registre national de la population, qui élabore les listes électorales ;
- les fournisseurs privés de technologies électorales ;
- l'office de statistiques danois, qui est chargé de rassembler les résultats.

Chacune de ces instances est responsable de sa sécurité informatique. Cependant, en cas d'incident, la population se tournera vers la section des élections pour une réponse.

Risques

La gestion décentralisée des élections et le recours à des processus majoritairement manuels sont considérés comme des points forts qui rendent la manipulation d'une élection dans son ensemble difficile. L'un des inconvénients est que les organismes locaux sont investis de la lourde responsabilité d'assurer la sécurité logistique des élections, y compris le fonctionnement des systèmes, sans toujours disposer des capacités requises à cet effet ou de la possibilité de collaborer, notamment pour l'évaluation des risques auxquels ils sont confrontés. En cas de menace à l'échelle municipale, la population tiendra le ministère pour responsable, qu'il le soit réellement ou non. Bien qu'un manuel centralisé pour l'organisation des élections locales ait été publié, il n'existe pas d'instructions ou de directives nationales en matière de sécurité informatique. En 2018, le département des élections a commencé à avertir chaque municipalité par courrier des risques en matière de sécurité informatique.

Quoique l'organisation décentralisée et hors-ligne des élections rende leur perturbation difficile, la perte de confiance (infondée) des électeurs en l'intégrité des processus électoraux constitue une préoccupation majeure. Pour préserver la perception du public, il est donc important d'informer les électeurs à propos du fonctionnement des élections et des méthodes de garantie de leur sécurité. Cette communication est assurée à la fois par le biais des médias traditionnels et des médias sociaux, et contribue à dissiper toutes les rumeurs qui peuvent circuler.

Les principaux risques technologiques encourus sont l'altération des sites publics d'organismes électoraux et les piratages de grande envergure visant les fournisseurs de systèmes essentiels, tels que ceux de l'état civil et de la gestion des élections.

Collaboration entre organismes

L'OGE danois est uniquement responsable du cadre législatif des élections et n'exerce aucun pouvoir de décision concernant leur financement. Les municipalités déterminent elles-mêmes la part de budget qui sera attribuée aux élections ainsi que les technologies et les fournisseurs qui seront mobilisés.

Au cours des dernières années est apparue la nécessité de renforcer la résilience face aux menaces informatiques et de communiquer avec le public à ce sujet. Les trois objectifs de la stratégie en matière de sécurité informatique du Danemark sont de recenser, de repérer ainsi que de gérer et de prévenir les attaques informatiques et les interruptions de systèmes.

En 2016, une équipe spéciale interministérielle a été créée sous l'impulsion de la section des élections. Coordonnée par le ministère de la Justice, cette équipe inclut les ministères de la Culture, de la Défense, des Affaires étrangères et de l'Économie, mais aussi le ministère de l'Intérieur (qui participe en tant qu'autorité électorale) ainsi que les services de sécurité intérieure et des organes administratifs

locaux. Étant chargé de la réglementation des médias, le ministère de la Culture joue un rôle d'auxiliaire.

Le fait que cette équipe ait été créée à la suite d'une décision prise en interne plutôt qu'en réponse à une pression médiatique ou politique a contribué à générer un fort sentiment d'appropriation ainsi qu'une grande volonté de collaborer parmi les organismes participants. Ces derniers disposent également des ressources financières suffisantes pour subvenir aux coûts supplémentaires entraînés. La collaboration ainsi mise en œuvre est largement informelle, les organismes se réunissant selon les besoins. Il a été décidé de manière volontaire que cette équipe spéciale ne serait pas dotée d'une structure formelle de partage des tâches et ne consisterait en rien de beaucoup plus complexe qu'un répertoire téléphonique comprenant les coordonnées des décideurs appropriés (suffisamment haut placés pour prendre des décisions, mais suffisamment proches des activités de terrain pour en avoir une bonne connaissance). L'adoption d'une telle structure est fondée sur la conviction que la gestion des crises ne devrait pas être imputée à un système distinct, les institutions et systèmes existants étant censés continuer à fonctionner normalement.

L'objectif principal des réunions de l'équipe spéciale est de définir les limites des responsabilités de chaque organisme ainsi que d'échanger des informations et d'établir des relations en amont d'éventuelles crises. On considère que l'une des sources de son efficacité est de viser haut tout en ayant commencé simplement. L'équipe spéciale a de plus renforcé le degré de sensibilisation aux responsabilités électorales des organismes participants, qui se sont montrés largement enclins à collaborer. En septembre 2018, trois ministères danois ont publié un plan d'action national pour lutter contre l'influence d'acteurs étrangers sur les processus électoraux et la démocratie.

Estonie

Structure de l'OGE

En Estonie, les élections sont supervisées par la commission électorale nationale, qui comprend sept membres. L'OGE de plus haut niveau du pays est le bureau électoral national. Indépendant sur le plan institutionnel, il relève toutefois de la compétence de la Chancellerie du parlement. Le bureau électoral national est responsable de conduire les élections ainsi que d'organiser et de certifier le décompte des votes électroniques. Il supervise également les activités des gestionnaires d'élections en plus d'être chargé de la conception et de la gestion des technologies nécessaires au déroulement des élections.

Usage des TIC

Le bureau électoral national recourt aux différentes technologies électorales suivantes :

- Un système de vote par Internet, fonctionnel depuis 2005 et utilisé par près d'un tiers des électeurs depuis 116 pays.
- Un système d'information pour les élections, fonctionnel depuis 1998 et utilisé en tant qu'outil électronique de gestion de la préparation des élections ainsi que de gestion des parties prenantes aux élections, des candidats, des statistiques et des résultats. Cependant, les résultats officiels s'appuient encore sur les documents papier.
- Une page Internet pour les résultats électoraux, où sont publiés les résultats et statistiques du système d'information pour les élections.
- Des listes électorales, constituées à partir du registre d'état civil centralisé du pays et gérées par le ministère de l'Intérieur depuis 2000. La création d'une liste électorale électronique, qui permettra à tous les bureaux de vote d'être reliés à un système d'information unique, est prévue pour 2021. Les données de ce système seront tirées des listes électorales, mais placées sous la responsabilité de l'OGE.

Les technologies électorales font partie d'un vaste ensemble d'outils d'administration en ligne fondés sur des systèmes des secteurs public et privé (énergie, télécommunications, opérations bancaires). Tous les citoyens estoniens possèdent une carte d'identité électronique pour l'accès et le recours à ces différents systèmes.

Bien que l'OGE soit responsable des technologies électorales, son mandat ne s'étend pas aux campagnes électorales, y compris celles menées sur les médias sociaux. Cependant, toutes les activités illégales détectées sur les médias sociaux sont immédiatement signalées à la police.

Risques

Depuis les attaques informatiques de grande envergure subies par les infrastructures électroniques et l'administration en ligne du pays en 2007, l'Estonie n'a fait la cible d'aucun autre piratage majeur. Des incidents mineurs sont cependant survenus, parmi lesquels la création de faux doubles des sites de l'OGE et de vote en ligne par des militants politiques. Pour ces incidents, une collaboration étroite avec la police a permis d'apporter des réponses rapides.

Le principal risque auquel l'Estonie est confrontée ne provient en réalité pas des piratages ou des atteintes à la sécurité du système avérés, mais des acteurs affirmant qu'ils sont capables de pirater ou de menacer la sécurité de n'importe

quel système informatique, nuisant ainsi à la confiance de la population en les processus électoraux. La gestion des relations publiques et la mise en œuvre d'une communication efficace concernant les technologies sont donc aussi importantes que la lutte contre les menaces informatiques en elles-mêmes, qui comprend trois dimensions :

- l'établissement d'un système de sécurité solide ;
- la sensibilisation de la population à ce dispositif de protection et aux mesures de sécurité en place ;
- l'élaboration d'un processus d'instruction rapide des plaintes qui évalue leur validité en quelques jours (et non en quelques années).

En cas d'incident, il est important de réagir rapidement pour préserver la confiance de la population. Une collaboration constante avec les services de police est donc assurée, ce qui permet de supprimer les fausses informations publiées en ligne le plus tôt possible. La Cour suprême estonienne procède à l'instruction des plaintes dans les sept jours suivant leur dépôt.

Conduite en 2017, la première évaluation globale des risques de sécurité informatique a conclu que les partis politiques et les candidats aux élections constituaient la cible privilégiée des attaques (Past, 2017). Bien que la sécurité informatique des partis et des candidats ne relève pas de la compétence de l'OGE, celui-ci est plus généralement chargé de protéger l'intégrité des élections.

L'évaluation globale a également mis au jour trois domaines de risques principaux :

- tous les systèmes électroniques utilisés pour les processus électoraux ;
- les risques relatifs à la gestion et à la collaboration ainsi qu'à la clarté de la répartition des responsabilités ;
- les risques mixtes liés aux guerres de l'information, y compris sur les médias sociaux, qui requièrent l'établissement d'une stratégie de communication claire.

Enfin, l'évaluation suggère que la hausse du niveau de risque est proportionnelle à l'envergure des élections (les élections locales étant peu exposées par rapport aux élections nationales et européennes).

Collaboration entre organismes

L'OGE estonien considère que la protection de l'intégrité des élections est la responsabilité de l'ensemble du gouvernement. La coopération visant à garantir la sécurité des technologies électorales prévoit la participation d'organismes tant du

secteur public que du secteur privé : le bureau national électoral et la commission électorale nationale, l'agence nationale des systèmes informatiques, son département de mesures de réponse, l'équipe de gestion de la sécurité informatique (CERT Estonie), Cybernetica et un fournisseur de certificats électroniques (SK ID Solutions). L'un des aspects essentiels de la sécurité est la mise en place d'une bonne hygiène informatique et de campagnes de sensibilisation à l'identité numérique, qui encouragent tous les citoyens à assurer la protection de leurs appareils personnels et de leur identité en ligne.

En Estonie, les organismes collaborent par le biais de multiples équipes spéciales et groupes de travail établis selon les besoins. Répartir les activités entre différentes plates-formes permet d'assurer une collaboration d'échelle réduite, ciblée et efficace. Les équipes spéciales sont fondées sur des relations personnelles et professionnelles, tandis que les groupes de travail comprennent généralement les représentants mandatés de différents organismes. En amont de chaque élection, un ensemble de groupes spéciaux sont constitués et affectés à la gestion de questions, de domaines d'action et de besoins spécifiques. Déterminés en fonction du contexte actuel, le nombre et la structure de ces groupes sont flexibles et peuvent être modifiés si besoin. Les groupes suivants ont notamment été créés :

- Le groupe de travail général hebdomadaire sur les TIC est responsable d'une variété de technologies comprenant les systèmes d'information, les sites hébergeant des services, etc. Il comprend l'OGE, l'agence nationale des systèmes informatiques et d'autres organismes compétents suivant les domaines abordés.
- Le groupe de travail hebdomadaire sur les relations publiques œuvre principalement à l'élaboration d'une stratégie de communication claire et uniforme concernant les processus électoraux et le suivi des informations circulant à leur sujet. Il est également chargé de fixer les seuils d'intervention relatifs à ces informations ainsi que de clarifier les réponses à apporter. Les organismes qui y participent sont l'OGE, le ministère des Affaires étrangères, le ministère de l'Intérieur, le ministère de l'Économie et des Communications ainsi que la chancellerie d'État et l'agence nationale des systèmes informatiques.
- Le groupe de travail sur les registres, les cartes d'électeur et les listes électorales est chargé de tout ce qui concerne l'inscription sur les listes électorales et leur gestion. Il comprend l'OGE, le ministère de l'Intérieur et son centre informatique ainsi que l'agence nationale des systèmes informatiques, lorsque certains domaines spécifiques sont traités.
- Le groupe de travail sur les restrictions imposées aux campagnes électorales examine l'application des restrictions concernant les dépenses de

campagne. Il est constitué de l'OGE et du service de la police et des gardes-frontières.

- L'équipe spéciale pour le vote à l'étranger est responsable de l'organisation et de la gestion des votes depuis l'étranger. Elle comprend l'OGE ainsi que les ministères de l'Intérieur et des Affaires étrangères.
- L'équipe spéciale pour le vote par Internet est responsable de l'organisation et de la gestion des votes en ligne. Les organismes qui y participent sont l'OGE, l'agence nationale des systèmes informatiques, l'entreprise de conception des systèmes (Cybernetica), un fournisseur tiers d'assistance téléphonique et de service à la clientèle ainsi qu'un auditeur indépendant.

La plupart des équipes spéciales ont élaboré des plans d'action conjointe. Elles font usage d'un canal de communication externe unique, généralement incarné par la personne chargée de la communication au sein de l'OGE. Afin de garantir l'efficacité de ces différentes entités, il est essentiel d'organiser des réunions entre des représentants de rang égal des organismes participants : les fonctionnaires de haut niveau avec les fonctionnaires de haut niveau, les experts en informatique avec les experts en informatique, etc.

L'OGE coopère également avec l'agence nationale des systèmes informatiques pour proposer des formations sur l'hygiène informatique adaptées aux besoins des candidats aux élections. Celles-ci comprennent des instructions relatives à l'utilisation des médias sociaux, à la protection des comptes créés, au repérage et à la prévention des tentatives d'hameçonnage, etc. Des formations similaires sont offertes aux partis politiques, en plus d'une évaluation de la sécurité de tous leurs systèmes électroniques et de leur activité en ligne. Bien que ces formations ou services ne soient pas imposés, les acteurs politiques les jugent très utiles. Enfin, des activités de coordination bilatérale sont menées avec le Danemark, la Finlande, la Lettonie et la Suède, et l'Estonie contribue aux efforts de l'Union européenne en matière de sécurité informatique des processus électoraux.

États-Unis d'Amérique

Structure de l'OGE

Avec plus de 8 000 organes électoraux indépendants au niveau local et national, l'administration électorale des États-Unis est loin d'être uniforme. Cette décentralisation permet aux organes compétents de spécialiser leurs processus et de servir au mieux les collectivités locales. Face aux menaces informatiques, de nombreux agents des renseignements fédéraux estiment que le caractère hétérogène des processus électoraux aux États-Unis est un atout en matière de sécurité.

Bipartite et indépendante, la Commission d'assistance électorale (CAE) est un organe d'administration électorale créé à la suite de la promulgation de la loi fédérale sur l'administration électorale (Help America Vote Act) en 2002. La CAE fait office de centre d'échange de données en matière d'administration électorale ainsi que de boîte à outils et de ressources pour la formation électorale. Elle administre également le formulaire d'inscription sur les listes électorales nationales et le programme d'essai et de certification des machines à voter. Elle diffuse les Consignes sur le système de vote (les seules normes nationales en la matière) et agit en tant que représentant fédéral des administrateurs des élections siégeant au Conseil des gouvernements des États. La CAE a également pour tâches principales de préserver la confiance des électeurs et de fournir des orientations aux fournisseurs de technologie.

Usage des TIC

Une large gamme de technologies électorales a été déployée dans l'ensemble du pays, ce qui est en partie dû aux investissements technologiques suscités par la loi fédérale sur l'administration électorale. Plus de dix ans se sont écoulés ; cette technologie vieillissante a entraîné des vulnérabilités croissantes, la nécessité de réinvestir pour l'améliorer et la remplacer, voire des appels à revenir à des systèmes sur support papier, qui à leur tour recréeraient des problèmes antérieurs, comme l'accessibilité et la chaîne de contrôle.

Les agents électoraux doivent à présent trouver la manière de prolonger la durée de vie des technologies de vote tout en maintenant les normes les plus élevées possible et, en dépit du financement limité disponible, développer des mesures de prévention capables de résister aux attaques et de s'en relever. Les fonds destinés à la mise à jour des systèmes et à l'acquisition de nouvelles compétences en matière de sécurité sont eux aussi insuffisants. Le renforcement des mesures de sécurité et l'élévation des normes des systèmes ne peuvent se faire au détriment de l'accessibilité des électeurs handicapés, de l'assistance linguistique aux électeurs qui en ont besoin, des militaires ou des personnes résidant à l'étranger. En 2018, 380 millions de dollars américains (USD) ont été mobilisés pour la mise à jour des systèmes et seront distribués sur une période de cinq ans en fonction de la population de chaque État.

Risques

Compte tenu de la structure de l'administration électorale des États-Unis, la définition des risques de sécurité informatique et des responsabilités est multidimensionelle et varie en fonction de l'acteur concerné. Les juridictions locales et fédérales sont responsables de leurs propres données et technologies. À cet égard, trois systèmes sont particulièrement importants :

- les systèmes d'inscription sur les listes électorales ;

- les machines à voter et les technologies connexes ;
- les systèmes de tabulation et d'établissement de rapports.

L'expérience montre que la perturbation à grande échelle des machines à voter n'est pas nécessairement le principal sujet d'inquiétude. La manipulation des listes électorales constitue un risque plus important, car ces systèmes sont souvent disponibles en ligne et reliés aux bases de données de différentes institutions. Par conséquent, préserver la confidentialité des données des électeurs en les protégeant des violations et des manipulations fait figure de priorité.

Si les fournisseurs de technologies électorales sont censés perfectionner la sécurité de leurs produits, les conventions DefCon de 2017 et 2018 ont mis en évidence la nécessité de renforcer la crédibilité de la sécurité : des pirates en chapeau blanc (*white hat)* ont lancé plusieurs attaques réussies contre les technologies électorales. Même si certaines de ces attaques se sont produites dans des conditions très éloignées de la réalité, elles ont cependant souligné que les fournisseurs de technologie sont tenus de parer à ces éventualités et, le cas échéant, d'ajuster leurs systèmes.

La perte de confiance des électeurs, même si elle n'est fondée que sur des rumeurs, représente un risque majeur. Si les électeurs pensent que la crédibilité d'un processus électoral est compromise, ils sont moins enclins à y participer.

Le premier amendement de la Constitution américaine garantit la liberté d'expression, ce qui affranchit les médias sociaux de la surveillance ou des réglementations de l'OGE. Néanmoins, des partenariats étroits ont été conclus avec des prestataires, tels que Google et Facebook, en vue d'améliorer l'autoréglementation. Les électeurs doivent donc être conscients des responsabilités qui leur incombent, y compris se tenir informés des actes d'influence et vérifier les données et les informations. La CAE diffuse des vidéos d'information en ligne afin d'éclairer les électeurs sur leurs responsabilités en matière d'intégrité électorale (CAE, 2018).

Collaboration entre organismes

Axée sur les partenariats, la CAE collabore avec différentes institutions, comme le Département de la Sécurité intérieure (DHS), l'Institut national des normes et de la technologie, le Département de la défense, le Service postal des États-Unis, l'Association nationale des directeurs électoraux d'État, la Conférence nationale des Parlements des États, le Bureau fédéral d'enquête (FBI), l'Agence nationale de la sécurité et les instituts de recherche sur les politiques publiques. Elle coopère également avec le secteur privé et les fournisseurs de technologies électorales.

La collaboration entre la CAE et le DHS a démarré avant les élections de 2016 ; elle a permis au DHS de transmettre des informations relatives à la sécurité aux administrateurs et aux agents électoraux, et de comprendre les

processus électoraux ainsi que les commentaires et la retours d'information des administrateurs électoraux. En 2017, le DHS a qualifié les élections d'infrastructure essentielle. Ce statut détermine la manière dont le gouvernement fédéral perçoit un secteur et interagit avec, et hiérarchise l'attribution des ressources liées à la sécurité. Par exemple, c'est en vertu de ce statut que le DHS a mis à la disposition des administrateurs électoraux ses importantes ressources en matière de sécurité, dont 240 000 employés, pour les aider dans différents domaines, allant de l'identification des risques au service-conseil lié à la sécurité informatique.

Les agents électoraux ont d'abord accueilli avec circonspection la coopération avec les agents fédéraux, tout particulièrement avec le DHS. La CAE, qui représente l'ensemble des administrateurs électoraux, a contribué de manière déterminante à légitimer la coopération avec le DHS. Un autre défi résidait dans le transfert d'informations utiles en temps voulu entre les agents électoraux. Le Centre d'analyse et de partage de l'information multi-États a créé un programme pilote de partage de l'information permettant aux propriétaires et aux utilisateurs des technologies électorales de mieux protéger leurs systèmes contre les menaces informatiques (Hicks, 2018).

La collaboration entre organismes s'articule autour de deux grands forums. Présente dans ces deux instances, la CAE a largement contribué à leur mise en place :

- Le Conseil de coordination sectoriel des autorités électorales tient des réunions bimestrielles où les OGE au niveau local, fédéral et des États échangent des informations et préparent leur résilience informatique avec l'appui du DHS. Cette coopération est largement formalisée et s'appuie sur des protocoles officiels de diffusion de l'information.
- Le Conseil de coordination sectoriel rassemble un large éventail d'acteurs privés, allant des fournisseurs de technologie aux représentants des médias. Auto-organisé, il tient des réunions par téléphone environ deux fois par mois.

La coopération avec le secteur privé présente un nouvel enjeu pour le DHS et la CAE, à savoir la nécessité de légitimer les nombreuses petites entreprises qui ont vu le jour en réponse aux préoccupations suscitées par la sécurité informatique.

Le processus électoral des États-Unis repose sur un grand nombre d'agents électoraux qui ne sont pas toujours formés à la sécurité technologique. La CAE leur dispense donc des formations sur la lutte contre les attaques informatiques. Fruits d'une coopération avec le Centre Belfer, des scénarios condensent six mois de travail électoral en exercices pratiques de trois heures.

Finlande

Structure de l'OGE

L'autorité électorale suprême de la Finlande est son ministère de la Justice. Les organismes locaux de gestion des élections comprennent 13 commissions électorales de district, 311 autorités et commissions électorales municipales ainsi que des commissions électorales dans 2 000 bureaux de vote environ. Des commissions électorales supplémentaires sont présentes dans près de 500 bureaux de vote anticipé ainsi que dans des établissements tels que des prisons ou des hôpitaux.

Le ministère de la Justice collabore étroitement avec le registre d'état civil, à partir duquel les autorités électorales élaborent les listes d'électeurs, ainsi qu'avec le ministère des Affaires étrangères, qui est responsable de la gestion des votes anticipés à l'étranger. La protection des données constitue une question de sécurité fondamentale pour tous les organismes participant à l'inscription sur les listes électorales.

Usage des TIC

Les organismes gouvernementaux finlandais répartissent les technologies qu'ils utilisent en deux catégories :

- Les systèmes de base, qui sont des logiciels génériques au fonctionnement assuré par une entité conjointe, en coopération avec des partenaires externes.
- Les systèmes complexes, qui sont des systèmes spécifiquement adaptés aux besoins de chaque organisme. Trois entreprises participent actuellement à la gestion de la panoplie de technologies électorales utilisées.

La plupart des élections d'échelle nationale (à l'exception de celles d'Åland, des référendums municipaux et des élections parlementaires de la Laponie) recourent au système de données électorales du pays. Celui-ci est divisé en cinq sous-systèmes :

- le système de données de base (gestion des circonscriptions électorales, des autorités électorales et des personnes qui s'y réfèrent, des coordonnées, des bureaux de vote) ;
- le système de données sur le droit de vote (listes électorales et outils de mise à jour et d'analyses relatifs à ce domaine) ;

- le système de données sur les candidats (partis, candidats aux élections, enregistrement des candidats) ;
- le système de calcul des résultats (tabulation des votes et décompte des voix) ;
- le système de publication des résultats (publications officielles concernant les résultats électoraux et diverses statistiques).

Le système de données électorales est la propriété du ministère de la Justice. Les données qu'il contient appartiennent conjointement au ministère de la Justice et au registre juridique, tandis que sa gestion et son fonctionnement sont la responsabilité du centre juridique de la Finlande pour les registres d'informations. Ce système a été conçu sur mesure par cinq entreprises. Basé en ligne, il offre différents niveaux d'accès par catégorie d'utilisateurs. La plupart de ses fonctionnalités ne sont actives qu'à des dates et à des heures définies. Un système distinct permet aux électeurs d'accéder à des informations publiques. La conception du système a commencé en 2002, et il est entièrement opérationnel depuis 2012.

En 2017, à la suite d'une étude sur le vote électronique, la Finlande a décidé de ne pas recourir à cette méthode, principalement pour des raisons de sécurité, notamment concernant le degré de protection des appareils des utilisateurs finaux et les coûts élevés qu'entraînerait le maintien d'un système sûr. En 2019, seule la province autonome d'Åland proposait à sa population réduite de 30 000 personnes de voter en ligne, nombre d'entre elles résidant à l'étranger.

Risques

Les composantes les plus à risque du système de données électorales sont les suivantes :

- les listes électorales, en raison des données sensibles et personnelles qu'elles contiennent (qui sont directement tirées du registre d'état civil) ainsi que de la nécessité de fournir des copies papier de ces données dans les bureaux de vote ;
- le système de calcul des résultats, qui est utilisé dans tous les lieux de vote pour saisir les résultats ;
- le système de publication des résultats, qui sert à leur diffusion par canaux distincts sur le site du ministère de la Justice et dans les médias.

Les organismes finlandais prennent au sérieux les menaces informatiques auxquels ces systèmes sont exposés, en particulier provenant de pirates qui agiraient par idéologie et pourraient donc se montrer très tenaces. Cependant,

certains des outils employés par des entités adverses disposant de larges ressources et représentant une menace complexe et persistante pourraient également être à la portée d'individus inoccupés qui se montreraient eux aussi suffisamment patients et déterminés pour mener des attaques réussies. Face à des risques accrus, l'OGE finlandais s'est vu accorder une hausse considérable de son budget pour mettre en place des mesures de protection supplémentaires. Les dispositifs de secours adoptés comprennent l'enregistrement sur papier de tous les processus critiques afin de permettre leur vérification indépendamment des systèmes informatiques.

Collaboration entre organismes

En dehors de la collaboration avec le registre d'état civil pour la constitution des listes électorales, les technologies relatives aux élections sont placées sous la responsabilité de six organismes :

- le département des élections du ministère de la Justice, qui est chargé de leur gestion globale ;
- le centre de services en matière de TIC, qui est directement responsable du système d'informations électorales ;
- trois prestataires privés de services relatifs aux TIC ayant signé un contrat avec le ministère de la Justice ;
- l'agence de l'État pour les technologies de l'information ;
- l'agence de l'État pour la sécurité informatique, au rôle consultatif, qui analyse les menaces existantes ;
- la police criminelle centrale, qui est chargée des enquêtes.

Il est nécessaire d'entreprendre des activités de collaboration supplémentaires avec la nouvelle agence responsable du système d'identification central et de l'identité numérique à l'échelle de l'ensemble des pouvoirs publics.

Les organismes précédemment cités coopèrent depuis des décennies. Cependant, en 2016, l'OGE a pris l'initiative de renforcer la collaboration. La vulnérabilité des élections face aux risques pesant sur leur sécurité ayant été reconnue, l'agence pour la sécurité informatique et la police judiciaire constituent désormais des acteurs plus importants de cette collaboration. Les élections et d'autres processus gouvernementaux ne sont pas considérés comme des infrastructures essentielles, cette désignation étant le plus souvent employée dans un contexte militaire.

L'année 2017 a vu le démarrage de nouvelles activités de collaboration avec des ministères et le milieu universitaire concernant l'adoption du vote par correspondance et les débats soulevés par l'institution du vote électronique. Bien que le vote par correspondance et un nouveau système informatique dédié aient

été mis en place, le vote électronique n'a pas été universellement instauré en raison des préoccupations concernant sa sécurité.

La collaboration entre les organismes finlandais comporte différents aspects :

- Des réunions à propos de différents sujets, y compris la sécurité informatique, qui sont organisées à intervalle irrégulier et auxquels les organismes participent selon les besoins.
- Un suivi continuellement mis à jour des risques et l'adoption de mesures d'atténuation de ces derniers fondées sur les évaluations et renseignements disponibles à leur égard ; une évaluation du contexte informatique, y compris de l'évolution récente de la situation internationale, est conduite à l'occasion de chaque élection.
- L'élaboration de plans de gestion de crise incluant toutes les parties prenantes et précisant les capacités en matière d'enquête.
- Des exercices et des simulations (principalement en salle) consistant en l'analyse étape par étape des situations envisagées, la clarification de la répartition des rôles, la préparation d'enquêtes et la gestion d'incidents.

La plupart de ces activités de collaboration sont informelles et peu d'informations sont publiées. Seul le ministère de la Justice reçoit des rapports écrits à leur sujet. Les acteurs du secteur de la sécurité ne considèrent pas forcément que les élections relèvent de leur responsabilité. Des barrières linguistiques et culturelles font obstacle à la collaboration entre les parties prenantes relevant du gouvernement/du domaine législatif et du secteur militaire.

Bien que l'OGE soit en contact avec les fournisseurs de médias sociaux, il ne se considère pas comme responsable des fausses informations qu'ils diffusent. Il ne considère pas non plus que la sécurité des technologies utilisées par les partis politiques est à la charge du gouvernement.

Concernant les campagnes d'influence par l'information, y compris sur les médias sociaux, le gouvernement finlandais entretient un système de contre-propagande interinstitutionnel pour coordonner ses réponses avec les organisations non gouvernementales (ONG) et les médias. Le centre d'excellence contre les menaces hybrides de l'Union européenne se trouve également à Helsinki. Cette plate-forme inter-organisationnelle est chargée de sensibiliser la population aux activités adverses en matière d'information, de former les autorités électorales locales et d'informer les médias et le grand public des mesures de protection des élections. Elle sert également de réseau aux agences gouvernementales qui effectuent un suivi international des médias traditionnels et des médias sociaux.

Concernant les communications publiques en général, le bureau du Premier ministre finlandais a publié en 2016 des directives gouvernementales centrales qui soulignent l'importance de la collaboration entre agences :

> Une coopération efficace entre les autorités, un haut niveau général d'éducation, une bonne éducation aux médias et le respect des bonnes pratiques journalistiques par ces derniers constituent les meilleures défenses contre les campagnes d'influence. Il est important de rapidement contrer la diffusion d'informations trompeuses visant à manipuler l'opinion en faisant circuler les informations exactes. Il convient de prendre des mesures spécifiques pour garantir la facilité d'accès aux informations véridiques et fiables que les autorités gouvernementales publient.

Géorgie

Structure de l'OGE

La commission électorale centrale (CEC) de Géorgie est un organe administratif indépendant, libre de toute influence des autres instances de l'État. Elle a pour responsabilité de préparer et de réaliser les référendums, les plébiscites, les élections présidentielles et législatives, ainsi que les élections des organes représentatifs (*sakreboulo*) et exécutifs (maire/*gamgebeli*) des gouvernements autonomes locaux. La CEC compile les données des listes électorales établies par l'Agence de développement des services publics du ministère de la Justice.

Usage des TIC

La CEC utilise, entre autres, les technologies suivantes :

- un système de gestion des élections ;
- un système de traitement des résultats et de transmission des données à partir des districts ;
- un site Internet public ;
- des listes électorales consultables permettant de vérifier les données personnelles ;
- une interface affichant les résultats des élections.

Une technologie de dépouillement des votes est actuellement à l'étude.

Risques

À l'été 2008, la Russie a mené une guerre éclair, mais intense contre la Géorgie. Outre les affrontements physiques, les attaques informatiques se sont multipliées dans l'ensemble du pays, ciblant des organismes gouvernementaux, des ministères, des médias et des forums en ligne. Cette guerre est à l'origine des initiatives suivantes :

- La création de l'Agence d'échange de données en 2010, relevant du ministère de la Justice et dont les fonctions principales ont trait à la gouvernance électronique, à l'échange de données, et à la sécurité des infrastructures et des informations.
- La création de l'équipe d'intervention d'urgence informatique (cert.gov.ge, CERT) en 2011, relevant de l'Agence d'échange de données du ministère de la Justice ; sa mission est d'identifier, d'enregistrer, d'analyser et de résoudre les incidents perturbant les infrastructures essentielles et les réseaux gouvernementaux.
- Le vote de la loi sur la sécurité de l'information (2012).
- La désignation de la CEC et des élections en tant qu'infrastructures essentielles, ce qui contraint la CEC à aligner son système de gestion de la sécurité de l'information sur les exigences de la norme ISO 27001.

Depuis 2008, aucun incident de piratage majeur n'a perturbé les processus électoraux en Géorgie.

La politique de gestion des risques de la CEC repose sur trois principes : la confidentialité, l'intégrité et la disponibilité. La plupart des informations gérées par la CEC étant publiques, l'intégrité et la disponibilité font donc figure de priorités absolues ; les sites Internet et les systèmes en ligne sont les plus exposés aux risques. Les informations confidentielles se limitent essentiellement aux données personnelles apparaissant sur les listes électorales. Ces dernières sont publiques et disponibles en ligne ; mais l'accès aux données personnelles est protégé et requiert la saisie du numéro d'identification personnelle.

Collaboration entre organismes

La CEC et son service informatique et de sécurité de l'information sont responsables de la sécurité des systèmes TIC utilisés dans le cadre des processus électoraux. L'Agence d'échange de données et la CERT se tiennent prêtes à fournir une aide d'urgence en cas d'incidents de piratage. La CEC bénéficie de l'appui et des conseils de la CERT, entre autres, sur l'application des mesures de sécurité nécessaires du fait de sa condition d'infrastructure essentielle ; par exemple, la mise en place d'un système de gestion de la sécurité de l'information.

La CEC et la CERT tiennent des réunions en fonction des besoins. La CERT fournit des informations et des recommandations relatives aux faits nouveaux et aux domaines dans lesquels la sécurité doit être renforcée, outre des conseils sur l'achat de nouveaux systèmes TIC.

La CEC maintient également un accord de coopération avec la police, qui lui apporte son aide lorsqu'un incident survient. Dans les domaines où la CEC manque de ressources internes, comme la protection contre les attaques DDoS, elle travaille étroitement avec le secteur privé et les fournisseurs de services Internet. La CEC n'entretient pas de contacts officiels avec les fournisseurs de médias sociaux, mais pourra être amenée à le faire si à l'avenir les processus électoraux font l'objet de campagnes de désinformation.

Aucune stratégie proactive de communication publique en matière de sécurité informatique n'est menée en amont des élections ; par ailleurs, les parties prenantes adressent rarement des questions à la CEC. Néanmoins, une politique de gestion des incidents a été mise en place. Elle définit les rôles et les responsabilités y afférents, ainsi que le moment opportun pour la communication publique et les annonces dans les médias.

Lettonie

Structure de l'OGE

En Lettonie, la commission électorale centrale (CEC) est l'organe indépendant responsable des différents scrutins – élections législatives (parlement/*Saeima*), élections municipales (communes rurales et petites villes) et élections du Parlement européen, ainsi que les référendums nationaux. La CEC déploie les commissions électorales régionales (119 bureaux de vote régionaux) et municipales (1 100 bureaux de vote locaux).

Le Parlement élit le président et sept membres de la CEC. La Cour suprême élit en plénière un membre de la CEC parmi les juges. Dans la pratique, le président et le vice-président de la CEC sont indépendants, tandis que les autres membres représentent des partis.

La chancellerie de l'État comprend le Cabinet du Premier ministre et les services rattachés. Elle prépare les réunions du cabinet et coordonne la planification des politiques nationales ; elle joue également un rôle de coordination et de prévention en matière de sécurité informatique. Elle organise des cours et des formations pour l'OGE, ainsi que pour les médias publics et privés. Les formations portent sur la prévention, les interventions en cas de crise et la communication avec les médias.

Usage des TIC

Les TIC jouent un rôle mineur dans les élections en Lettonie : il n'existe ni vote électronique ni liste électorale. Pour prouver leur identité et voter, les Lettons

doivent présenter leur passeport au bureau de vote. Le dépouillement s'effectue dans des bureaux décentralisés, où les bulletins de vote sont scannés et projetés sur un grand écran, de sorte que toutes les personnes présentes puissent surveiller le processus. Le système de gestion des résultats est indépendant des serveurs de l'OGE et n'est déployé que pendant la période électorale. L'OGE transmet les résultats par voie électronique, mais fait des sauvegardes sur papier.

En Lettonie, les élections constituent des infrastructures essentielles. Dans la pratique, ce statut a une incidence sur les institutions concernées, les normes appliquées et les normes obligatoires de sécurité, et garantit la fourniture d'un soutien 24 heures sur 24, sept jours sur sept en cas de crise.

Risques

Les coupures d'électricité et d'Internet sont considérées comme des risques et ont donné lieu à l'élaboration de plans de sauvegarde. Pour sa part, la chancellerie de l'État estime que les rapports tendancieux représentent un risque plus grave que le piratage informatique des technologies électorales.

Dans son histoire récente, la Lettonie a été épargnée par la diffusion de fausses informations visant à perturber les élections et par les stratégies de suppression d'électeurs directs. Mais 20 ans de flux d'informations russes ont entraîné la suppression d'électeurs indirects, ce qui, d'après la chancellerie de l'État, nuit aux affaires courantes du pays et les déstabilise. Par exemple, les informations russes transmettent une mauvaise image de l'OTAN et accordent une attention disproportionnée à seulement deux des partis politiques lettons.

Collaboration entre organismes

En Lettonie, le Groupe de travail sur la sécurité informatique des processus électoraux encadre la collaboration entre organismes et comprend, entre autres membres :

- l'Équipe d'intervention d'urgence informatique (CERT) ;
- le Service de sûreté de l'État ;
- le Centre de la radio et de la télévision publiques de Lettonie, qui veille à la sécurité des télécommunications, entre autres, en assurant la protection contre les attaques DDoS ;
- les entreprises privées qui conçoivent les logiciels pertinents ;
- d'autres acteurs intervenant de manière ponctuelle.

Les membres du groupe de travail collaborent avec l'OGE en prenant soin de préserver son indépendance. En juillet 2018, la chancellerie de l'État a également

mis sur pied une équipe spéciale de lutte contre la désinformation, chargée des activités suivantes :

- surveiller les informations sur les influences externes publiées dans les médias traditionnels et les médias sociaux ;
- collaborer avec les médias sociaux, les ONG et les partis politiques ;
- instruire l'OGE.

L'équipe spéciale veille à ce que les informations émanant de la Russie n'exercent pas une influence indue sur les médias lettons ou l'opinion des citoyens. Pour contrecarrer les informations douteuses, elle :

- met au point des scénarios de campagnes de désinformation (avant, pendant et après les élections) et réalise des simulations avec les forces de l'ordre, la CEC et les médias pour qu'ils apprennent à réagir en cas d'incident ;
- forme les médias, les forces de l'ordre et la CEC (avec l'aide de Google) au fonctionnement des médias sociaux, en se centrant sur la vérification des sources, et l'identification des fausses informations, des trolls et des bots sur les médias sociaux.

L'équipe spéciale a été lancée en amont des élections générales du 6 octobre 2018. Le Cabinet du Premier ministre a décidé d'installer l'équipe spéciale au sein de la chancellerie de l'État, afin qu'elle puisse instaurer une coordination la plus efficace possible avec tous les services concernés et les agences de sécurité. L'équipe spéciale tient des réunions de manière ponctuelle et en cas de besoin.

Mexique

Structure de l'OGE

L'Institut national électoral du Mexique (INE) est un organisme autonome et permanent, responsable de l'organisation et de la supervision des élections fédérales au Mexique, qui collabore également avec les OGE locales pour la tenue des élections locales. Le Conseil général est son instance suprême de direction.

Les responsabilités et le mandat de l'INE se sont étoffés au fil du temps et couvrent aujourd'hui la formation électorale et l'éducation civique à l'échelle nationale, la délimitation des circonscriptions et l'inscription sur les listes électorales, le choix des bureaux de vote et la désignation de leur personnel, les règles relatives aux résultats préliminaires, les sondages d'opinion, le

dépouillement rapide et le matériel électoral, ainsi que la surveillance des partis politiques et du financement des campagnes électorales. Le Tribunal électoral est un organisme autonome chargé de résoudre les différends électoraux.

Usage des TIC

Les systèmes internes de l'INE s'appuient sur des technologies de pointe, dont les pare-feux, les services d'informatique en nuage et 35 systèmes d'information. L'INE confie le suivi de ses systèmes à des fournisseurs tiers.

Le vote électronique est réservé aux Mexicains résidant à l'étranger, mais en 2018, seuls 3 000 électeurs ont eu recours à cette méthode. L'INE compte augmenter les capacités en matière de vote électronique en vue de prochaines élections, mais se heurte à des problèmes techniques (par exemple, l'absence d'identification électronique) et politiques.

Risques

On relève des tentatives d'attaques DDoS et d'autres actes de piratage informatique depuis de nombreuses années. L'INE utilise plusieurs technologies en ligne qui sont donc vulnérables aux menaces informatiques, à savoir :

- le site Internet et les applications en ligne ;
- le système de suivi des bureaux de vote ;
- les interactions qui requièrent que le système soit disponible.

L'INE est habilité à intervenir en cas de désinformation ciblant directement les électeurs sur les médias sociaux, mais n'est pas compétent pour traiter les messages problématiques, comme les fausses informations. Pour lutter contre la désinformation concernant la situation dans les bureaux de vote, l'INE a mis au point une application mobile qui permet aux équipes de suivi d'inspecter les bureaux de vote le jour du scrutin, d'examiner les éventuels problèmes et de porter les messages devant être supprimés à la connaissance de l'INE (qui à son tour prévient les fournisseurs de médias sociaux). C'est à la suite d'un incident en ligne que l'INE a entamé sa collaboration avec les médias sociaux en 1998 ; aujourd'hui il travaille étroitement avec la division politique de Google, et a conclu des mémorandums de coopération avec Facebook (El Universal, 2018) et avec Twitter (INE, 2018).

Il exerce en outre un suivi financier des médias. Par exemple, les partis politiques n'ont pas le droit d'acheter du temps d'antenne. L'INE a également conclu des arrangements avec Facebook et Twitter pour surveiller le respect des règles par les partis politiques. Les campagnes en ligne menées depuis des sites Internet situés en dehors du Mexique ne relèvent pas de la compétence de l'INE.

Collaboration entre organismes

Fruit d'une approche descendante, la collaboration entre organismes en matière de sécurité des élections existe depuis de nombreuses années au Mexique. L'INE collabore avec un large éventail d'acteurs :

- le milieu universitaire ;
- l'équipe d'intervention d'urgence de l'Agence nationale de la sécurité ;
- les opérateurs de télécommunications, qui bloquent toute modification des systèmes pendant la semaine précédant les élections ;
- les fournisseurs d'électricité, pour réduire au minimum les coupures de courant ;
- le secteur du bâtiment et des travaux publics, afin de stopper tout travail de construction le jour du scrutin et d'éviter toute perturbation.

La supervision de la sécurité des technologies électorales comprend trois niveaux :

- un groupe de sécurité interne rassemblant 15 experts ;
- un groupe de sécurité externe qui contrôle les systèmes par l'intermédiaire d'une société privée ;
- le milieu universitaire, qui assure le troisième échelon de vérification et consolide la confiance dans les systèmes.

À l'heure actuelle, la désignation des élections en tant qu'infrastructures essentielles fait l'objet d'un débat au Mexique. Le processus d'attribution des marchés publics, fortement transparent, risque de faciliter la divulgation d'informations sensibles pendant les appels d'offres. La liberté de s'enquérir d'informations sensibles suscite des inquiétudes similaires. En donnant aux élections le statut d'infrastructures essentielles, il serait possible de limiter la transparence dans ces domaines.

Moldavie

Structure de l'OGE

En République de Moldavie, la CEC est autonome et indépendante du pouvoir exécutif. À l'exception de la Commission électorale de l'Entité territoriale autonome de Gagaouzie, les OGE de niveau inférieur, placés sous la juridiction de la CEC, ont pour responsabilité d'organiser les élections à l'échelon

infranational. Le système d'inscription sur les listes électorales est passif et automatique. La liste des électeurs est tirée du Registre national des électeurs, qui est lui-même relié au Registre national de la population, mis à jour quotidiennement.

Usage des TIC

La CEC a recours aux nouvelles technologies pour réaliser une série d'activités :

- Les résultats sont présentés sur support papier et sous forme électronique.
- Chaque bureau de vote compte un double mécanisme de vérification des électeurs : les listes électorales sont à la fois sur papier et numériques.
- La CEC extrait les listes électorales du Registre national des électeurs, qui est tenu par ses représentants.
- Le site Internet de la CEC retransmet en direct le dépouillement dans les bureaux de vote.

Risques

Les listes électorales sont reliées par Internet aux serveurs de la CEC. Il existe un risque d'attaque informatique le jour du scrutin, lorsque chaque municipalité intègre les données émanant des bureaux de vote dans les listes électorales avant de transmettre ces dernières à la CEC. Compte tenu de la nature décentralisée du système, il suffit qu'un seul système soit perturbé, à la suite d'une erreur humaine ou technique ou d'une attaque délibérée, pour compromettre la crédibilité des autres modules reliés au registre, comme les listes électorales et les listes de candidats.

Collaboration entre organismes

Pour parer à ces risques, en 2014, la CEC a créé un groupe de travail conjoint avec le Service de sécurité informatique et des technologies de l'information et le Service de renseignement et de sécurité, qui traite des menaces possibles, prévoit des scénarios d'intervention et définit la répartition des rôles. Ces services s'alignent sur la norme ISO 27001 relative à la sécurité de l'information, notamment pour la mise au point des procédures de planification et d'intervention correspondant à différents scénarios. Dans certains cas, des acteurs tels que le ministère de l'Intérieur et les fournisseurs de services Internet entrent également en jeu.

Le groupe de travail se réunit seulement six mois avant la tenue d'élections puis quotidiennement pendant la dernière semaine de la campagne ; le jour du scrutin, il est présent sur le terrain. Les élections se tenant généralement tous les ans, cette collaboration s'est renforcée, prouvant que la fréquence des élections influe

positivement sur l'intensité de la collaboration entre organismes. Des discussions sont en cours à propos de la gestion de certains équipements technologiques ; la CEC considère que sa responsabilité à cet égard est incompatible avec son rôle d'administrateur électoral.

La CEC confie certains de ses systèmes de communication aux services de sécurité. Ainsi, le Service de renseignement et de sécurité est chargé de rendre publiques les attaques DDoS. La coopération quotidienne entre la CEC et les organismes de sécurité s'effectue au niveau technique et opérationnel, les hauts responsables contribuant aux processus décisionnels selon les besoins.

La CEC ne travaille pas avec les fournisseurs de médias sociaux et n'est pas chargée d'informer le grand public sur les risques de sécurité informatique. Qui plus est, ni les organismes de sécurité ni la CEC ne fournissent un appui ou des orientations en matière de sécurité informatique au niveau local, même si la CEC considère que l'accès local aux listes électorales représente un grand risque.

Norvège

Structure de l'OGE

Le ministère norvégien des Collectivités locales et de la Modernisation est responsable de l'organisation générale et de la tenue des élections nationales et locales ; il définit par ailleurs le cadre juridique et approuve les programmes pilotes. Il fait également figure d'instance d'appel et traite les contentieux des élections locales.

La Direction des élections produit le système informatique centralisé utilisé pendant les scrutins, dispense des conseils et des formations aux autorités locales, et informe le grand public. Par ailleurs, elle fournit et distribue le matériel électoral et présente des informations sur les résultats des scrutins.

L'administration électorale est décentralisée. Les OGE sont présents au niveau des comtés et des municipalités. Le jour du scrutin, 30 000 agents électoraux assurent toutes les tâches pratiques, allant de la validation des listes des partis au comptage des bulletins de vote. Il est généralement considéré que la décentralisation contribue à la protection du processus électoral ; jusqu'à présent, aucune attaque ne s'est produite.

Usage des TIC

En Norvège, le système électronique d'administration des élections (*Elektronisk Valgadministrativt**) a été conçu pour les élections de 2013. Il couvre l'ensemble du processus électoral, de l'enregistrement des candidats au traitement des résultats, sans négliger la lecture optique des bulletins de vote et le marquage électronique de la liste électorale. En 2011 et 2013, un système de vote électronique a été mis à l'essai puis abandonné pour des questions de sécurité.

Risques

La sécurité du système informatique et électronique a été remise question en 2017, d'abord sur les médias sociaux puis dans les médias traditionnels. Dix jours avant le jour du scrutin, la promulgation d'une nouvelle réglementation a contraint toutes les municipalités à instaurer le dépouillement manuel pour établir les résultats préliminaires. Cette exigence sera à nouveau évaluée avant les prochaines élections.

Loin de remettre en question le système d'administration des élections, suffisamment testé et sécurisé, la réglementation avait pour but d'éviter toute spéculation et de dissiper toute incertitude quant aux résultats des élections de 2017, et de contribuer à instaurer un climat de sécurité et de confiance indispensable à toute élection.

Collaboration entre organismes

Dans le cadre des élections législatives de 2017, le ministère de la Justice, les autorités de sécurité nationales norvégiennes et les forces de sécurité ont entamé une coopération informelle pour :

- surveiller le système administratif électronique en vue de détecter et d'empêcher toute action informatique malveillante ;
- observer les activités des médias sociaux ;
- évaluer les menaces ciblant spécifiquement les élections ;
- fournir des informations aux partis politiques et aux parties prenantes clés ;
- fournir des conseils et des informations aux responsables des élections locales.

Cette collaboration est en cours de formalisation.

Pays-Bas

Structure de l'OGE

Aux Pays-Bas, les élections sont fortement décentralisées, ce qui ne favorise pas la collaboration entre organismes. Les rôles de l'OGE sont répartis entre la Commission électorale (*Kiesraad*), le ministère de l'Intérieur et les municipalités :

- Les 355 municipalités du pays ont pour principale responsabilité d'organiser les élections, par exemple en imprimant les bulletins de vote et en établissant 9 500 bureaux de vote.

- La Commission électorale se charge d'établir la liste des candidats, de compiler les votes à l'échelle nationale, de déclarer les résultats nationaux et d'en informer le gouvernement. Par le passé, elle a également mis des logiciels à la disposition des municipalités.
- La responsabilité du ministère de l'Intérieur est d'ordre politique et concerne la mise en œuvre de la loi électorale, et l'élaboration des politiques, des règles et des réglementations connexes. En cas de perturbation des élections, le Parlement peut demander des comptes au ministre de l'Intérieur.

S'agissant de la sécurité informatique des processus électoraux, le ministère de l'Intérieur assume trois rôles différents par l'intermédiaire de sa Direction des élections, des services généraux de renseignement et de sécurité, et du Centre national de sécurité informatique.

Usage des TIC

Aux Pays-Bas, les processus électoraux ont recours aux technologies suivantes :

- Les listes électorales sont extraites, par municipalités, du Registre des citoyens, qui est tenu et mis à jour par les autorités fiscales. Les listes électorales des bureaux de vote sont sur support papier, mais le traitement des données personnelles servant à établir les listes électorales relève des infrastructures électorales essentielles.
- Avec l'abolition du vote électronique en 2006, le principal système TIC toujours en place est le logiciel OSV, qui compile les résultats du dépouillement manuel et calcule les résultats des élections municipales.
- L'application sur tablette mesurant la participation électorale (StembureauApp) et les lecteurs de cartes d'identité.
- Certaines municipalités ont récemment utilisé des applications privées facilitant la tabulation des votes et l'obtention des résultats.

Risques

Le logiciel OSV représente à l'heure actuelle le principal facteur de risque pour la Commission électorale. En 2017, un groupe néerlandais de pirates à chapeau blanc a entrepris de démontrer les failles de sécurité d'OSV. S'ils n'ont pas convaincu la Commission électorale, les répercussions médiatiques et politiques de leur action ont cependant amené le ministre de l'Intérieur à renoncer soudainement à l'OSV, au grand dam des municipalités et de la Commission électorale.

Depuis, la sensibilisation du public et les débats sur OSV ont prouvé que la perception des risques en matière de sécurité informatique peut avoir des effets perturbateurs presque aussi importants que les interférences malintentionnées. Cela a également mis en évidence que les principes de sécurité et les logiciels d'hier sont loin d'être adaptés aux nouvelles menaces informatiques. Il ne suffit pas de mettre à jour les logiciels ; il faut également y soumettre les procédures et le matériel.

Collaboration entre organismes

Dans un contexte marqué par la sensibilisation du public et des médias aux enjeux de l'informatisation des processus électoraux, les nombreux acteurs concernés ont peiné à définir leurs rôles en matière de sécurité informatique des processus électoraux ; quant à la loi électorale, elle n'aborde pratiquement pas le sujet. Début 2018, un organisme externe a été chargé d'examiner les responsabilités de chacun et de définir une stratégie facilitant l'exercice de ces responsabilités, y compris en prévoyant l'appui politique, le savoir-faire et les ressources nécessaires.

S'appuyant sur son expérience des médias, la Commission électorale a pris trois mesures. Premièrement, anticipant des défaillances informatiques réelles ou perçues, elle a préparé des réponses toutes faites. Deuxièmement, chaque fois qu'elle adapte ses systèmes informatiques, elle veille à incorporer les critiques potentielles du public dans le processus. Troisièmement, elle confie à des experts informatiques externes le soin de relever les faiblesses potentielles.

Roumanie

Structure de l'OGE

L'Autorité électorale permanente (AEP) est l'OGE permanent de la Roumanie. Trois mois avant les élections, les bureaux de vote provisoires sont établis dans la capitale et dans les juridictions locales (pas moins de 3 000) en fonction du type de scrutin. Le Bureau électoral central, composé de juges, de commissaires et de représentants des partis, supervise les élections. Les bureaux électoraux locaux ont pour mission d'organiser les scrutins dans pas moins de 18 000 bureaux de vote. Leur responsabilité prend fin avec la proclamation des résultats officiels.

Les données des listes électorales sont extraites du registre civil tenu par le ministère de l'Intérieur ; c'est ainsi que les citoyens sont automatiquement enregistrés le jour de leurs 18 ans.

Usage des TIC

Les listes électorales (principaux systèmes informatiques utilisés entre les élections) sont tenues et régulièrement mises à jour par le personnel des mairies dans l'ensemble du pays. Cela permet aux bureaux électoraux de disposer de listes électorales actualisées le jour du scrutin.

L'AEP fournit à l'ensemble des bureaux électoraux les outils en ligne, accessibles depuis un réseau privé, qui permettent de réaliser des tâches telles que la gestion des bureaux de vote, la gestion des résultats, la transmission des données et la présentation des résultats en ligne. Les bureaux de vote utilisent un système électronique de contrôle de la participation électorale basé sur des lecteurs de cartes d'identité afin d'éviter les votes multiples et les votes émis par des électeurs qui n'en ont pas le droit. L'AEP utilise en outre un système de tabulation des résultats et d'attribution des sièges. De plus, l'OGE est présente sur Internet et fournit des données en ligne aux parties prenantes électorales pour la publication des résultats des élections.

La technologie a contribué de manière significative à renforcer la confiance des électeurs dans le processus électoral. Le nombre de réclamations concernant les listes électorales, l'usurpation d'identité des électeurs et la multiplication des votes a diminué ; le système a également mis un terme aux fraudes, dont le ramassage d'électeurs.

Risques

Les principaux risques de sécurité informatique concernent les listes électorales électroniques et d'autres systèmes en ligne de l'autorité électorale. Des mesures de protection informatique doivent être mises au point pour l'AEP et l'ensemble des bureaux électoraux ; la protection est basée sur le principe de résilience de tous les organes concernés.

Les mécanismes de protection consistent à préparer et analyser des scénarios, ainsi qu'à simuler les interventions suivant différentes infractions aux mesures de sécurité. La principale caractéristique en matière de sécurité, et par ailleurs possible option de remplacement, est la trace sur papier de l'ensemble du processus. En cas d'incident, la trace sur papier contient les informations officielles qui peuvent être utilisées pour examiner toute anomalie présentée par le système TIC.

Les systèmes électroniques ont subi de nombreuses attaques, dont les DDoS, le détournement du contenu des sites Internet, les escroqueries et l'injection SQL (langage d'interrogation structuré). Néanmoins, ces attaques n'étaient pas très sophistiquées ou n'ont pas causé de dommages importants.

La désinformation axée sur les systèmes informatiques de l'AEP constitue un vecteur d'attaque plus dangereux. Lors d'élections précédentes, les médias, interprétant de manière erronée des dossiers d'appel d'offres, ont dénoncé les défaillances du système informatique de l'AEP. Cela a gravement nui à la crédibilité des systèmes informatiques et de l'AEP en général. Ces incidents montrent qu'il est difficile de contrecarrer les désinformations concernant le processus électoral une fois qu'elles atteignent un large public.

Collaboration entre organismes

L'AEP ne possède pas d'équipe dédiée à la sécurité informatique. Son personnel informatique s'en occupe avec le soutien d'autres organismes. Si les élections ne sont pas officiellement des infrastructures essentielles, la plupart des parties prenantes électorales les considèrent cependant comme telles.

S'agissant du registre électoral, la CERT effectue des audits de sécurité et émet des recommandations annuelles à cet égard. Après une attaque, les « fichiers journaux » sont remis à la CERT pour analyse. Par ailleurs, une société privée réalise des audits de sécurité tous les deux ou trois mois.

Les années sans élections, l'AEP effectue les audits de sécurité de concert avec le Service spécial des télécommunications, doté d'un statut militaire, qui fournit des dispositifs de communication sécurisés à l'ensemble des institutions de l'État et coordonne les activités connexes. Ce service est également le principal collaborateur de l'AEP en matière de sécurité informatique. Leur coopération continue prévoit des audits de sécurité, qui sont effectués à chaque modification ou mise à jour des technologies électorales. Le ministère de la Défense fournit à l'AEP des infrastructures de sauvegarde, hors site, situées dans des installations militaires.

Les mesures de sécurité sont renforcées pendant les années électorales, d'où la collaboration avec CyberIT, une branche des services de renseignement roumains, qui a pour responsabilité d'assurer la sécurité informatique de l'ensemble des infrastructures étatiques. CyberIT réalise également, à l'échelle nationale, des exercices basés sur des scénarios rassemblant diverses institutions et un large éventail d'acteurs issus tant du milieu universitaire que des services secrets et de l'administration électorale. Compte tenu du passé parfois sombre des services de renseignement en Roumanie, la coopération entre les services d'intelligence et d'autres acteurs publics fait débat.

Depuis 2016, dans le sillage de la campagne médiatique qui a entamé la confiance dans la technologie de l'AEP, la commission invite les partis politiques à mandater des experts pour contrôler les technologies électorales dans leur ensemble, y compris en examinant les codes sources correspondant au traitement des résultats et au calcul des mandats. Les représentants des partis sont autorisés à essayer et à vérifier ces systèmes sur leur ordinateur personnel et à y reproduire l'ensemble du processus d'obtention des résultats. Ils peuvent également participer à une démonstration se tenant peu avant et après les élections et prouvant que le système soumis à leur examen est réellement celui utilisé par l'AEP.

La Roumanie n'a subi aucune vaste campagne de désinformation nationale ou venant de l'étranger. Si les mesures techniques sont en place depuis longtemps, les anciennes rumeurs et légendes urbaines concernant, par exemple, les doubles votes et les électeurs décédés figurant sur les listes électorales, ont encore un écho auprès de la population.

Les programmes de formation à l'hygiène informatique destinés aux partis politiques sont centrés sur la protection des informations internes et des données relatives aux élections fournies par l'AEP. Toute attaque ou fuite de données émanant des partis politiques peut donc être perçue comme une attaque réussie contre l'AEP.

Royaume-Uni

Structure de l'OGE

Au Royaume-Uni, les élections sont organisées par les directeurs de scrutin indépendants intervenant au sein des autorités locales et, en Irlande du Nord, par le directeur général des élections. La Commission électorale du Royaume-Uni, organe régulateur indépendant, est chargée de leur supervision, de l'enregistrement des partis, de la réglementation du financement des partis politiques, de la recherche, de l'établissement des normes, et de fournir un appui à la tenue des élections et des référendums sur l'ensemble du territoire national. Le gouvernement est responsable du Code électoral et des modifications de la loi, mais s'appuie pour cela sur les rapports et le travail politique global de la Commission.

Usage des TIC

Le vote électronique n'existe pas au Royaume-Uni. Les préposés à l'inscription sur les listes électorales interviennent au niveau local et il n'existe pas de registre électoral centralisé. Les votes et le dépouillement du scrutin sont des processus manuels, mais plusieurs applications des TIC sont en place :

- un système permettant de soumettre en ligne les demandes d'inscription sur les listes électorales des autorités locales ;
- un logiciel de gestion des élections qui couvre l'administration des registres et des élections ;
- une base de données sur les contributions financières destinées aux partis ainsi qu'un système de soumission en ligne ;
- un logiciel de consolidation des résultats mis au point pour le Référendum sur l'appartenance à l'Union européenne de 2016.

Risques

Le système électronique d'inscription sur les listes électorales est disponible sur le site Internet du gouvernement britannique, qui est tenu par le Département du numérique relevant du Cabinet du gouvernement. Ce système d'inscription sur les listes électorales est de plus en plus populaire auprès des citoyens. Étant

disponible sur un site Internet public, il est susceptible de faire l'objet d'attaques. Parmi les garde-fous et les options de remplacement, citons les méthodes d'inscription traditionnelles effectuées manuellement par le personnel local et les contrôles supplémentaires qui soumettent l'utilisation du système à la saisie de données personnelles.

Les autorités locales utilisent des systèmes de gestion électorale conçus par quatre prestataires. Les principaux risques pesant sur les systèmes hors ligne sont les attaques avec demande de rançon, les logiciels malveillants et la divulgation illicite de données personnelles. Si aucun incident n'a été signalé, le Centre national de sécurité informatique (NCSC) a diffusé des orientations aux autorités locales portant, entre autres, sur la sécurité, la sensibilisation et le comportement du personnel. La plupart des données sont détenues de manière séparée par les autorités locales, ce qui limite la portée des attaques individuelles.

Parallèlement au système électronique de consolidation des résultats, conçu à l'origine pour le Référendum sur l'appartenance à l'Union européenne de 2016, un système de sauvegardes sur papier est en place. La diffusion de données des élections aux médias et d'autres canaux de communication de résultats représentent également des facteurs de risque.

Pour les partis politiques, la fuite des données personnelles d'individus et de sympathisants, les logiciels malveillants et les attaques avec demande de rançon sont les principaux facteurs de risque.

Le numérique ne jouant qu'un rôle mineur dans les processus électoraux, jusqu'à présent, exception faite de quelques théories conspirationnistes, les menaces informatiques n'ont pas vraiment entamé la confiance des électeurs. Les élections n'ont pas le statut d'infrastructures essentielles au Royaume-Uni. Cependant, les processus manuels ne sont pas sans risques : des erreurs peuvent se produire et le vote par correspondance peut poser des problèmes ; par le passé, des voix se sont élevées pour critiquer la manipulation des votes par correspondance.

Pour la Commission électorale et le NCSC, le caractère évolutif des menaces informatiques et des entités adverses constitue un défi de taille. Il faut trouver des solutions pour faire face à l'émergence de nouvelles menaces dans un environnement en pleine mutation. Par conséquent, la définition des risques de sécurité informatique change d'une élection à l'autre.

Nombre de défis liés à l'utilisation d'Internet ont trait aux campagnes numériques, au microciblage et aux répercussions subies par les entreprises de médias sociaux, les partis et le gouvernement, sans compter la nécessité de doter la Commission électorale de pouvoirs supplémentaires en matière d'accès à l'information, de respect des règles et de sanction des auteurs d'infractions.

Collaboration entre organismes

Au Royaume-Uni, outre la Commission électorale, un large éventail d'organismes ont pour mandat d'assurer la protection des élections contre les attaques

informatiques, dont le NCSC, le Commissaire à l'information, le groupe constitutionnel du Bureau du Cabinet (en particulier pendant la période précédant les élections), l'Agence nationale de lutte contre la criminalité et la police.

La sécurité des différentes applications des TIC présentées ci-dessus est la responsabilité principale de leurs titulaires, qui sont souvent des administrations locales. La Commission électorale du Royaume-Uni n'est donc pas directement responsable de la protection contre de nombreux risques de sécurité informatique. Néanmoins, en cas de problème, même à l'échelle locale, la Commission électorale est automatiquement référente, car elle est l'organe électoral ayant le plus de visibilité. Si elle ne peut pas protéger (et ne protège pas) les administrations locales, elle peut cependant émettre des recommandations à la suite d'une défaillance du système de sécurité local.

La Commission électorale collabore avec le NCSC depuis 2016, après la mise en évidence des ingérences étrangères dans les élections présidentielles aux États-Unis. Depuis, le NCSC joue un rôle de coordination important bien qu'informel avec la Commission électorale et le groupe constitutionnel au sein du Bureau du Cabinet. Ses tâches officielles consistant à fournir des orientations et un appui à la gestion des incidents, sa mission dans le cadre des élections est de recenser les risques y afférents et de conseiller ces organes. Le NCSC se concentre essentiellement sur les élections générales, mais offre également son assistance pour les élections locales. Les organismes tiennent des réunions ponctuelles, en fonction des besoins et lorsque des risques sont identifiés ; la fréquence des réunions s'intensifie avec la proximité des élections. À l'échelle locale, le NCSC publie un manuel sur la sécurité informatique destiné aux scrutateurs et fournit des conseils à l'association des administrateurs électoraux.

Les campagnes des partis politiques sur Internet et la diffusion d'informations fausses et trompeuses sur les médias sociaux sont une grande source de préoccupation pour la Commission électorale, mais ne relèvent pas directement de son mandat, contrairement à d'autres sujets d'inquiétude connexes, comme la confiance des électeurs et le financement des partis (y compris le financement des campagnes sur Internet). La Commission émet d'ailleurs des recommandations législatives à cet égard.

Sa juridiction se limite au territoire du Royaume-Uni. Elle considère que les ingérences étrangères dans les processus électoraux sont la responsabilité première des agences nationales chargées de la sécurité. Le Commissaire à l'information du Royaume-Uni est chargé de superviser l'intégrité des données et l'utilisation des données personnelles des citoyens.

Le NCSC et le Centre national pour la protection des infrastructures ont diffusé des exposés, des orientations et des informations sur les bonnes pratiques de sécurité informatique que doivent suivre les responsables des systèmes étayant la tenue des élections au Royaume-Uni. Citons, entre autres, les orientations

destinées aux partis politiques relatives aux risques de violation des données, y compris les attaques par hameçonnage ou par harponnage, et la présentation de preuves de tentatives récentes. Suivant à un protocole rigoureux visant à ne pas heurter les sensibilités politiques, le NCSC informe régulièrement les partis politiques et les candidats aux élections, en vue de leur rappeler l'existence des risques de sécurité informatique. Le NCSC traite en outre des questions liées à la sécurité informatique avec les médias audiovisuels.

L'importance attachée à la sécurité informatique et le vif intérêt manifesté à l'égard des élections étayent la collaboration intergouvernementale et entre les organismes. Compte tenu du mandat restreint de la Commission électorale et des responsabilités électorales de nombreux organismes, les partenariats et la collaboration avec d'autres organismes revêtent une importance capitale.

Si les activités de chaque organisme sont généralement clairement établies, leurs responsabilités ne sont pas définies dans la législation ni dans les procédures. La Commission électorale a donc dû acquérir une compréhension approfondie du rôle de chaque organisme.

La collaboration, largement informelle, s'est intensifiée de manière organique au fil du temps. Elle se déroule sous forme de réunions individuelles, de dialogue régulier, de partage des informations et de planification des interventions d'urgence. La Commission électorale coopère étroitement avec le Commissaire à l'information.

Tous les acteurs étant rarement réunis autour d'une même table, la Commission électorale du Royaume-Uni joue un rôle déterminant dans l'organisation de ces échanges d'informations. Puisqu'un excès d'exigences ne semble pas indiqué dans un tel contexte, la Commission peut fournir des conseils et son expertise, et s'assurer que les messages appropriés sont rendus publics.

À des fins de communication publique, la Commission électorale a défini des stratégies relatives à la gestion des incidents liés aux élections et à la diffusion de messages renforçant la confiance des citoyens, qui attendent des réactions rapides et crédibles.

Bien qu'aucun membre du personnel de la Commission électorale ne se consacre exclusivement aux menaces informatiques, une petite équipe est disponible pour prendre en main les problèmes ayant trait aux médias sociaux et communique régulièrement avec les fournisseurs de médias sociaux.

Le chef de file de l'intervention faisant suite à un incident dépend du type de menace. Quelques exercices visant à assurer la sécurité des élections ont également eu lieu. Dans l'ensemble, la volonté de coopérer dépend de la menace ; elle est généralement limitée en dehors des périodes électorales. Les services de sécurité responsables de l'évaluation des risques doivent déterminer l'utilisation de leurs ressources et n'interviennent que s'ils considèrent le risque suffisamment grave.

Suède

Structure de l'OGE

En Suède, l'administration électorale est fortement décentralisée. Le principal organisme, l'Autorité électorale suédoise (*Valmyndigheten*), emploie quelque 20 personnes à temps plein et fournit une assistance et des conseils à 21 comtés, qui ont chacun une ou deux personnes en charge des élections. Au niveau administratif suivant, on recense 291 municipalités. Environ huit à neuf mois avant le jour du scrutin, le personnel électoral de chaque comté et municipalité passe d'une ou trois à environ dix personnes au service de l'administration centrale. Le personnel des bureaux de vote reçoit également des renforts importants à chaque élection.

Le mandat de l'Autorité électorale est principalement centré sur la planification et la mise en œuvre du processus électoral, dont l'enregistrement des partis, la fourniture du matériel électoral (entre autres, les listes électorales, les cartes d'électeur et les bulletins de vote), la diffusion d'informations sur le processus électoral auprès des électeurs, et la conception et l'entretien des systèmes informatiques pour le traitement des résultats électoraux. La supervision des campagnes, les activités des médias sociaux en lien avec les élections, l'éducation des électeurs et les appels à voter ne sont pas des responsabilités qui lui incombent. Toute activité illégale concerne les organismes de sécurité ou les forces de l'ordre public.

Usage des TIC

La gestion des élections en Suède est principalement manuelle. Tous les éléments clés du processus électoral sont sur support papier ; la technologie n'intervient que pour accroître l'efficacité. Cependant, il semble inévitable que la technologie joue un rôle croissant lors des élections à venir.

Le dépouillement électronique fait seulement figure de système parallèle et superflu. L'Autorité électorale utilise un système informatique centralisé pour la transmission et la tabulation des résultats et l'attribution des sièges. Ce système est le principal actif placé sous son autorité. Un autre système numérique transmet les résultats des élections aux médias.

L'administration fiscale produit les données sur tous les résidents pour l'établissement des listes électorales et met à la disposition de l'Autorité électorale son site Internet et les infrastructures connexes. À l'heure actuelle, l'Autorité électorale n'est pratiquement pas présente sur les médias sociaux.

Risques

La sécurité de l'ensemble des systèmes informatiques électoraux est assurée en tout temps, conformément aux normes industrielles ; des mesures de sécurité

supplémentaires pendant les périodes électorales ne sont pas nécessaires. Les attaques informatiques de faible ampleur, telles que les attaques DDoS, peuvent survenir à n'importe quel moment, y compris entre les élections, mais cela ne perturbe pas le fonctionnement de l'Autorité électorale ou de ses systèmes. Des plans de continuité des opérations sont en place pour parer à toute défaillance du système, et il est possible de basculer vers des procédures manuelles, sur support papier à tout moment.

Une importance capitale est accordée à la protection des données, car la fuite ou la perte de données sont des problèmes encore plus difficiles à résoudre que les défaillances du système. Les risques de sécurité informatique sont donc étroitement liés à la sécurité des informations, qu'il s'agisse de désinformation ou de violation des données. La protection des systèmes au niveau municipal est un autre domaine important, compte tenu des ressources limitées disponibles à ce niveau.

Collaboration entre organismes

Chaque année, l'ensemble des autorités suédoises reçoivent les instructions écrites du gouvernement définissant clairement toutes leurs responsabilités. Si les élections ne sont pas explicitement considérées comme telles, depuis 2017, elles font de plus en plus office d'infrastructures essentielles nationales. De ce fait, l'Agence suédoise pour les contingences civiles, qui est également responsable de la sécurité publique, la gestion des urgences et la défense civile si aucune autre autorité n'en a la charge, a facilité la collaboration étroite entre les organismes chargés des élections afin de sécuriser les processus électoraux. À cet égard, la responsabilité consiste à prendre les mesures nécessaires avant, pendant et après une situation d'urgence ou une crise.

La coopération entre organismes joue un rôle déterminant dans la protection du processus électoral contre les risques de sécurité informatique. Si la coopération entre les 312 autorités électorales locales est une pratique établie de longue date, la coordination avec les organismes de sécurité et d'autres acteurs apparaît de plus en plus nécessaire.

L'Agence suédoise pour les contingences civiles a pour mission de contrecarrer toute activité d'influence visant à perturber, entraver ou manipuler les élections. Pour ce faire, elle collabore avec de multiples acteurs, dont l'Autorité électorale, les services de renseignement, la police de sécurité, les forces de l'ordre public, la police locale, l'ensemble des administrations électorales au niveau local et des comtés, l'administration fiscale, l'organisme de transport et les médias.

Sa stratégie comprend différentes étapes :

- évaluation de la menace (identification des éventuelles activités d'influence, évaluation des vulnérabilités et des risques, et identification des acteurs clés) ;

- mise au point de méthodes et de recommandations visant à contrer les influences, à accroître la sensibilisation des autorités (via la diffusion d'informations et la formation des autorités concernées et la diffusion d'informations auprès du public) ;
- appui à la coopération entre les autorités (en vue d'atténuer les vulnérabilités) ;
- renforcement de la sensibilisation du public (afin de réduire les effets des activités d'influence) ;
- création d'une organisation chargée de surveiller, d'identifier et de contrer toute activité d'influence pendant les élections ;
- élaboration de stratégies de communication et d'exposés descriptifs.

La gestion des crises s'appuie sur le principe de la responsabilité des autorités autonomes souveraines : « Quiconque est responsable d'une activité particulière dans des circonstances normales est également responsable de cette activité en situation de crise. » L'Agence suédoise pour les contingences civiles apporte son soutien à ces autorités en fournissant un état des lieux, en partageant les informations et en coordonnant le processus décisionnel. Elle surveille la situation et publie les informations avérées émanant de multiples organismes sur de nombreux supports, dont un site Internet et plusieurs médias sociaux, qui sont les principaux vecteurs d'informations importantes pour les citoyens.

La coordination du partage des informations permet d'éviter de diffuser des messages contradictoires et des informations lacunaires et d'éroder la confiance. La coopération entre organismes garantit donc que l'ensemble des organismes sont pleinement informés sur la situation actuelle et transmettent le même message sur les menaces informatiques.

La collaboration entre organismes repose sur la tenue régulière de réunions de haut niveau. Si par le passé, certains organismes rechignaient à coopérer ou à partager les informations, ils comprennent désormais l'importance d'une telle coopération, adhèrent pleinement au concept et le soutiennent. La coopération nouée autour de questions liées aux élections a également fait ses preuves dans d'autres domaines de gouvernance.

Une attention particulière est accordée à la transparence, à l'information des électeurs et à la préparation des médias. Tous les organismes transmettent le même message : le système suédois est décentralisé, largement manuel et, par conséquent, très solide et efficacement protégé contre les attaques informatiques. Si le processus manuel contribue à tempérer les préoccupations concernant les attaques informatiques, il a cependant fallu expliquer pourquoi les technologies électorales sont si peu présentes dans un pays où pratiquement tout est numérique.

L'objectif global est d'éviter que tout incident de piratage, présumé ou réel, ne surprenne le public et de convaincre, en amont, de la solidité des systèmes.

Ukraine

Structure de l'OGE

La Commission électorale centrale (CEC) de l'Ukraine est un organisme public permanent et indépendant qui organise les élections présidentielles et législatives et qui supervise des organismes autonomes locaux, ainsi que les référendums. Les autorités publiques locales chargées des registres, indépendantes de la CEC, tiennent à jour le registre électoral.

Usage des TIC

Les technologies suivantes sont utilisées dans les processus électoraux en Ukraine :

- le registre électoral électronique de l'État ;
- le Système unifié d'information et d'analyse « Élections », un système de gestion électorale couvrant plusieurs étapes du cycle électoral, dont les systèmes de tabulation et de transmission des résultats, l'enregistrement des candidats, l'établissement de rapports sur le financement des campagnes, l'enregistrement des observateurs, le système de collecte de signatures pour les initiatives citoyennes et les flux documentaires connexes ;
- le site Internet de la CEC.

Risques

En 2014, les élections présidentielles et législatives ont été la cible d'une série d'attaques informatiques simultanées. Outre l'envoi de logiciels malveillants et des attaques par hameçonnage, des attaques DDoS et l'altération du site publiant les résultats électoraux ont perturbé la transmission des résultats par les commissions électorales de districts. De même, des attaques DDoS ont été lancées contre la CEC en amont des élections présidentielles de 2019.

Ces événements mettent en lumière les menaces informatiques majeures suivantes :

- les attaques généralisées visant à pénétrer les ressources des réseaux internes et publics ;
- les logiciels malveillants avec une aide à l'interne et les attaques par hameçonnage ;

- les attaques DDoS ciblant les principales infrastructures électorales et les sites Internet publics.

S'il existe de fortes présomptions sur l'origine des attaques, il est difficile de trouver des preuves tangibles et les pirates n'ont toujours pas été identifiés.

Les principaux risques de sécurité informatique concernent les listes électorales, la publication des résultats des scrutins, les activités de désinformation visant à saper la confiance dans les processus électoraux, la suppression d'électeurs et la diminution de la participation électorale. Citons, entre autres :

- Compromettre les données et les systèmes afin d'entraver ou d'empêcher la mise en place des procédures électorales, par exemple en forçant les retards pendant les élections dans les régions.
- Modifier sans autorisation les données d'inscription des électeurs afin de fausser les listes électorales et de forcer la contestation des résultats des élections.
- Fausser les informations ou bloquer l'accès aux ressources, dont le traitement des résultats, en vue de discréditer les organes électoraux et leur capacité à sécuriser les processus électoraux, et créer des occasions de diffuser de faux messages sur les résultats des scrutins pour saper la confiance des électeurs et réduire la participation électorale.

Collaboration entre organismes

L'accent est mis sur le renforcement des capacités techniques de la CEC à protéger les bases de données et les registres électroniques, ainsi que les systèmes de télécommunication et d'information dont ils dépendent, contre les menaces et les problèmes informatiques. La collaboration entre organismes en matière de sécurité informatique des élections repose principalement sur la coopération entre la CEC et le Service de sécurité (le principal organisme ukrainien responsable de la sécurité informatique), qui remonte à 2010 et s'est intensifiée après les attaques de 2014. Pour les élections de 2019, le Service de sécurité a bénéficié de l'appui du Fonds d'affectation spéciale OTAN-Ukraine consacré à la cyberdéfense pour renforcer les capacités techniques de la CEC à se protéger contre les attaques informatiques.

Née de la collaboration quotidienne entre la CEC et le Service de sécurité, une commission conjointe structure leur projet et leur travail commun au niveau technique et de l'encadrement. Le Service de sécurité fournit du matériel et son expertise technique à la CEC.

En outre, le Département des services informatiques de la Police nationale ukrainienne, le Service d'État chargé des communications spéciales et de la

protection de l'information de l'Ukraine (SSSCIP) et le Service de sécurité, ainsi que des entreprises publiques et des prestataires privés, participent au développement, à la certification et à la protection des TIC dans le domaine des élections. Avant d'être utilisés par la CEC, les systèmes d'information électoraux font l'objet d'une évaluation et reçoivent un certificat de conformité. Cela couvre l'approbation du cahier des charges et de la documentation par le SSSCIP, les tests préliminaires, et l'évaluation de la conformité des systèmes avec les cahiers des charges et les exigences en matière de protection de l'information. Les experts du SSSCIP surveillent le fonctionnement des systèmes et les protègent contre les attaques.

En 2018, l'Ukraine a mis à jour la liste de ses infrastructures essentielles afin d'identifier clairement les ressources dont l'État doit assurer la protection. La CEC est chargée de toutes les communications publiques sur la protection informatique.

Union européenne

Mandat de l'organisme de gestion des élections

L'organisation d'élections dans les États membres de l'Union européenne relève strictement de leur souveraineté. Les compétences électorales de l'Union européenne ne sont que limitées. Cependant, dans un contexte de menaces grandissantes, la peur de voir l'Union européenne outrepasser les limites de son mandat a peu à peu cédé la place à une reconnaissance de la nécessité de renforcer les activités de collaboration.

Risques

Les attaques informatiques survenues par le passé n'ont que peu attiré l'attention du grand public. C'est lorsqu'elles ont commencé à devenir un sujet de débat commun qu'il a clairement fallu définir des normes, améliorer la coopération et gérer un plus grand panel de menaces informatiques que celles pesant sur les processus électoraux. Il a également été reconnu qu'une attaque subie par l'un des 27 États membres de l'Union européenne au cours des élections parlementaires européennes pourrait nuire à la capacité de constitution du Parlement.

En septembre 2018, la Commission européenne a présenté une série de mesures visant à garantir des élections européennes libres et équitables. Celles-ci comprennent différents éléments, y compris une communication, une recommandation et des orientations de la Commission ainsi qu'un projet de règlement. L'objectif est de renforcer la sécurité informatique, de réglementer les campagnes électorales en ligne, d'améliorer la transparence des activités en ligne, de lutter contre la désinformation et de garantir la protection les données.

Cette série de mesures s'appuie sur différents documents :

- le recueil de l'Union européenne sur la cybersécurité des technologies électorales (groupe de coopération en matière de SRI, 2018) ;
- son code de bonnes pratiques contre la désinformation (Commission européenne, 2018d), qui définit des pratiques d'autorégulation pour le secteur numérique ;
- son plan d'action contre la désinformation (Union européenne, 2018c) ;
- la recommandation relative aux réseaux de coopération électorale, à la transparence en ligne, à la protection contre les incidents de cybersécurité et à la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen (Commission européenne, 2018b).

La directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (2016) a mené à la création d'un groupe de coordination entre tous les États membres. Ce groupe distingue les menaces informatiques *techniques* des *activités relatives à l'information*, qui sont souvent plus visibles. Il a servi de plate-forme pour les débuts de la collaboration en matière de sécurité informatique et d'élections ainsi que pour l'élaboration du recueil de l'Union européenne.

Collaboration entre organismes

La recommandation relative aux réseaux de coopération en matière d'élections de la Commission européenne (2018) déclare que « chaque État membre devrait mettre en place un réseau électoral national, associant les autorités nationales compétentes pour les questions électorales et les autorités chargées de la surveillance et de l'application des règles relatives aux activités en ligne pertinentes dans un contexte électoral », en plus de contenir les recommandations suivantes :

- « Faciliter l'échange rapide et sécurisé d'informations sur les questions susceptibles de perturber les élections au Parlement européen, notamment en identifiant conjointement les menaces et les failles, en partageant les constatations et l'expertise et en se concertant sur l'application et le respect des règles applicables dans l'environnement en ligne. »
- « En fonction des besoins et conformément au droit national, consulter les services répressifs nationaux compétents et coopérer avec eux. » Lorsqu'il y a lieu, Europol peut faciliter la coopération entre les services répressifs nationaux au niveau européen.

- « Les États membres devraient apporter le soutien nécessaire aux réseaux visés au point (1) et veiller à ce qu'ils soient dotés des moyens nécessaires pour permettre un partage d'informations rapide et sécurisé. »
- « Afin de faciliter l'échange d'expertise et de bonnes pratiques entre les États membres, notamment sur les menaces, les failles et le respect des règles, chaque État membre devrait désigner un point de contact unique […] »
- « Les États membres devraient prendre des mesures techniques particulières pour assurer la disponibilité, l'authenticité, la confidentialité et l'intégrité des services électoraux qui dépendent de réseaux et de systèmes d'information. » « Pour garantir le bon déroulement de chaque phase de l'élection, les États membres devraient protéger de manière adéquate les réseaux et les systèmes d'information utilisés pour tenir les listes électorales et enregistrer les candidats ; recueillir, traiter et compter les voix ; publier les résultats électoraux et les communiquer au grand public. »
- « Les partis politiques, fondations politiques et organisations de campagne opérant au niveau tant européen que national devraient mettre en œuvre des mesures spécifiques et appropriées pour prévenir les incidents de cybersécurité et se protéger des cyberattaques. »
- « Les États membres devraient effectuer une analyse approfondie des risques associés aux élections au Parlement européen en vue d'identifier les incidents de cybersécurité potentiels qui pourraient porter atteinte à l'intégrité du processus électoral. » « Les États membres devraient mettre en place les procédures nécessaires pour prévenir, détecter, gérer et contrer les cyberattaques, dans le but de minimiser leurs effets, et garantir un échange d'informations rapide à tous les niveaux pertinents, qu'ils soient techniques, opérationnels ou politiques. » « Pour ce faire, ils devraient veiller à ce que les autorités nationales chargées des questions électorales soient dotées de ressources adéquates, notamment d'équipements techniques et de personnel compétent, pour traiter ce type d'incidents […] »
- « Les États membres devraient collaborer avec des tiers, notamment les médias, les plates-formes en ligne et les fournisseurs de technologies de l'information, pour mener des activités de sensibilisation visant à renforcer la transparence des élections et à instaurer un climat de confiance dans les processus électoraux. »
- « En cas d'incident de cybersécurité comportant des attaques contre des systèmes d'information visant le processus électoral, les États membres devraient prévoir une réaction pénale appropriée, sur la base de la

directive 2013/40/UE relative aux attaques contre les systèmes d'information. » « Les États membres devraient permettre une coopération étroite entre les autorités nationales compétentes, les autorités chargées de la cybersécurité et les services répressifs […] »

En mars 2019, le réseau européen de coopération électorale a organisé un exercice de simulation en salle inédit pour tester la préparation de l'Union européenne en matière de sécurité informatique en amont des élections parlementaires de 2019, cet exercice a permis aux participants (Commission européenne, 2019) de :

- « Obtenir une vue d'ensemble du niveau de résilience (en matière de politiques adoptées, de capacités et de compétences disponibles) des systèmes électoraux dans l'UE, y compris une évaluation du degré de sensibilisation des autres parties prenantes (par exemple, les partis politiques, les organisateurs de campagnes électorales et les fournisseurs d'équipements informatiques pertinents).
- Renforcer la coopération entre les autorités compétentes au niveau national, notamment les autorités électorales et d'autres organes et agences compétents, tels que les autorités chargées de la cybersécurité, les centres de réponse aux incidents de sécurité informatique (CSIRT), l'autorité chargée de la protection des données (DPA), les autorités chargées des questions de désinformation, les unités spécialisées en cybercriminalité, etc.
- Vérifier la capacité des États membres de l'UE à évaluer correctement les risques liés à la sécurité informatique dans le cadre des élections européennes, à prendre rapidement conscience de la situation et à coordonner la communication publique.
- Tester les plans de gestion de crise existants et les procédures pertinentes pour prévenir, détecter et gérer les cyberattaques et les menaces hybrides, y compris les campagnes de désinformation, et pour y réagir.
- Améliorer la coopération transfrontalière et renforcer le lien avec les groupes de coopération concernés au niveau de l'UE (par exemple, le réseau de coopération électorale, le groupe de coopération en matière de SRI et le réseau des CSIRT) afin de consolider la capacité de réaction coordonnée en cas d'incidents de cybersécurité transfrontaliers.
- Recenser toutes les autres lacunes potentielles ainsi que les mesures adéquates d'atténuation des risques qui devraient être mises en œuvre avant les élections du Parlement européen. »

Références et ressources supplémentaires

Bay, S. et Šnore, G., *Protecting Elections: A Strategic Communications Approach*, [Protection des élections : approche stratégique de la communication], Riga, Centre d'excellence pour la communication stratégique de l'OTAN, 2019, <https://www.stratcomcoe.org/protecting-elections-strategic-communications-approach>, consulté le 23 mai 2019

Cabinet du Premier ministre finlandais, *Central Government Communications Guidelines*, [Directives en matière de communication du gouvernement central], Helsinki, Cabinet du Premier ministre finlandais, 2016, <https://vnk.fi/en/central-government-communications-guidelines>, consulté le 10 octobre 2018

Centre Belfer pour la science et les affaires internationales, Harvard Kennedy School, *The Cybersecurity Campaign Playbook*, [Stratégie des campagnes de sécurité informatique], Defending Digital Democracy, 20 novembre 2018a, <https://www.hks.harvard.edu/publications/cybersecurity-campaign-playbook>, consulté le 21 août 2017

Centre Belfer pour la science et les affaires internationales, Harvard Kennedy School, NDI et IRI, *The Cybersecurity Campaign Playbook, European Edition*, [Stratégie des campagnes de sécurité informatique, édition européenne], novembre 2018b, <https://www.ndi.org/sites/default/files/european_campaign_playbook_-_web.pdf>, consulté le 21 août 2017

Centre de la sécurité des télécommunications (CST) du Canada, *Cybermenaces contre le processus démocratique du Canada*, 2017, <https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-f.pdf>, consulté le 8 mai 2018

—, *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019*, 2019, <https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report-f_0.pdf>, consulté le 16 avril 2019

Commission d'assistance électorale des États-Unis (CAE), *Election Security Preparedness*, [Préparation en matière de sécurité des élections], n.d., <https://www.eac.gov/election-officials/election-security-preparedness/>, consulté le 11 novembre 2018

—, « Election Security Video », [Vidéo sur la sécurité des élections], <https://www.eac.gov/electionsecurity/>, consulté le 11 novembre 2018

—, *Starting Point: U.S. Election Systems as Critical Infrastructure,* [Point de départ : Le système électoral des États-Unis en tant qu'infrastructure essentielle], Silver Spring, MD, USEAC, 2017, <https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf>, consulté le 8 mai 2018

Commission électorale australienne, *Electoral Backgrounder: Electoral Communications and Authorization Requirements*, [Fiche d'information électorale : communications sur les élections et exigences en matière d'autorisation], 23 avril 2019, <https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm>, consulté le 10 octobre 2018

—, How the Senate result is determined, [Comment les résultats du Sénat sont établis] <https://www.aec.gov.au/Voting/counting/senate_count.htm>, consulté le 11 octobre 2018

Commission européenne (CE), *Election Interference in the Digital Age, Building Resilience to Cyber-enabled Threats*, [Interférence dans les élections à l'ère numérique, Renforcer la résilience aux menaces informatiques], Bruxelles, CE, 2018a, <https://ec.europa.eu/epsc/publications/other-publications/election-interference-digital-age_en>, consulté le 9 novembre 2018

—, *Recommandation de la Commission sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement*

européen, Bruxelles, CE, 2018b, <https://ec.europa.eu/transparency/regdoc/rep/3/2018/FR/C-2018-5949-F1-FR-MAIN-PART-1.PDF>, consulté le 6 novembre 2018

—, *Action Plan on disinformation: Commission contribution to the European Council*, [Plan d'action contre la désinformation : contribution de la Commission au Conseil européen], Bruxelles, CE, 2018c, <https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en>, consulté le 17 juin 2019

—, *Code of Practice on Disinformation*, [Code européen de bonnes pratiques contre la désinformation], Bruxelles, CE, 2018d, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>, consulté le 17 juin 2019

—, *Les États membres de l'UE testent leur préparation en matière de cybersécurité pour que les élections européennes de 2019 soient libres et équitables,* Bruxelles, CE, 2019, Communiqué de presse, <https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_2011>, consulté le 5 avril 2019

DefCon, *DEFCON 25 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, [DEFCON 25, Attaques contre les machines à voter, Atelier de piratage des machines à voter, Rapport sur les vulnérabilités informatiques des bases de données, des infrastructures et des équipements électoraux aux États-Unis], septembre 2017, <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf>, consulté le 16 octobre 2018

—, *DEFCON 26 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, [DEFCON 25, Atelier « Voting Village », Rapport sur les vulnérabilités informatiques des bases de données, des infrastructures et des équipements électoraux aux États-Unis], septembre 2018, <https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf>, consulté le 16 octobre 2018

Département de la Sécurité intérieure des États-Unis, *National Cyber Incident Response Plan*, [Plan national d'intervention contre les incidents informatiques], Washington, DC, DHS, 2016, <https://www.us-cert.gov/

sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf>, consulté le 11 novembre 2018

El Universal, Facebook – Instituto Nacional Electoral, *Memorandum of Cooperation*, [Mémorandum de coopération], 2018, <http://interactivo.eluniversal.com.mx/graficos/online/pdf-18/convenio-facebook.pdf>, consulté le 6 novembre 2018

Élections Canada, « Comment Élections Canada contribue-t-il à la sécurité des élections ? », s.d., <https://www.elections.ca/content.aspx?section=vot&dir=bkg/sec&document=legal&lang=f>, consulté le 6 février 2019

Financial Review, « Australian Electoral Commission strengthens defenses against foreign hacking », [La Commission électorale australienne renforce ses moyens de défense contre les pirates informatiques étrangers], 30 avril 2018, <https://www.afr.com/news/australian-electoral-commission-strengthens-defences-against-foreign-hacking-20180430-h0zfzz>, consulté le 10 octobre 2018

Fondation internationale pour les systèmes électoraux (IFES), *Social Media, Disinformation and Electoral Integrity*, [Réseaux sociaux, désinformation et intégrité électorale], IFES, 2019, livre blanc, 2019, <https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf>, consulté le 20 juin 2018

G7, *Commitment on Defending Democracy from Foreign Threats*, [Engagement à défendre la démocratie contre les menaces étrangères], Charlevoix, G7, 2018, <https://www.mofa.go.jp/files/000373846.pdf>, consulté le 20 juin 2018

Gouvernement australien, Attorney-General's Department, « The Protective Security Policy Framework », [Cadre politique relatif à la protection de la sécurité], s.d., <https://www.protectivesecurity.gov.au/Pages/default.aspx>, consulté le 10 octobre 2018

Gouvernement australien, Cyber Security Centre, *Information Security Manual*, [Manuel sur la sécurité de l'information], s.d., <https://acsc.gov.au/infosec/ism/>, consulté le 10 octobre 2018

Gouvernement australien, Department of Home Affairs, *Cyber Security Strategy*, [Stratégie de sécurité informatique], Commonwealth of Australia, 2016, <https://cybersecuritystrategy.homeaffairs.gov.au/>, consulté le 10 octobre 2018

Gouvernement australien, *International Cyber Engagement Strategy*, [Stratégie internationale d'engagement informatique], 2017, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, consulté le 10 octobre 2018

Groupe de coopération NIS, *Compendium on Cyber Security of Election Technology*, [Recueil sur la sécurité informatique des technologies électorales], Publication du GC, 2018, <http://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf>, consulté le 11 octobre 2018

Institut Poynter, *A Guide to Anti-misinformation Actions around the World*, [Guide mondial des actions de lutte contre la désinformation], 2018, <https://www.poynter.org/news/guide-anti-misinformation-actions-around-world>, consulté le 8 mai 2018

« Electoral watchdog powerless to crack down on offshore political ads targeting Australians », [Le gendarme électoral incapable de réprimer les annonces politiques étrangères ciblant la population australienne], in *The Guardian*, 24 juillet 2018, <https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>, consulté le 11 octobre 2018

Hicks, T., « Defending and recovering American election systems » [Défendre et réhabiliter les systèmes électoraux américains], *Brown Journal of World Affairs*, 24/2 (2018), <http://bjwa.brown.edu/24-2/defending-and-recovering-american-election-systems/>, consulté le 20 juin 2018

INE, Twitter-Instituto Nacional Electoral, *Memorandum of Cooperation*, [Mémorandum de coopération], 11 juin 2018, <http://centralelectoral.ine.mx/wp-content/uploads/2018/03/Memorandum-de-Entendimiento-con-Twitter.pdf>, consulté le 6 novembre 2018

IP-Watch, « A Digital Geneva Convention: Nobel Prize-Worthy or Dangerous? », [Convention de Genève numérique : prix Nobel, une récompense ou un danger ?], 19 décembre 2017, <http://www.ip-watch.org/2017/12/19/

digital-geneva-convention-nobel-prize-worthy-dangerous/>, consulté le 10 octobre 2018

Documents d'orientation de Microsoft, *A Digital Geneva Convention to Protect Cyberspace*, [Convention de Genève numérique : Protéger l'espace informatique], Redmond, WA, Microsoft, 2017, <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>, consulté le 8 mai 2018

Organisation pour la sécurité et la coopération en Europe, Bureau des institutions démocratiques et des droits de l'homme (OSCE/BIDDH), *International Election Observation Mission North Macedonia, Presidential Election*, [Mission d'observation électorale internationale en République de Macédoine du Nord, élections présidentielles], avril 2019, <https://www.osce.org/odihr/elections/north-macedonia/417818?download=true>, consulté le 23 mai 2019

Parlement du Commonwealth d'Australie, *Status Report of the Joint Standing Committee on Electoral Matters*, [Rapport de situation du Comité permanent mixte sur les questions électorales], mars 2019, <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024259/toc_pdf/Statusreport.pdf>, consulté le 14 avril 2019

Past, L., « All elections are hackable: scalable lessons from secure i-voting and global election hacks », [Toutes les élections peuvent être piratées : leçons progressives sur le vote électronique sécurisé et le piratage des élections au niveau mondial], in *European Cyber Security Journal*, 3/3, 2017, p. 34-47, <https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF>, consulté le 8 mai 2018

République d'Estonie, *Information System Authority*, [Agence nationale des systèmes informatiques], n.d., <https://www.ria.ee/en.html>, consulté le 11 octobre 2018

Union européenne, Directive on Critical Information Systems, [Directive sur les systèmes d'information essentiels], Bruxelles, UE, 2016, <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, consulté le 6 novembre 2018

—, *Code of Practice on Disinformation*, [Code européen de bonnes pratiques contre la désinformation], Bruxelles, EU, 2018, <https://ec.europa.eu/

newsroom/dae/document.cfm?doc_id=54454>, consulté le 9 novembre 2018

Verificado, *Noticias Falsas,* [Les fausses informations], 2018, <https://verificado.mx/categoria/noticias-falsas>, consulté le 15 avril 2019

Wolf, P., « Cybersecurity and Elections: An International IDEA Round-table Summary », [La sécurité informatique et les élections : Résumé de la table ronde d'International IDEA], La Haye, International IDEA, 2017, <https://www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary>, consulté le 8 mai 2018

À propos des auteurs

Sam van der Staak est le chef du Programme régional Europe d'International IDEA et à ce titre, il fournit des conseils sur un large éventail de réformes démocratiques aux partis politiques, aux commissions électorales et à d'autres institutions étatiques. Il est l'auteur de plusieurs publications portant sur des sujets tels que le développement des partis politiques, les mouvements citoyens et les financements politiques, et intervient régulièrement dans plusieurs médias européens. Avant de s'engager dans l'assistance à la démocratie, il a travaillé pour la Chambre des Représentants des Pays-Bas.

Peter Wolf est directeur technique pour les processus électoraux à International IDEA. Ses recherches et son travail sont centrés sur le rôle des TIC dans les élections et la démocratie, et tout particulièrement sur les applications de la technologie fiables et durables dans les processus électoraux. Il détient une expérience avérée de l'assistance internationale et est l'auteur de nombreuses publications dans ce domaine.

À propos d'IDEA International

L'Institut international pour la démocratie et l'assistance électorale (IDEA International) est une organisation intergouvernementale dont la mission est de promouvoir la démocratie dans le monde, laquelle est à la fois une aspiration humaine universelle et un moteur du développement durable. Pour ce faire, nous contribuons à la mise en place, au renforcement et à la protection d'institutions et processus politiques démocratiques à tous les niveaux. Notre vision est celle d'un monde dans lequel les processus, acteurs et institutions démocratiques sont non seulement inclusifs et responsables, mais suscitent également un développement durable qui bénéficie à tous.

En quoi consiste notre mission ?

Nos activités se concentrent sur trois grands domaines d'influence : les processus électoraux, les processus d'élaboration de la constitution, ainsi que la participation et la représentation politiques. L'égalité des genres et l'inclusion, la sensibilisation au conflit et le développement durable sont autant de questions qui sont intégrées à l'ensemble de nos domaines d'intervention.

IDEA International œuvre sur plusieurs fronts : nous fournissons une analyse sur les tendances démocratiques mondiales et régionales ; produisons des données comparatives relatives aux bonnes pratiques démocratiques internationales ; offrons une assistance technique aux acteurs engagés dans les processus démocratiques, contribuons au renforcement des capacités en matière de réforme démocratique ; et nous engageons un dialogue sur les questions qui relèvent du débat public sur la démocratie et sa mise en place.

Où sommes-nous basés ?

Notre siège se trouve à Stockholm et nous avons des bureaux régionaux en Afrique, en Asie et dans le Pacifique, en Europe, en Amérique latine et dans les

Caraïbes. Observateur permanent auprès des Nations Unies, IDEA International est également accrédité auprès des institutions de l'Union européenne.

<https://www.idea.int>

Les technologies de l'information et de la communication ont un poids grandissant dans les procédures de gestion électorale et les processus démocratiques, y compris dans les pays où le vote électronique n'est présent sous aucune forme. Si ces technologies offrent de nouvelles possibilités, elles entraînent également de nouvelles menaces dans leur sillage. À l'heure actuelle, la sécurité informatique représente un enjeu électoral majeur. La sécurité informatique implique un grand nombre d'intervenants, à commencer par les organismes de gestion des élections, les entités spécialisées en cybersécurité et les agences de sécurité.

Dans de nombreux pays, il s'est dégagé un consensus autour du caractère essentiel de la collaboration entre organismes afin de préserver les processus électoraux des menaces numériques. Ces dernières années, cette coopération s'est structurée et intensifiée, tant au niveau national qu'international.

Ce document se propose de dresser un état des lieux sur les progrès enregistrés en matière de sécurité informatique en contexte électoral dans différents pays. Regroupant une vingtaine d'études de cas menées dans le monde entier, il constitue une mine d'informations pour quiconque souhaite se prémunir contre les attaques informatiques.

International IDEA
Strömsborg
SE–103 34 Stockholm
Suède
Téléphone : +46 8 698 37 00
Courriel : info@idea.int
Site Internet : ‹https://www.idea.int›

ISBN: 978-91-7671-329-7 (PDF)