Présidentielle 2022 et cybersécurité

Agir, maintenant.

FRANCE DIGITALE

The Positive Way
WAVESTONE

Sommaire

01

CHAPITRE 1

Les élections à l'heure de l'avènement du numérique.

Opportunités démocratiques & enjeux cyber.

02

CHAPITRE 2

Les multiples facettes du risque cyber sur la présidentielle 2022.

Le risque majeur n'est pas là où on le croit.

03

CHAPITRE 3

Quelles solutions concrètes pour faire face au risque cyber ?

Les élections présidentielles ont toujours été la cible d'opérations de déstabilisation et ce bien avant l'arrivée d'Internet et des réseaux sociaux. Mais l'avènement du numérique simplifie et amplifie grandement ce phénomène. Les campagnes électorales sont devenues de plus en plus numériques : la mobilisation, les débats se tiennent majoritairement sur des plateformes numériques, les programmes se construisent de manière collaborative en ligne, les meetings sont retransmis sur Internet, les sondeurs interrogent les internautes, les résultats sont consolidés via Internet... L'ensemble de l'écosystème électoral est numérique.

Ces espaces numériques sont fréquemment la cible d'attaques, de plus en plus pernicieuses et puissantes. Les précédents observés lors de nombreuses élections, et nous nous souvenons en particulier de la présidentielle américaine de 2016, montrent clairement que l'élection présidentielle de 2022 n'a aucune raison d'être épargnée par ces menaces. Des acteurs français de l'écosystème électoral ont déjà fait face à des attaques cyber par le passé : la République en Marche a fait face à des fuites massives de ses données en 2017 en amont du second tour des présidentielles, TV5 Monde, M6 ou encore Adrexo ont également fait l'objet d'attaques. Alors que les menaces cyber mutent rapidement, de nouveaux scénarios d'attaques apparaissent plus ou moins sophistiqués : utilisation de réseaux d'ordinateurs zombies, recours aux deepfakes, arrosage d'emails frauduleux, exfiltration de données, etc.

Quels sont alors les risques cyber qu'encourt la vie démocratique française ? Quelles sont les données et les systèmes à protéger ? Comment le faire dans un environnement extrêmement dynamique comme celui d'une élection d'ampleur avec la mobilisation nécessairement rapide de millions de personnes ? Quelles solutions utilisées et comment garantir une forme de souveraineté dans la protection de nos élections ? Autant de questions auxquelles il faut répondre dès aujourd'hui, et ce pour l'ensemble des acteurs de l'écosystème. Car, face à un évènement de cette ampleur, les attaquants vont rapidement se pré-positionner et commencer leurs actions de reconnaissance pour être prêts à frapper quand le moment opportun sera venu !

Marianne Tordeux Bitker
Directrice des Affaires publiques,
France Digitale

Gérôme Billois
Associé Cybersécurité,
Wavestone

01

Les élections à l'heure de l'avènement du numérique

Opportunité démocratique & enjeux cyber

La longue histoire des attaques électorales

IL ÉTAIT UNE FOIS LA FRAUDE ÉLECTORALE

Les menaces sur le système électoral ne sont pas nées avec le numérique.

À l'ère pré-numérique, les menaces concernant le système électoral étaient de différents ordres.

La fraude électorale pouvait consister à une modification des listes électorales, un bourrage d'urnes, un vol de votes, une destruction de bulletins de vote, une proclamation de résultats erronés.

Les exemples ne manquent pas.

- Le candidat républicain Rutherford B. Hayes est élu lors de l'élection présidentielle américaine de 1876 après des vols d'urnes, des menaces physiques à l'encontre d'électeurs démocrates et des trucages massifs de bulletins de vote.

- Plus récemment, en 1989, en Guinée équatoriale, Teodoro Obiang Nguema Mbasogo obtient un score électoral de 99% à l'élection présidentielle. Les bulletins de vote ne sont même pas comptabilisés. Le pouvoir en place décide arbitrairement des résultats.

La déstabilisation des opinions se déroulait au travers d'intenses débats de presse, les médias devenant l'intermédiaire et le canal des expressions collectives. La création d'instituts de sondage « orientés » a également été observée, ce qui a poussé les États à légiférer.

Depuis l'élection du président de la République au suffrage universel direct en 1962, les élections présidentielles sont devenues un moment charnière de la vie démocratique française. Les menaces sur le processus électoral sont d'autant plus fortes.

Numérique et élections : de l'opportunité à la menace

L'IRRUPTION DU NUMÉRIQUE DANS LE PROCESSUS ÉLECTORAL, UNE LÉGENDE ROSE QUI VIRE AU NOIRE

Le numérique fait sa première apparition dans les campagnes électorales en 1996, dans le cadre de l'élection présidentielle américaine (Bill Clinton vs. Bob Dole). À la fin du premier débat télévisé entre les candidats, le Républicain annonce publiquement l'adresse de son site web. En France, il faut attendre la présidentielle de 2002 pour qu'Internet apparaisse comme l'une des parties prenantes de l'élection : "Cette présidentielle sera la première élection où Internet va être utilisé de façon significative en France", pronostique Thierry Vedel en 2002, chercheur au Cevipof. La mobilisation contre Jean-Marie Le Pen dans l'entre-deux-tours se joue en effet aussi sur Internet. Des sites plaidant pour le front républicain ont enregistré, chaque jour, entre 700 et 2 000 connexions. Cependant, la presse écrite a gardé un rôle essentiel, celui de relais catalyseur, en citant dans de nombreux articles cette nouvelle forme de mobilisation.

Utilisé pour gérer de gigantesques bases de données électorales, faciliter les communications entre militants et équipes de campagne, informer les militants et électeurs, voire lever des fonds, le numérique et ses usages se diversifient à partir des années 2000.

Avec l'avènement de l'usage de technologies dans le processus électoral naissent de nouvelles menaces cyber. Ces dernières tendent, soit à modifier purement et simplement le résultat des votes, soit à affecter la confiance des électeurs dans l'élection, et donc dans le processus démocratique de façon plus globale.

MacronLeaks, première manœuvre cyber étrangère d'importance significative lors d'une élection française

Deux jours avant le second tour de la présidentielle de 2017, plus de 20 000 échanges privés du parti En Marche ! sont diffusés publiquement. Parmi ces données, un nombre significatif de correspondances sont fausses. L'impact est négligeable sur les résultats du scrutin. En effet, le Code électoral précise qu'à partir de la veille du scrutin, les médias traditionnels ainsi que les candidats sont limités dans la propagande et la polémique électorale. Il n'y pas eu d'effet médiatique d'amplification.

La campagne d'Obama en 2008 : premier exemple de l'utilisation des technologies au service de l'influence démocratique

La première campagne électorale de Barack Obama en 2008 est la première "utilisation intelligente et très efficace de technologies modernes au service de modalités très traditionnelles de campagne. Le Web, les réseaux sociaux et les téléphones portables se sont révélés d'une efficacité inédite dans un champ d'actions stratégiques que nous pouvons réunir en cinq axes : recruter des militants, les motiver, les informer, les organiser et récolter des fonds", d'après François Heinderyckx, professeur de sociologie des médias.
Il faut cependant nuancer l'impact du numérique sur cette élection. A ce propos, le sociologue relève que cette élection "marque indiscutablement un tournant, non pas vers une quelconque virtualisation ou numérisation de la campagne électorale, mais bien vers un retour à des modes de mobilisation, d'action et de persuasion politiques très classiques, rajeunis et catalysés par ce que nous proposons de qualifier d'inflexion numérique".

Déstabilisation du processus électoral

LES EXEMPLES LIÉS AU NUMÉRIQUE SE MULTIPLIENT DEPUIS LES ANNÉES 2000

Etats-Unis
2000

Élection présidentielle aux États-Unis (Bush vs. Al Gore).

- Recours à un système de vote électronique et à des machines à voter. Difficultés de comptage des votes en Floride.
- Al Gore est annoncé Président élu par CNN mais Bush est vainqueur selon Fox News.
- Quelques heures plus tard, CNN s'aligne sur son concurrent.
- Des recours pour recompter les votes en Floride sont déposés mais la Cour Suprême rend un arrêt critiqué (Bush v. Gore, 531 US 98) entérinant la victoire de GW Bush. **La partialité de la décision fait débat.**

Royaume-Uni
2015

Référendum sur le retrait du Royaume-Uni de l'Union Européenne.

- Scandale Facebook-Cambridge Analytica : **Facebook admet avoir laissé l'entreprise accaparer les données personnelles de plus 87 millions d'utilisateurs**, dans le but de faire un ciblage électoral contre leur gré.
- Christopher Wylie, lanceur d'alerte, affirme que **le camp conservateur n'aurait pas gagné le référendum, qui s'est joué à moins de 2% des votes, sans ces données**

Ghana
2015

Élection présidentielle au Ghana.

- **Piratage du site Internet & des réseaux sociaux de la Commission électorale du Ghana.**
- Publication de résultats erronés depuis le compte Twitter de la Commission électorale alors que le comptage des voix était encore en cours. Effacement de ce message erroné au bout de quelques heures sans impact sur les résultats électoraux.

Etats-Unis
2016

Élection présidentielle américaine (Trump vs. Clinton).

- **Ingérence étrangère accréditée par le Sénat en 2019** : piratage informatique des systèmes de messagerie du parti démocrate et recours massif à des campagnes de désinformation

France
2017

Élection présidentielle en France.

- **Fuite de milliers de mails** du parti En Marche !, dont des fausses données, deux jours avant le second tour.

Brésil
2018

Élection présidentielle au Brésil.

- Utilisation massive de WhatsApp par les partisans de Jair Bolsonaro (élu) afin de **diffuser plusieurs centaines de millions de messages alléguant de fausses informations** comme celle du kit gay (un supposé manuel scolaire, promu par son opposant Fernando Haddad, lorsqu'il était ministre de l'Éducation, qui inciterait les enfants à changer de genre)

Inde
2019

Élections législatives en Inde.

- Usage des réseaux sociaux par **+340 millions d'Indiens.**
- **Diffusion massive de fausses informations afin de discréditer les candidats.**
- **Tensions religieuses exacerbées** par le biais des réseaux sociaux, ayant peut-être contribué à la réélection du **nationaliste hindou Narendra Modi en tant que Premier ministre.**

Etats-Unis
2020

Élections présidentielles aux États-Unis (Biden vs. Trump).

- Prise en compte en amont de la menace cyber, via une **forte mobilisation des instances fédérales.**
- **L'élection n'a pas directement été victime d'attaques cyber,** ce qui n'a pas empêché de nombreuses opérations de désinformation, en particulier sur les réseaux sociaux.

De 2016 à 2020, Élections présidentielles américaines

DEUX ÉLECTIONS, DEUX SCÉNARIOS, DEUX RÉACTIONS

2016 : la révélation des failles numériques du système électoral américain

/ **Viralité des fausses informations, plus partagées que les informations vérifiées et impréparation générale dans la lutte contre la désinformation :** les 20 fausses informations les plus partagées, provenant de plateformes spécialisées dans les canulars et de blogs partisans, ont généré sur les trois derniers mois avant le jour de scrutin, plus de 8,7 millions de partages, réactions et commentaires sur Facebook, alors que les 20 articles les mieux classés de sites d'informations comme le New York Times, le *Washington Post* ou le *Huffington Post* ont atteint seulement 7,4 millions de partages sur le même réseaux social) .

/ **Piratage de la boite mail privée du directeur de campagne d'Hillary Clinton 5 semaines avant l'élection.** Plus de 50% des électeurs de Trump (ie. environ 23% des Américains ayant voté) pensent que les mails de Clinton et son équipe de campagne, contiennent des noms de code de rites satanistes, pédophiles ou de réseaux de trafic d'êtres humains.

/ **Ingérence de puissances étrangères** concernant la mise en œuvre d'atteintes cyber, révélées par le Congrès américain en 2019. Les autorités américaines ont imputé les attaques à des Russes.

/ **Soupçons de piratage des machines à voter** (utilisées dans 18% des circonscriptions électorales) sans que ces allégations soient officiellement avérées à ce jour.

2020 : l'union du public et du privé pour contrecarrer la menace cyber

/ **Mobilisation des agences américaines de sécurité,** en particulier l'agence CISA créée en novembre 2018, dont le rôle est d'assurer la sécurité des élections au niveau fédéral. Elle a pour but d'améliorer le niveau de sécurité informatique à tous les niveaux de l'État fédéral, de coordonner les programmes de cybersécurité avec les États fédérés et d'améliorer la protection des États-Unis en général face aux menaces cyber.

/ **Programme Protect Election :** Le secteur de la cybersécurité aux États-Unis enregistre 5 milliards de dollars d'investissement en 2020 contre 2,9 milliards en 2016.

/ **Contribution d'entreprises privées** (notamment Microsoft) dans la détection d'attaques visant des individus et organismes en lien avec les élections.

/ **Nouveau rôle auto-octroyé par les réseaux sociaux en tant que remparts contre la désinformation et la haine en ligne.** Facebook crée une « cour suprême privée » 10 jours avant l'élection présidentielle, dont le rôle est d'émettre des sanctions contre des utilisateurs (jusqu'au bannissement à vie du réseau social). Le 7 janvier 2021, à la suite de l'attaque du Capitole, Facebook supprime pour deux ans le compte officiel du candidat Donald Trump sur décision interne. Twitter fait de même.

Les particularités du système électoral américain accentuant l'impact d'une attaque cyber, même minime :

/ 7 États américains utilisent des machines à voter, qui ne délivrent aucune trace sous format papier du vote enregistré.
/ Recours massif au vote par correspondance (environ 50% des électeurs), ce qui augmente la surface potentielle d'attaque.
/ Le système de vote basé sur des grands électeurs par État crée des points focaux plus nombreux pour les attaquants, qui peuvent influencer le scrutin en prenant pour cible certains "swing States" particulièrement sensibles.

02

Les multiples facettes du risque cyber sur la présidentielle 2022

Le risque majeur n’est pas là où on le croit

Les trois motivations des cyberattaquants

UNE MULTITUDE DE RISQUES CYBER DANS UN CONTEXTE ÉLECTORAL

L'avènement du numérique met au premier plan le risque cyber. On distingue trois principales motivations des cyberattaquants dans un contexte électoral :

Cybercriminalité : une nouvelle réalité pour les élections

L'écosystème cybercriminel s'est largement développé ces dernières années et pourra cibler les acteurs des élections : vol d'informations personnelles ou stratégiques en vue de la revente, blocage de systèmes contre le versement de rançon, etc.

Conséquences potentielles: interruption de la campagne pour les victimes, démobilisation des militants, interruption de réunions publiques, chantage à la révélation de secrets de campagne, etc.

Espionnage : une menace à moyen/long terme

Les attaques cyber peuvent être perpétrées à des fins d'espionnage avec à la clé de lourdes conséquences pour les intérêts nationaux. En contexte électoral, des puissances étrangères pourraient s'insérer dans les systèmes d'information, exploiter et manipuler des données volées, intercepter des communications de partis politiques et de candidats et révéler publiquement des données confidentielles. Les conséquences ne sont pas immédiatement visibles et portées à la connaissance de l'acteur concerné mais sont utilisées à long terme.

Conséquences potentielles : affaiblissement du parti espionné grâce à l'interception d'informations stratégiques divulguées ou récupérées par des acteurs concurrents, publication d'informations confidentielles discréditant un acteur...

Déstabilisation : avant tout liée à la désinformation

La déstabilisation peut prendre de nombreuses formes, allant de l'interruption des systèmes centraux de vote à la modification des listes électorales, mais celle qui est la plus probable est la déstabilisation des candidats par des campagnes de désinformation : modification des résultats lors des élections le jour J, publication d'informations confidentielles, diffusion massive de fausses informations, etc.

Conséquences potentielles : basculement des votes, élection d'un candidat non légitime, retrait d'un candidat...

x4

du nombre de ransomware en 2020 selon l'ANSSI

45%

des cyberattaques en France sont motivées par le gain financier (Benchmark CERT 2020, Wavestone)

Le risque cyber sera l'essence jetée sur le feu de la désinformation

Focus sur... la désinformation, le risque numéro 1 de l'élection

LES CYBERATTAQUES AMPLIFIENT LA DÉSINFORMATION - ET VICE VERSA

Les 2 facettes de la désinformation

L'information (erronée, incorrecte) relayée par les médias ou les réseaux sociaux.
Le support de transmission de l'information étant connu, la modération des contenus est possible. Les rédactions de médias et les plateformes ont déjà institutionnalisé la modération de contenus par la suppression des fausses informations ou le décryptage de fausses informations (decodex, factuel, etc.).

L'information disséminée de manière sporadique au travers une myriade de faits, sur différentes plateformes et/ou dans des cercles privés.
Ces informations participent à créer des biais cognitifs auprès des lecteurs. Ces derniers sont difficilement détectables par les instituts de sondage ou les pouvoirs publics.

63% des Français déclaraient en 2020 avoir rencontré des fausses informations plus d'une fois par mois. 70% pour les moins de 35 ans.
(Baromètre Kantar-La Croix sur les médias, janvier 2021)

Plus la désinformation est basée sur des éléments réels ou pouvant y être assimilés, plus celle-ci a de chances d'être considérée comme vraie.
Et c'est là où des attaques cyber peuvent fournir les éléments clés par exemple par le piratage de messagerie ou le vol de photos/vidéos.

Exemples d'attaques cyber crédibilisant une *fake news*

- **Pirater la messagerie** ou les comptes sur réseaux sociaux d'un candidat ou d'une personne influente pour relayer de fausses informations
- **Voler des vidéos/audios personnels** et les modifier pour y ajouter des éléments faux
- **Voler des données légitimes** sur les partages de fichiers et y insérer des fausses données pour les légitimer
- **Pirater le site internet d'un parti politique, d'un média ou d'un institut de sondage** pour y intégrer du faux contenu
- **Prendre le contrôle d'une chaine de télévision** pour y diffuser des informations fausses

Ou à l'inverse, la désinformation peut alimenter une attaque cyber

Utilisation des réseaux sociaux pour provoquer un mouvement massif d'internautes qui entraînera ainsi **l'arrêt du service** (attaque par déni de service)

Un écosystème électoral complexe et décentralisé

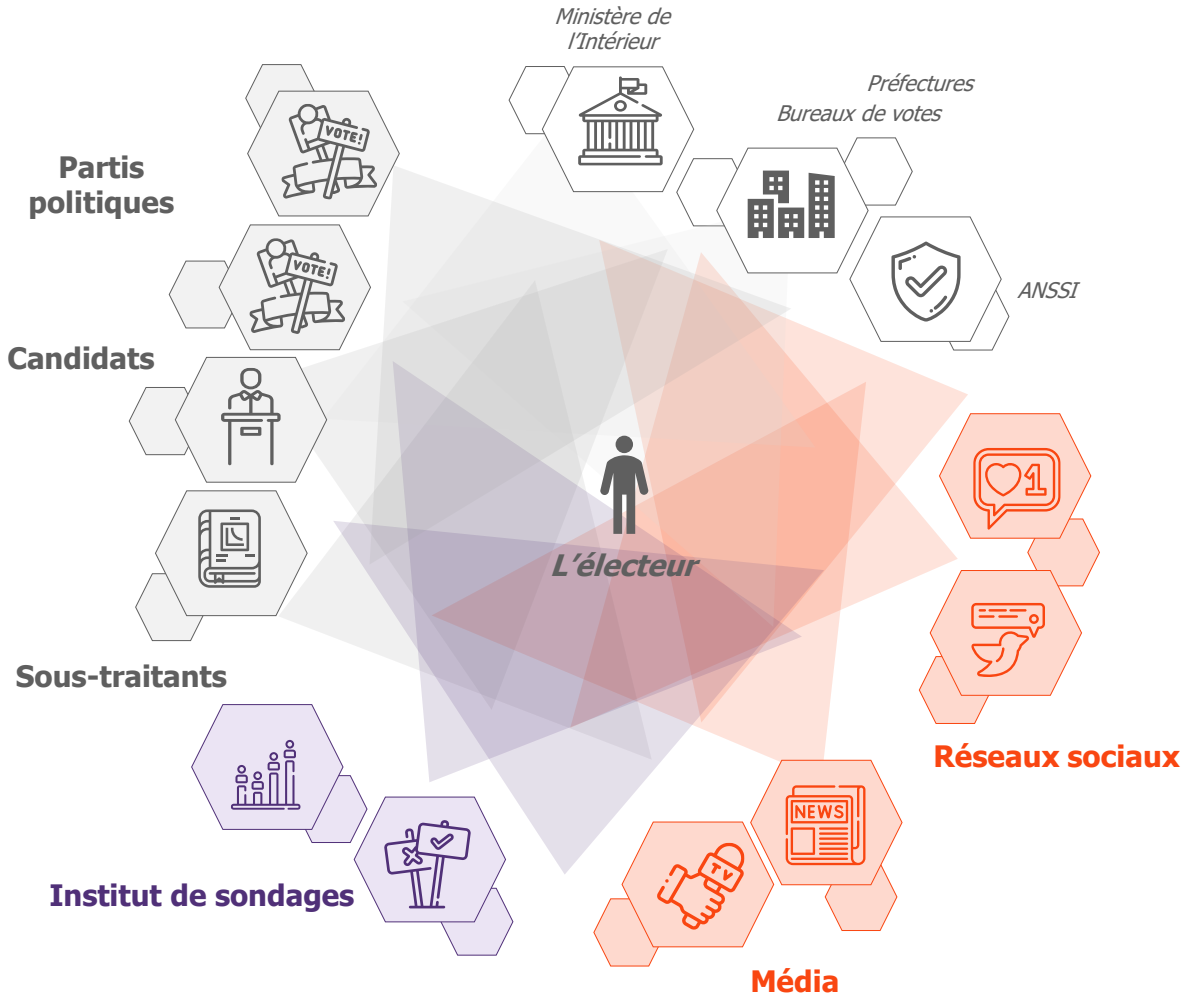
LES CIBLES PRINCIPALES DES CYBERATTAQUES NE SERONT CERTAINEMENT PAS LES SYSTÈMES ÉTATIQUES

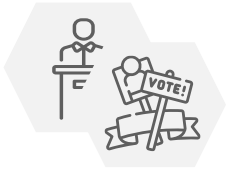
En France, les élections sont faiblement numérisées, plusieurs initiatives de vote électronique ont vu le jour mais n'ont pas été généralisées en particulier du fait des risques cyber.

Des systèmes numériques sont tout de même utilisés par exemple pour gérer les listes électorales, ou pour consolider les résultats des différents bureaux. Les équipes en charge sont centralisées et sous la responsabilité du ministère de l'Intérieur. Elles disposent de systèmes informatiques régulièrement audités et contrôlés par les autorités, en particulier par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

S'il existe incontestablement un risque cyber pesant sur ces acteurs, ce risque est connu et anticipé par l'Etat qui a les moyens d'agir. Ainsi, notre étude ne porte pas sur ce périmètre.

A l'inverse, d'autres acteurs de l'écosystème électoral sont plus vulnérables : partis politiques, candidats, instituts de sondage et leurs sous-traitants, médias et citoyens constituent des cibles bien plus simples pour les cyberattaquants.





Partis politiques et candidats aux élections

LES CIBLES IDÉALES

Les partis politiques ont un statut particulier (association loi 1901), et peuvent adopter l'organisation interne de leur choix, sous réserve de respecter des règles strictes en matière de financement.
Ils rassemblent deux grandes catégories d'individus :

- une équipe opérationnelle, composée le plus souvent de salariés
- des membres (les « militants »), le plus souvent bénévoles.

Cet écosystème est largement réparti sur le territoire.

L'identification du **candidat** et la création de son équipe dédiée pour l'élection entraînent de nombreuses modifications dans la gestion de l'organisation. Tout un **écosystème numérique** se crée pendant la campagne : site web, groupes sur les réseaux sociaux, utilisation de technologie innovante (par exemple les hologrammes en 2017, etc.)

Principales données sensibles

- Communications internes (courriels, messages, conversations téléphoniques)
- Programme et idées en cours de discussion
- Données relatives aux finances
- Données personnelles des militants, des soutiens, des équipes opérationnelles, des candidats, des sous-traitants

Fragilités intrinsèques majeures

Vélocité de la campagne électorale

Ancrage territorial forçant la décentralisation

Multiplication des parties prenantes sur le terrain (militants, prestataires...)

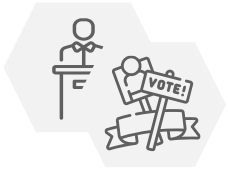
Règles de financement strictes laissant peu de moyens financiers dédiés à la cybersécurité

Financement des frais de campagne et cybersécurité : sortir la cybersécurité des comptes de campagne

Une loi électorale fixe à chaque présidentielle un plafond de dépense maximum (pour l'élection présidentielle 2017, ce plafond était de 16,851 millions d'euros pour les candidats au premier tour et de 22,509 millions d'euros pour le second tour). Le candidat est en droit d'être financé par autant de partis, de banques et d'acteurs privés qu'il le souhaite. Cependant, il est dans l'obligation d'une transparence totale. Pour 2022, c'est à partir du 1er juillet 2021 que toute dépense d'un candidat potentiel ou déjà déclaré, entre dans le cadre des comptes de campagne.

Afin de ne pas freiner les investissements nécessaires en cybersécurité, il nous semblerait important que les frais directement liés à la cybersécurité ne soient pas inclus dans les frais de campagne afin de garantir un socle commun de sécurité, et le bon déroulement démocratique de l'élection.

De quelques dizaines de personnes à plusieurs milliers, une croissance exponentielle pendant la campagne !



Des risques cyber pouvant impacter violement leur campagne

LES SCÉNARIOS DE CYBERATTAQUES LES PLUS PROBABLES

Confidentialité

/ Fuite de **messages, courriels, conversations téléphoniques, vidéoconférences**
/ Fuite des **comptes de campagne/information sur les soutiens financiers**
/ Fuite du **programme, des idées, et débats internes** au sein du parti
/ Fuite des **données personnelles** des militants, soutiens, candidats, équipes

Image

/ Mise en ligne de **vidéos compromettantes (réelles, à la suite d'une fuite de données, altérées ou créées de toute pièce)**
/ **Chantage** sur un candidat ou membre du parti pour empêcher la publication de contenu confidentiel / compromettant

Crédibilité / Accessibilité

/ **Interruption des réunions publiques en particulier leur retransmission**
/ **Dysfonctionnement majeur long des plateformes numériques** via une attaque en déni de service au moment clé de mobilisation
/ **Détournement des plateformes de dons** au parti politique

Des risques pouvant provenir du parti, de l'équipe du candidat mais aussi de tous les sous-traitants et bénévoles mobilisés !

Quand l'actualité rattrape la fiction

La société Adrexo a annoncé avoir été victime d'une supposée cyberattaque de type **ransomware** en amont du premier tour des élections régionales en juin 2021, complexifiant la distribution des professions de foi des candidats en temps et en heure.

Les instituts de sondages

DES CIBLES PROTÉGÉES PAR LEUR NOMBRES

Les sondages sont parties intégrantes des stratégies de campagne et servent d'outils de pilotage aux partis politiques. En plus des sondages publics rythmant la campagne, des études confidentielles sont commandées par les candidats. La fiabilité des estimations le soir des élections représente en outre évidemment un enjeu de taille pour la confiance dans les résultats de l'élection.

Un risque limité par la multitude d'acteurs et des mesures de contrôle humain

Loin d'être en situation de monopole, une multitude d'instituts se partagent le marché, atténuant ainsi le risque de sondage erroné à grande échelle et de perturbation des élections.
La plupart des écarts ou des fausses publications de sondage pourrait rapidement être détectée voire corrigée grâce aux interventions humaines dans le processus d'analyse et de publication. Mais cela pourrait quand même avoir un impact sur la confiance dans les instituts au niveau de l'opinion publique.

Principales données sensibles

Etudes d'opinion, en particulier celles confidentielles, commandées par les partis politiques pour tester des idées.

Données personnelles sur les panels de sondés.

Collecte de résultats électoraux pour réaliser des estimations « sortie d'urne » le jour du vote.

Fragilités intrinsèques majeures

Exposition plus forte aux risques du fait de la visibilité des élections par rapport à la situation courante

Utilisation de systèmes numériques anciens ou sur Internet.

Mobilisation de nombreux nouveaux collaborateurs et de multiples systèmes techniques additionnels.

Rapidité attendue des résultats et pression des donneurs d'ordre.

Départager des candidats par le biais d'un sondage ?

En vue des élections présidentielles, les Républicains ont décidé de désigner le candidat du parti grâce à un sondage. Le parti va commander au Cevipof deux grandes enquêtes d'opinion sur un panel représentatif de 15 000 personnes (de droite ou du centre droit) pour déterminer le candidat à la présidentielle du parti.

Les systèmes comme le personnel des instituts de sondage peuvent être ciblés par les attaquants

Les sondages, au cœur de la stratégie des partis politiques

LES SCÉNARIOS DE CYBERATTAQUES LES PLUS PROBABLES

Confidentialité

/ **Fuites des études confidentielles** commandées par les partis politiques, dévoilant ainsi des informations stratégiques (pistes de programmes, potentielles réformes, etc.)
/ **Fuites des communications internes** – relatives par exemples aux méthodes de redressement - utilisées à des fins de décrédibilisation des sondages ou de l'institut de sondage
/ **Fuite des résultats des estimations** avant leur publication (finalisés ou avant le redressement)

Intégrité

/ **Modification des résultats des études confidentielles** commandées par les partis politiques
/ **Manipulation des résultats** d'un sondage et publication pour déstabilisation
/ **Publication de fausses estimations** le jour de l'élection
/ **Paramétrage des différents modèles d'estimation**

Publication / Indisponibilité

/ **Impossibilité de publier les estimations** le jour des élections (perturbation du fonctionnement des logiciels de remontées, de la transmission des résultats...)

Les médias face aux maquis de la désinformation

ACTEURS DÉCISIFS ET CIBLES NATURELLES DE LA DÉSINFORMATION

Producteurs et relais d'information, les médias traditionnels (presse, télévision, radio) occupent une place décisive dans les campagnes électorales. Ces derniers ont la capacité d'orienter le débat politique vers certains thèmes d'actualité plutôt que d'autres et jouent donc un rôle majeur en contexte d'élections (fonction d'agenda).

Conscients du risque de désinformation, les médias se dotent d'outils de vérification d'information pour s'assurer de la véracité des informations qu'ils partagent. Dans la même lignée, des plateformes anti-fake news ont été mises en place pour permettre au grand public de vérifier la véracité d'une information (Decodex par le Monde, Factuels par l'AFP, etc.).

Mais les médias restent la cible potentielle de cyberattaques les visant directement.

Principales données sensibles

Sources des journalistes et échanges internes
Sondages d'opinion ou estimation en avant-première

Fragilités intrinsèques majeures

Augmentation majeure de leur visibilité et attaque sur leur légitimité
Difficulté de vérification de l'information dans un contexte où la rapidité est clé

LES SCENARIOS D'ATTAQUES LES PLUS PROBABLES

Diffusion

/ Interruption **du site web ou arrêt de diffusion** d'un débat ou des résultats de l'élection

Intégrité et désinformation

/ Publication **d'une fausse information** remettant en doute l'intégrité du média

Confidentialité

/ Diffusion des **sources des journalistes** ou d'information sous embargo

52% **des Français ont confiance en la radio, les journaux (48%) et la télévision (42%)** selon le baromètre Kantar-La Croix sur les médias de janvier 2021.

Les réseaux sociaux, théâtre des élections

CRÉATEURS ET VECTEURS D'INFORMATION

De l'information directe...

L'usage des réseaux sociaux dans les campagnes électorales évolue rapidement : de simple relai d'information à théâtre d'interactions entre candidats ou entre communautés (via Twitch, Clubhouse, Tiktok, Twitter, etc.), les réseaux sociaux occupent désormais une place centrale dans les campagnes électorales, pour diffuser de l'information et atteindre une cible différente de celle des lecteurs de médias traditionnels. Ils offrent également une tribune pour les influenceurs d'opinion, sans filtre éditorial.

... à l'exploitation des informations personnelles des utilisateurs. Les réseaux sociaux sont aussi le vecteur de réalisation de sondages d'opinion, voire de segmentation des bases électorales, grâce aux données personnelles disponibles sur les réseaux.

Principales données sensibles

Données personnelles des utilisateurs, en particulier leurs orientations politiques ou idéologiques
Identifiant/mot de passe de connexion de personnalités majeures

Fragilités intrinsèques majeures

Intégrité des informations transmises
Volume d'information et rapidité de diffusion

LES SCENARIOS D'ATTAQUES LES PLUS PROBABLES

Confidentialité

- Accès frauduleux aux comptes de personnes clés sur les réseaux sociaux et fuite des **communications privées**
- **Vols de données** personnelles des utilisateurs avec risque d'appropriation à des fins de manipulation d'opinion

Intégrité et désinformation

- **Diffusion massive** de fausses informations
- Détournement des algorithmes / de la segmentation pour favoriser tel ou tel acteurs
- **Vol de comptes et modification de publication** sur un réseau à l'insu de son auteur

Accessibilité

- **Blocage de l'accès** aux plateformes ou aux comptes pour certains utilisateurs
- **Rupture du service,** arrêt des plateformes à des moments clés

28% **des Français déclarent avoir confiance dans les informations recueillies sur internet.** Les sites des titres de presse écrite sont privilégiés (29%) devant les réseaux sociaux (20%) selon le baromètre Kantar-La Croix sur les médias de janvier 2021.

La nouvelle fabrique de l'opinion, Thomas Huchon (2019)

Ce documentaire démontre que les posts likés, partagés ou commentés, enferment l'utilisateur de Facebook dans une "bulle" où ses opinions sont confortées par la mise en avant d'informations ne remettant pas en cause ses idées. Or le débat d'opinion naît de la confrontation d'idées contradictoires. Ce cloisonnement de l'utilisateur met en péril la démocratie. Qu'adviendrait-il si des attaquants arrivaient à influencer les algorithmes de réseaux sociaux pour enfermer sciemment les utilisateurs dans une bulle idéologique ?

Focus sur... les deepfakes

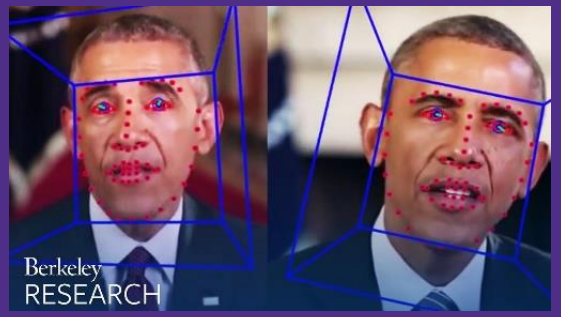
MENACE NOUVELLE GÉNÉRATION ?

Qu'est que le deepfake ?

Le deepfake désigne la modification d'images ou de vidéos via de l'Intelligence Artificielle (et notamment du « Deep Learning » et les Generative Adversarial Network – GAN ») pour présenter une vision falsifiée (« fake ») de la réalité.

Au cœur des élections, le deepfake peut être une arme majeure de déstabilisation.

Beaucoup de communications autour de ces vidéos modifiées ont été relayées. Parmi les plus connus figurent les exemples d'**Emmanuel Macron ou de Barack Obama.** Celles-ci participent à la connaissance du phénomène et alertent les internautes.



Les deepfakes représentent un risque non négligeable pour les élections présidentielles. Le FBI a d'ailleurs récemment publié un avertissement selon lequel des acteurs malveillants *« tireront certainement parti des deepfakes pour des opérations d'influence cyber et étrangères au cours des 12 à 18 prochains mois »*.

Ce risque est tout de même à nuancer compte tenu du caractère flagrant que ces modifications de vidéos peuvent prendre en 2021. Des deepfakes de bonne qualité, faisant tenir aux candidats des discours exagérés ou absurdes, seraient vite détectés.

- Le risque réside plutôt dans la **création de vidéos de basse qualité,** comme des vidéos volées, **des "cheap fake"** qui paraitraient certainement encore plus crédibles.
- La **facilité de réalisation de ces vidéos**, même de mauvaise qualité, peut polluer la campagne obligeant les candidats à démentir sans arrêt des nouveaux éléments.

Une création simplifiée
De nombreuses applications permettent de créer une deepfake en transformant le visage de personnalités (ex: Deepword, DeepFaceLab, Zao, etc.)

Même si la détection des deepfakes sur les réseaux sociaux est souvent possible à l'œil nu, les algorithmes évoluent très rapidement améliorant considérablement leur vraisemblance. En conséquence, certains outils ont été développés pour les détecter.

Detection in progress...

Microsoft's Video Authenticator tool, le français Buster IA ou bien encore Facebook (et la Michigan State University) développent des IA capables de détecter les deepfakes

« Deepfake Detection Challenge » 2019

Facebook et Microsoft s'unissent pour lancer un concours pour détecter les deepfakes. L'objectif est de disposer d'une base de données suffisante pour pouvoir repérer plus facilement les deepfakes.

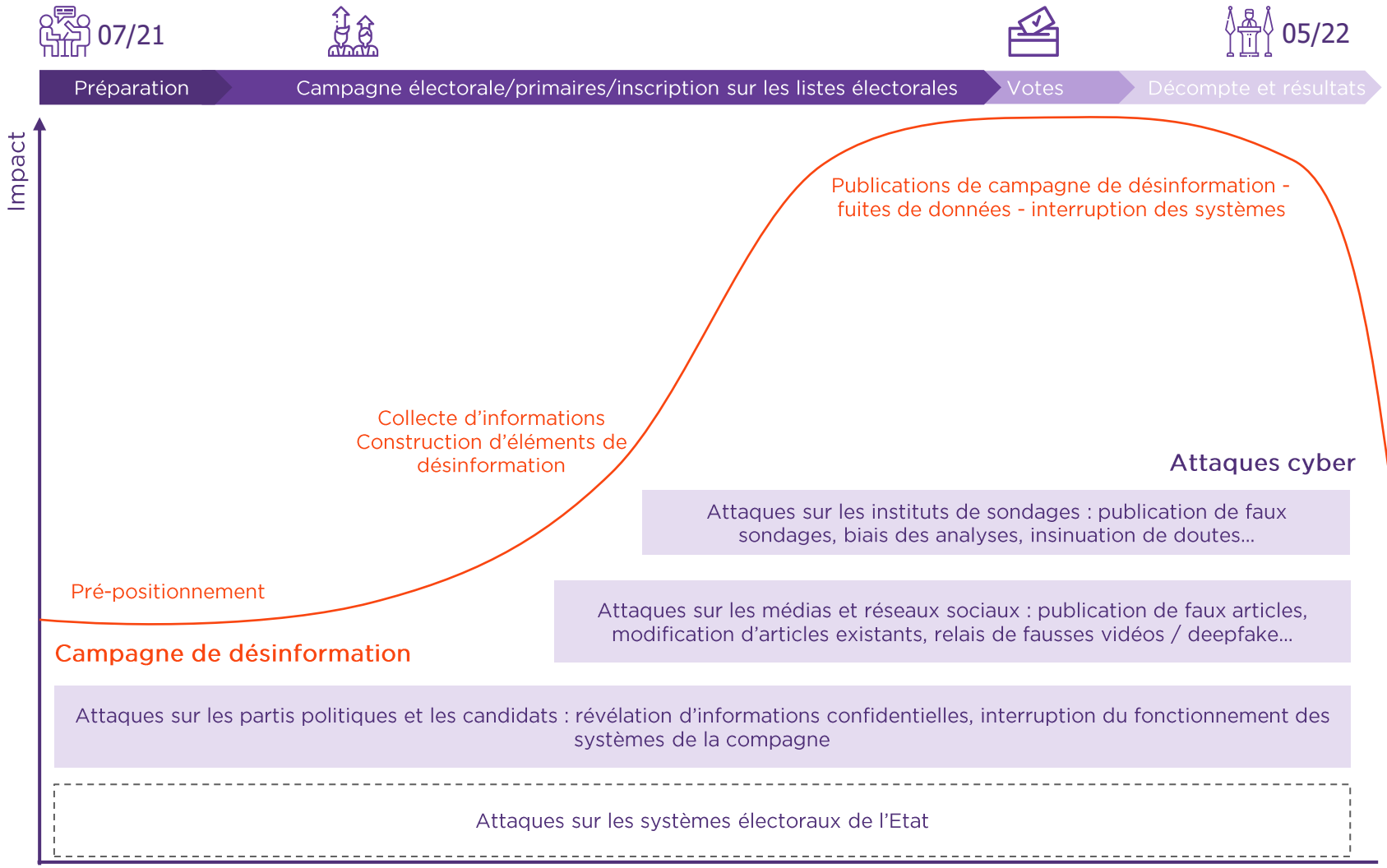
Le risque cyber est déjà réel et va s'intensifier

UN CALENDRIER D'ATTAQUES DÉPENDANT DES CIBLES

Même si les actions les plus visibles auront lieu dans les dernières semaines de la campagne, il ne faut pas négliger le fait que les attaquants vont commencer leurs actions en amont.

Des opérations de pré-positionnement, d'interception d'information ou de construction de campagne de désinformation sont certainement déjà en cours.

L'enjeu principal pour l'ensemble des cibles est de commencer à se protéger dès maintenant.



03

Quelles solutions concrètes pour faire face au risque cyber ?

5 réflexes

Pour gérer le risque cyber

Pour l'ensemble des acteurs, une sélection de mesures et de solutions de sécurité à prévoir est indiquées. Elles s'appliquent à tous en tant qu' utilisateurs des mêmes solutions numériques (ordinateur, téléphone, courriels, etc.).

Sont présentées, à titre indicatif et non exhaustif, des startups françaises pouvant apporter des solutions concrètes.

L'Etat se mobilise également par l'intermédiaire de l'ANSSI en mettant en place des actions de sensibilisation et en créant un lien avec les partis politiques pour assurer leur sécurité.

S'organiser & sensibiliser

Faire de la cybersécurité une préoccupation partagée

Protéger ses communications et ses données

Sécuriser les données échangées, savoir qui est qui et qui accède à quoi

Solidifier son système d'information

Une protection à prévoir sur toutes les dimensions du numérique

Détecter & réagir à une cyberattaque

Connaitre ses failles et celles des ses fournisseurs, préparer la gestion de crise

Contrer La Désinformation

Une désinformation inventée de toute pièce ou alimentée par des fuites de données réelles

S’organiser & sensibiliser

FAIRE DE LA CYBERSÉCURITÉ UNE PRÉOCCUPATION PARTAGÉE

- ☐ Un **responsable de la cybersécurité** doit être identifié, avec, si besoin, une équipe à ses côtés.
- ☐ Identifier en réalisant une analyse de risques, **les cercles de sensibilité** (VIP, candidats, élus, équipes dirigeantes, salariés, membres, militants, etc.), et les mesures de sécurité à mettre en place (chiffrement, authentification forte, etc.) sur les différents systèmes et outils de communication (courriel, messagerie instantanée, gestion des documents…)
- ☐ Prévoir un **budget dédié à la cybersécurité,** en fonction des approches adoptées (compétences existantes ou non en interne, utilisation de systèmes open source, recours à des prestataires externes, etc.). Ce budget oscille usuellement autour des 5% du budget consacré au numérique.
- ☐ Des **actions de sensibilisation** aux risques cyber et aux bonnes pratiques doivent être réalisées pour l’ensemble des personnes. Des ateliers en personne peuvent être prévus pour les profils les plus sensibles, des actions de communication peuvent être envisagées plus largement.
- ☐ Le **niveau de sensibilisation** doit être testé régulièrement, en particulier de fausses campagnes de phishing doivent être organisées.
- ☐ Des **règles de sécurité** doivent être formalisées dans une charte sur les sujets les plus importants (communication, partage d’information, alertes, échanges avec des tiers, solidité des mots de passe). **Cette charte** doit être communiquée et validée individuellement.

25%

des attaquants se sont infiltrés dans le réseau de l’organisation par un email de phishing *(benchmark du CERT-Wavestone, 2020)*

Les solutions des startups françaises

- mantra — Sensibilisation
- Augmented CISO — Règles et politiques de sécurité
- AVANTDECLIQUER.COM — La sensibilisation à la cybersécurité réinventée — Simulation de phishing
- phinasoft — Management des risques
- Citalid — Impact financier des cyberattaques
- EGERIE — INTEGRATED CYBERRISK MANAGEMENT — Management des risques

Focus sur.... les élus et les militants

LES GESTES SIMPLES ET EFFICACES À APPLIQUER À L'ÉCHELLE D'UN INDIVIDU

- [ ] **Renouveler ses mots de passe** avant et pendant la campagne, utiliser des mots de passe différents, et utiliser un coffre-fort de mot de passe pour les gérer plus simplement sans devoir les retenir
- [ ] **Activer** un code en plus du mot de passe (authentification forte) sur ses réseaux sociaux, sa messagerie et les systèmes de gestion/édition de documents (solution gratuite chez les principaux fournisseurs)
- [ ] Renforcer la confidentialité de ses échanges dans les transports grâce à un **filtre de confidentialité** sur le PC et le téléphone mobile
- [ ] **Adopter les bons réflexes dans sa messagerie et détecter les tentatives de fraude aux faux-emails (phishing/hameçonnage ») :**

  / Vérifier l'expéditeur et la cohérence du contenu (orthographe, grammaire, mise en forme, etc.)

  / Ne pas ouvrir les pièces-jointes d'un expéditeur inconnu

  / Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles (mot de passe, compte...).

  / En cas de doute, contacter avec les numéros usuels les interlocuteurs ou aller directement sur les sites mentionnés sans cliquer sur les liens présents dans l'email qui peuvent être piégés

  / Et surtout alerter votre organisation !

Qu'est que le phishing (hameçonnage) ?

Le phishing est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, etc.) et/ou bancaires en se faisant passer pour un tiers de confiance.

Si vous pensez avoir été victime ou témoin d'un contenu illicite ?

Changer immédiatement les identifiants éventuellement compromis et vos mots de passe

Signaler un acte de cybermalveillance ou un contenu illicite sur internet sur le site www.cybermalveillance.gouv.fr

Protéger ses communications et ses données

SÉCURISER LES DONNÉES ÉCHANGÉES, SAVOIR QUI EST QUI ET QUI ACCÈDE À QUOI

Assurer la confidentialité des échanges

- ☐ Utiliser des **outils de communication** (messagerie instantanée, courriel, visioconférence…) professionnels dont le niveau de sécurité est vérifié indépendamment, en particulier pour les échanges les plus sensibles. Ces systèmes doivent permettre le chiffrement et l'identification des interlocuteurs.
- ☐ Mettre en place **un code en plus du mot de passe** (authentification forte) pour accéder aux données les plus sensibles.
- ☐ Protéger avec un code ou une vérification de l'identité **l'accès aux visioconférences**.
- ☐ Mettre en place **un système de gestion des identités** (comptes, mot de passe, droit d'accès…) et **revoir régulièrement qui a accès à quoi**. Ceci dans les systèmes internes de l'organisation mais aussi sur les différents canaux numériques, en particulier **les groupes de discussion** dans les messageries instantanées.

Pouvoir prouver ce que l'on a dit et suivre les documents

- ☐ Pour les documents les plus sensibles, mettre en place une **solution de chiffrement et de restriction des droits** (copie, impression, etc.) pour garantir la confidentialité durant la création (DRM).
- ☐ Disposer d'une **solution pour marquer électroniquement** les documents et pouvoir suivre leurs consultations lors de diffusions plus larges (watermarking).
- ☐ Pouvoir **signer électroniquement** un document pour en prouver son authenticité ultérieurement.

POUR ou CONTRE utiliser Telegram & Whatsapp ?

Telegram ne garantit pas le chiffrement des communications et a donc accès à la majorité des contenus échangés.

WhatsApp/Signal utilisent une structure centralisée d'annuaire qui permet de connaitre l'existence d'échanges entre deux individus et qui empêche d'apporter une garantie forte sur l'identité de vos interlocuteurs.

D'autres modèles existent, complètement décentralisés, comme celui d'Olvid (solution française certifiée par les autorités) qui garantit un plus haut niveau de confidentialité des échanges incluant le chiffrement et une meilleure garantie sur l'identité des interlocuteurs.

Les solutions des startups françaises

- Olvid — Messagerie instantanée
- tilkee — Partage de documents et traçabilité
- Whaller — Plateforme collaborative
- ilex International — IAM
- reachfive — IAM
- yousign — Signature électronique
- inwebo — Authentification forte
- WaToo — Marquage de documents
- TIXEO SECURE VIDEO CONFERENCING — Vidéoconférence
- pradeo — Protection des terminaux mobiles

Solidifier son système d'information

UNE PROTECTION A PRÉVOIR SUR TOUTES LES DIMENSIONS DU NUMÉRIQUE

Pour les équipements et services des utilisateurs

- ☐ Fournir et gérer centralement **les équipements numériques** (ordinateurs, téléphones, tablettes…) des personnes les plus sensibles. Imposer **le chiffrement du contenu**, le déploiement automatique des **correctifs de sécurité** et la présence **d'un code de déverrouillage.** Restreindre au maximum les usages personnels.
- ☐ Sur les ordinateurs, prévoir **l'installation d'un logiciel de sécurité dédié** (EDR).
- ☐ Mettre en place une **solution de filtrage des emails et des accès Internet** pour réduire le risque de phishing, de spam, de visite de sites dangereux et la fuite d'information.
- ☐ S'assurer que les systèmes de travail collaboratif et les espaces de stockage de documents utilisent **du chiffrement lors des échanges ou de l'accès à distance** (VPN).
- ☐ Mettre en place **un système de sauvegarde**, fréquemment réalisé, externalisé et testé régulièrement.

Pour les systèmes centraux et locaux

- ☐ Gérer centralement les serveurs, s'assurer de **la traçabilité** des actions réalisées et du chiffrement de leur contenu.
- ☐ Sécuriser **le réseau wifi** (WPA3, authentification machine) et mettre en place **un wifi invité** avec des identifiants de connexion et une traçabilité.
- ☐ **Segmenter le réseau de l'organisation** pour protéger les données les plus sensibles, protéger l'accès aux locaux de l'organisation et en particulier aux salles serveurs et aux locaux techniques.
- ☐ Prévoir **la mise en place de solutions de sécurité** sur les systèmes exposés à l'extérieur, pare-feu réseau et application mais également pour éviter les attaques par saturation (anti DDOS).
- ☐ Identifier précisément **les administrateurs des systèmes**, leur faire signer une charte de bonne conduite et imposer l'authentification forte pour réaliser les actions d'administration.
- ☐ Répliquer les exigences de sécurité de l'organisation dans **les contrats de services des prestataires.**

Les solutions des startups françaises

- THEGREENBOW — VPN
- TEHTRIS (FACE THE UNPREDICTABLE) — Détection des menaces (EDR)
- HARFANGLAB — Détection des menaces (EDR)
- Sesame it (Cyber-sécurité | Sondes de détection) — Sondes de détection
- DATADOME — Protection contre les bots
- vade — Filtrage de messagerie
- GATEWATCHER — Détection des menaces (EDR)
- CrowdSec — Détection des menaces (EDR)
- OZON — Détection des vulnérabilités
- Cyberwatch — Gestion des vulnérabilités
- MAILINBLACK — Sécurité email

Détecter & réagir à une cyberattaque

CONNAITRE SES FAILLES ET CELLES DES SES FOURNISSEURS,
PRÉPARER LA GESTION DE CRISE

Vérifier ses systèmes et détecter les attaques

- ☐ Régulièrement **auditer la sécurité** des systèmes numériques (internes et externes), soit via des audits cybersécurité soit en utilisant les plateformes de bug bounty.
- ☐ Prévoir dans tous les contrats de services, **le droit d'auditer** et l'obligation de **corriger les failles identifiées**.
- ☐ Suivre quotidiennement **les alertes de sécurité** (via le site du CERT-FR) pour être en mesure de réagir et corriger d'éventuelles vulnérabilités.
- ☐ Surveiller en **24/7** les systèmes les plus critiques pour détecter des tentatives d'intrusion (IPS) et **les fuites de données** (DLP) soit en interne soit via des fournisseurs de services externes spécialisés.

Qu'est que le Bug Bounty ?

Le bug bounty - prime aux bogues en français - désigne un programme de récompenses destinés aux personnes qui identifient et remontent des vulnérabilités. Cette approche est plus dynamique que les audits traditionnels et fonctionne en continue grâce à la communauté de hacker éthiques qui se mobilise via la plateforme.

Des capacités de détection trop faibles face à la rapidité des attaquants (benchmark CERT-W 2020, Wavestone)

29 jours
Délai moyen pour qu'un attaquant réussisse une attaque ransomware en France en 2020

94 jours
Délai moyen pour détecter une cyberattaque dans le système d'information par son propriétaire

Les solutions des startups françaises

YES WE HACK
Bug bounty

YogOsha
Bug bounty

SEKOIA
Renseignement sur les menaces (CTI)

HACKUITY
Gestion des vulnérabilités

SHADLINE
Plateforme d'échanges sécurisés

Détecter & réagir à une cyberattaque

CONNAITRE SES FAILLES ET CELLES DE SES FOURNISSEURS,
PRÉPARER LA GESTION DE CRISE

Réagir

- [ ] Définir **comment réagir** en cas de cyberattaque : qui alerte, qui mobiliser, quelles compétences disponibles, qui porte plainte, quelle réaction médiatique, quel délai pour reconstruire les systèmes touchés…
- [ ] Anticiper les **réponses médiatiques et juridiques** en cas d'attaque (un porte-parole, arbre de décision, tableau de réponse, etc.).
- [ ] Envisager **la souscription à un contrat de cyber assurance** et/ou un **contrat d'intervention en urgence** auprès de spécialiste de l'investigation numérique et de la gestion de crise cyber (CERT).
- [ ] Disposer de **moyens pour gérer la crise** (communication, partage de fichiers…) indépendants du système d'information usuel au cas où il serait détruit.
- [ ] Réaliser un **exercice de crise** ou « stress test » pour simuler une attaque et voir comment l'organisation réagirait, de manière organisationnelle ou technique.

Qu'est qu'un CERT ?

Un CERT (Computer Emergency Response Team) est une équipe de réaction aux incidents informatiques capable d'intervenir en urgence pour analyser et contrer des attaques mais aussi réparer les systèmes touchés. Les CERT réalisent également de la veille sur les menaces et peuvent aider à anticiper de futures attaques.

Combien de temps pour un retour à une situation technique normale ? (benchmark CERT-W 2020, Wavestone)

De plus en plus d'attaques combinées (ransomware et vol de données), nécessitant de nouvelles parties prenantes dans la gestion de crise : communicant, DPO, etc.

3 semaines
Délais moyen de clôture d'une crise

Contrer la désinformation

UNE DÉSINFORMATION INVENTÉE DE TOUTE PIÈCE OU ALIMENTÉE PAR DES FUITES DE DONNÉES RÉELLES

Surveiller et alerter

- ☐ Veiller **les tendances montantes** (hashtag, sujets du moment) et être attentif dans les opérations de modération aux éléments évoqués pour détecter les fausses informations
- ☐ **Surveiller régulièrement la présence numérique** des acteurs clés de la structure (candidats, VIP, etc.) pour détecter des informations sensibles (historiquement présentes ou ajoutées récemment) ou le vol de comptes
- ☐ **Sensibiliser les collaborateurs et/ou les militants** aux risques de la désinformation et à la manière de réagir
- ☐ Créer des **canaux d'alertes simples** pour pouvoir faire des signalements

Réagir efficacement

- ☐ Intégrer dans les **scénarios** préparés par les cellules de **riposte médiatique** un volet cyberattaque, en particulier sur la fuite de données ou la création de faux contenu
- ☐ Mettre en place des **outils de riposte technologique** en cas d'attaque sur les réseaux afin de faciliter la modération du contenu et la réponse (automatisation des actions, publication d'éléments de réponse…)
- ☐ Anticiper une **réponse juridique** en particulier s'il y a vol de données ou divulgation d'éléments confidentiels, incluant un dépôt de plainte et des actions auprès des hébergeurs / réseaux sociaux pour demander l'effacement du contenu

Une approche disruptive : La contre-offensive de En Marche !, 2017

Pour contrer les cyberattaques, l'équipe de campagne de En Marche ! a affirmé avoir mêlé à ses données de fausses informations afin d'obliger les attaquants à vérifier les données récupérées, au risque de se décrédibiliser. Parmi ces fausses informations, on compte notamment des faux identifiants de connexion, et de faux documents internes. Si ce dispositif est astucieux, il doit être mis en œuvre avec grande précaution pour éviter d'alimenter la désinformation.

Les solutions des startups françaises

Bodyguard — Modération de contenus haineux

Buster.Ai — Détection deepfake/fake news

ANOZR WAY (cyber artificial intelligence) — Analyse des profils des collaborateurs clés pour anticiper des attaques

leakwatch — Détection de fuite de données

CybelAngel — Détection de fuite de données et renseignement sur les attaques

Focus sur .... L'Agence nationale de lutte contre la manipulation de l'information

UNE INITIATIVE DE L'ETAT POUR LUTTER CONTRE LA DÉSINFORMATION

Le Secrétariat Général de la Sécurité et la Défense Nationale (SGDSN) a annoncé le 2 juin la création d'une agence nationale de lutte contre la désinformation en provenance de l'étranger et visant à « déstabiliser l'État » : *le Service de vigilance et de protection contre les ingérences numériques étrangères : VigiNum.*

Cette cellule a pour objectif d'analyser la menace, de pouvoir alerter les acteurs concernés et d'y répondre collectivement. Elle ne vise pas à définir ce qui est « vrai » ou « faux » mais bien à identifier les tendances fortes de manipulation de l'information (relais par des réseaux de faux comptes ou de comptes automatisés, mouvement massif...).

Cette agence va monter en puissance progressivement et se mobilisera fortement sur les élections présidentielles.

2021
Septembre

60

Source ouverte

Comité d'éthique

Une tendance internationale

« Il ne s'agit pas de corriger ou rétablir la vérité, mais d'arriver à détecter les attaques quand elles viennent de l'étranger, pouvoir les caractériser et d'une certaine manière les attribuer »

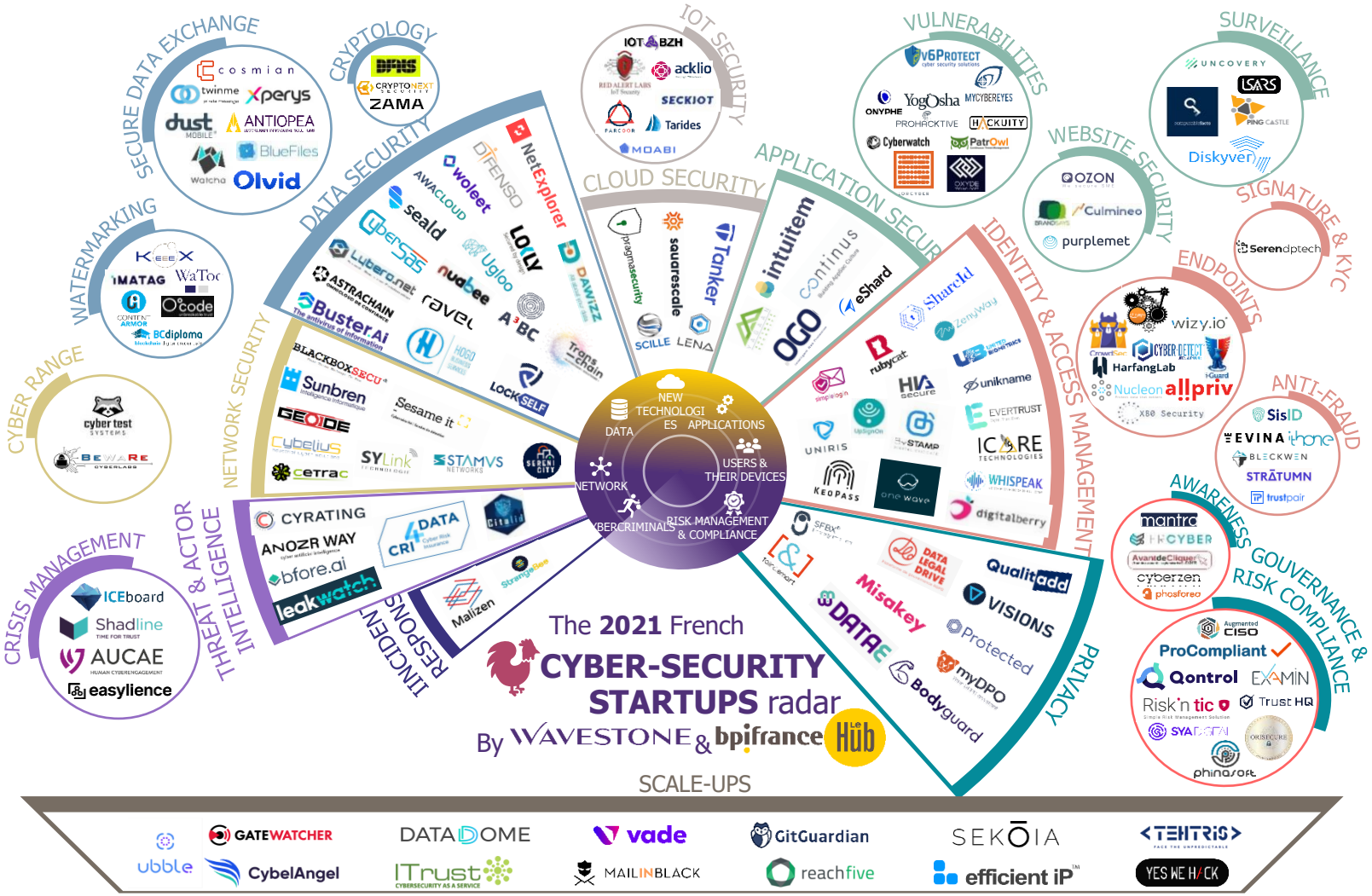
Stéphane Bouillon, SGDSN

L'écosystème français de la cybersécurité est prêt à se mobiliser

DES GÉANTS DU NUMÉRIQUE AUX STARTUPS

Au delà des **startups et PME** mises en avant dans les pages précédentes, la France héberge **un écosystème complet** qui permet de lutter contre les menaces cyber. Il est composé de plusieurs centaines d'acteurs, grandes entreprises, PME, ETI mais aussi de plus de **150 startups et de 13 scale-ups** répartis sur tout le territoire. Elles représentent un patrimoine unique et une chance pour notre économie.

Startup : - de 7 ans d'existence, - de 35 collaborateurs ; Scale-up : levée de fonds de plus de 10M€ sur les 3 dernières années ou critère de croissance de CA. Détails disponibles sur wavestone.com



Conclusion

AGIR MAINTENANT

Avril 2022… une élection présidentielle évidemment sous haute tension.

C’est la mobilisation de tous qui permettra de limiter le risque de cyberattaque et ses éventuels impacts.

Agissons maintenant !

Méthodologie et remerciements

Auditions

Cette étude est basée sur la réalisation d'analyse documentaire et d'entretiens à la fois avec des acteurs institutionnels, des acteurs de l'écosystème électoral (partis politiques, instituts de sondage…) et des startups françaises pouvant apporter des solutions aux risques identifiés.

Durant ces entretiens, le fil conducteur de la discussion a été d'identifier les risques cyber pesant sur les acteurs de l'écosystème des élections. Nous avons souhaité appréhender les cas d'usage, les dispositifs déjà mis en œuvre ainsi que les besoins.

France Digitale et Wavestone souhaitent particulièrement mettre en avant des startups françaises qui sont en mesure de proposer des réponses aux enjeux électoraux.

- Nassima Auvray - Conseillère Innovation et numérique, Cabinet de Madame la Ministre des Armées Florence Parly
- Caroline Faillet – Opinion Act, CEO et cofondateur
- Julien Mardas - Buster.AI, CEO et cofondateur
- Matthieu Boutard et Bastien Poncet – Bodyguard, respectivement DG et responsable ventes/partenariats
- Florent Grosmaitre et Ludovic Perret - Cryptonext Security, respectivement CEO ainsi de cofondateur et CPO
- François Mattens – GICAT, Directeur des affaires publiques et de l'innovation
- Patrick Ragaru – Hackuity, CEO
- Olivier Perroquin – InWeBo, CEO
- Luc Pallavadino – Yousign, CEO
- Guillaume Vassault-Houlière -YesWeHack, CEO
- Cédric Sylvestre et Thomas Baignères - Olvid, co-founders, respectivement responsable business development et CEO
- Jurgita Miseviciute et Serge Droz – Proton Mail, respectivement public policy-government affairs lead et head of cybersecurity
- Thomas Huchon – Spicee et LCI, journaliste et animateur de l'émission Anti-complot
- François Lavaste – Ace Capital partners, venture & growth
- Frédéric Micheau – OpinionWay, directeur général adjoint, en charge du département opinion et politique
- Des responsables des outils numériques de partis et mouvements politiques
- Sarah Nicole, Policy analyst, France Digitale

Sources

Martin Untersinger. Des pirates informatiques russes, chinois et iraniens ont visé la présidentielle américaine, selon Microsoft. Le Monde. 11/09/2020

Martin Untersinger. Bugs, cyberattaques, suspicions… le système élecotoral américain sous pression. Le Monde. 29/09/2020

Grégor Brandy. QAnon : aux racines de la théorie conspirationniste qui contamine l'Amérique. Le Monde. 21/01/2021

Auteur inconnu. Le chiffre du jour - Les vrais croyants complotistes de QAnon aux États-Unis. Courrier international. 28/05/2021

Michaël Szadkowsky. « Infox » au Brésil : comment les fausses informations ont inondé WhatsApp. 27/10/2018

Ghernaouti, S. & Dufour, A. Chapitre premier - Des origines aux réalités de l'Internet. Presses Universitaires de France. 2017

Laurent De, B. *L'élection présidentielle 2002 se jouera aussi sur Internet*. La Croix 24/02/2002

Corinne Petiprez. L'influence de Cambridge Analytica sur le Brexit. École de Guerre économique. 29/12/2018

Auteur inconnu. Succès des fausses informations dans les derniers mois de la campagne américaine. Le Monde 17/11/2016

Véronique Le Billon. Cybersécurité: attaqués, les États-Unis se mettent en ordre de bataille. Les Échos. 10/05/2021

Baromètre Kantar-La Croix sur les médias, Janvier 2021

Benchmark du CERT-Wavestone, 2020

Radar des startups cybersécurité, 2021, BPI France et Wavestone

Les Echos, « Fake news : la France se dote d'une agence de surveillance des réseaux », 2 juin 2021

Podcast: le financement d'une campagne présidentielle, comment ça marche? Émission Élysée, la bataille. France Info. 18/06/2021

Cara Manke, Researchers use facial quirks to unmask 'deepfakes', Berkeley News, https://news.berkeley.edu/2019/06/18/researchers-use-facial-quirks-to-unmask-deepfakes/

Contributeurs

FRANCE DIGITALE

Marianne Tordeux
Directrice des affaires publiques
marianne@francedigitale.org

Mathieu Richard
Policy Analyst
mathieu@francedigitale.org

Lara Rouyres
Board member
Lara@levia.ai

WAVESTONE

Gérôme Billois
Associé
Cybersécurité
gerome.billois@wavestone.com

Marguerite Quichaud
Consultante
Cybersécurité
marguerite.quichaud@wavestone.com

FRANCE DIGITALE

Fondée en 2012, France Digitale est la plus grande association de startups et VC's en Europe. L'association représente plus de 1800 entrepreneurs et investisseurs du numérique. France Digitale se donne pour mission de créer des champions européens du numérique et d'animer l'écosystème des startups en France.

France Digitale est co-présidée par Frédéric Mazzella, co-fondateur de BlablaCar, et Benoist Grossmann, CEO d'Eurazeo Investment Manager.

La crise de la Covid-19 souligne l'impréparation du monde face à la transition numérique. La résilience ainsi que la relance de la France se basent sur l'appropriation d'outils et solutions numériques. 2022 est une année présidentielle. il est indéniable d'affirmer que cette élection se jouera aussi dans l'espace numérique. France Digitale est convaincue que les startups françaises peuvent proposer des solutions pour répondre à ce défi.

Plus d'informations sur www.francedigitale.org
@fFRdigitale

WAVESTONE

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Parmi les leaders indépendants du conseil en Europe, Wavestone rassemble plus de 3 000 collaborateurs dans 8 pays dont plus de 600 consultants en cybersécurité. Ces derniers accompagnent des organisations sur tous les enjeux de cybersécurité, des plus stratégiques à la mise en œuvre opérationnelle, en passant par la réponse à incident et l'investigation numérique.

Wavestone est coté sur Euronext à Paris.

Plus d'informations sur www.wavestone.com/fr/
@Wavestone_
@RiskInsight