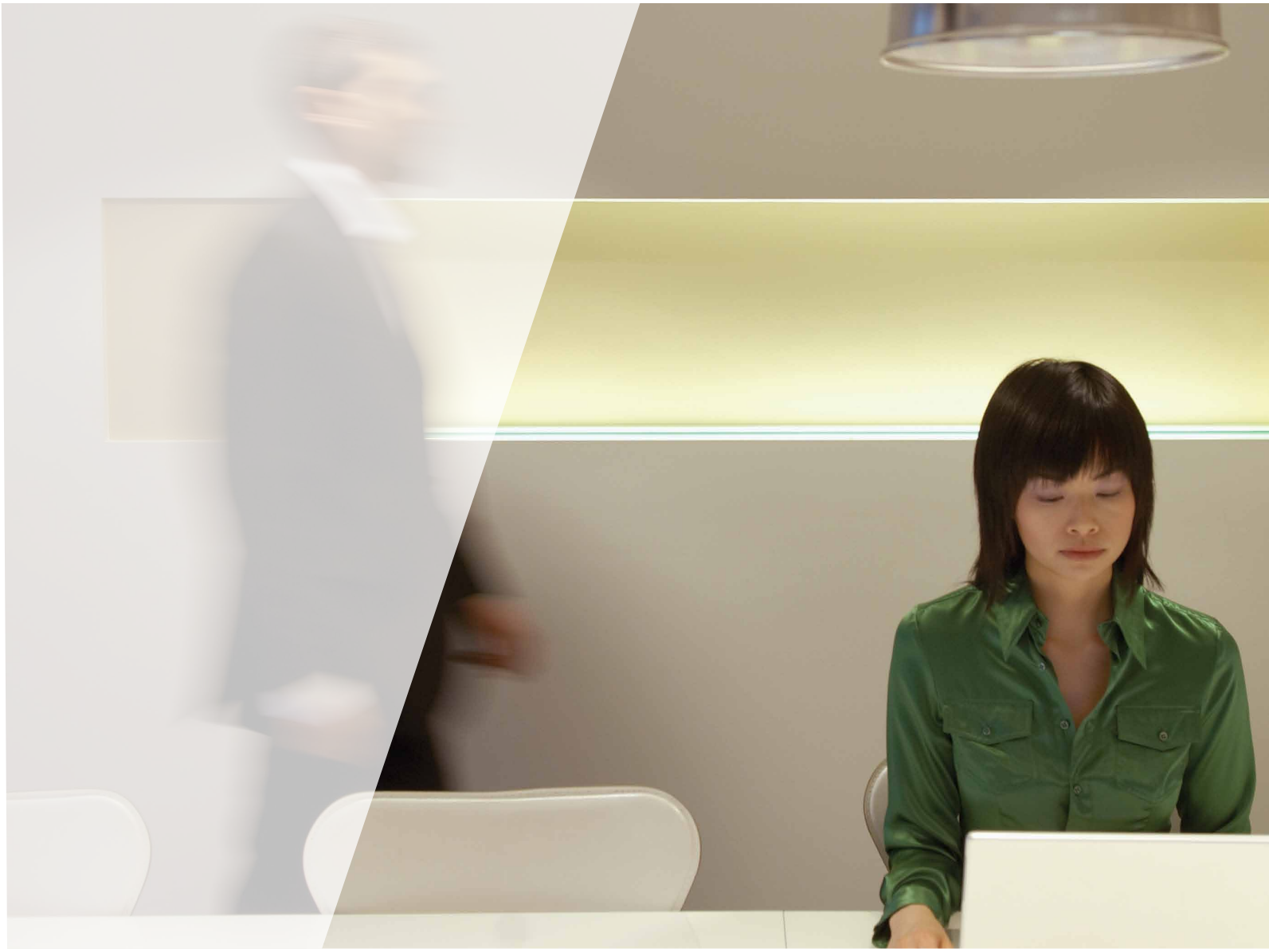
# Dans la ligne de mire

## Les infrastructures critiques à l'aube de la guerre numérique

Rapport mondial sur les menaces posées aux secteurs d'activité clés



## Dans la ligne de mire

Auteurs :

Stewart Baker, membre invité distingué du CSIS, partenaire chez Steptoe & Johnson

Shaun Waterman, chercheur et rédacteur pour le CSIS

George Ivanov, chercheur auprès du CSIS

## SOMMAIRE

# Introduction et contexte de l'étude

Dans un monde de plus en plus interconnecté, les vulnérabilités informatiques des infrastructures critiques représentent un enjeu de taille tant pour leurs propriétaires et opérateurs, quel que soit le secteur, que pour les pouvoirs publics et ce, à l'échelle mondiale.

Compte tenu de la fragilité de l'économie mondiale après la crise financière de l'année dernière, les Etats sont tentés de reléguer au second plan de leurs priorités l'intégrité et la disponibilité de secteurs d'activité d'importance capitale au niveau national alors qu'elles restent des facteurs déterminants de vulnérabilité stratégique.

Six cents cadres dirigeants en informatique et en sécurité de diverses entreprises gérant des infrastructures critiques dans sept secteurs et 14 pays ont répondu de façon anonyme à un questionnaire complet et détaillé sur leurs pratiques, attitudes et politiques en matière de sécurité. Les questions portaient notamment sur l'impact des réglementations, leurs relations avec les pouvoirs publics, les mesures de sécurité spécifiques mises en place sur leur réseau ainsi que les types d'attaques auxquels ils sont confrontés.

Les propriétaires et opérateurs de ces infrastructures critiques affirment que leurs réseaux informatiques font l'objet d'attaques répétées, souvent par des adversaires de grande envergure. Ces attaques ont généralement un impact majeur, et leur coût élevé se fait ressentir à tous les niveaux.

Bien que ces cadres dirigeants se déclarent globalement satisfaits des ressources dont ils disposent pour assurer la sécurité de leur entreprise, les réductions de coûts liées à la crise sont généralisées et parfois importantes. Ils s'inquiètent aussi de l'état de préparation des infrastructures critiques face à des attaques de grande ampleur.

Grâce aux données recueillies sur les mesures de sécurité mises en place par les organisations, nous avons pu établir une comparaison objective de la sécurité dans différents secteurs utilisant des infrastructures critiques et dans différents pays. Les cadres responsables de systèmes de contrôle opérationnel ou industriel ont également répondu à une série de questions spéciales sur les mesures de sécurité mises en œuvre sur ces systèmes.

Les résultats révèlent que la Chine est de loin le pays où l'on enregistre le plus haut taux d'adoption de mesures de sécurité, en ce compris le chiffrement et l'authentification forte des utilisateurs. En revanche, il apparaît que le secteur de la distribution d'eau et du traitement des eaux usées est à la traîne dans ce domaine.

L'analyse des données par secteur et par pays révèle des variations significatives en termes de perception concernant les réglementations et d'autres initiatives gouvernementales ainsi que leur impact. D'après les réponses fournies par les cadres dirigeants, c'est en Inde que le niveau de réglementation est le plus élevé, suivie de près par la Chine et l'Allemagne. En revanche, c'est aux Etats-Unis qu'il est le plus bas. Les avis quant à l'impact et à l'efficacité des réglementations divergent sensiblement, mais la plupart des cadres s'accordent à dire qu'elles contribuent à améliorer la sécurité.

La plupart des cadres dirigeants sont convaincus de l'implication de gouvernements étrangers dans des attaques réseau perpétrées contre les infrastructures critiques de leur pays. Les Etats-Unis et la Chine sont cités comme les principaux agresseurs potentiels. Néanmoins, la difficulté à attribuer clairement les responsabilités dans le cyberespace offre aux responsables la possibilité d'opposer un « démenti plausible ».

### Méthodologie

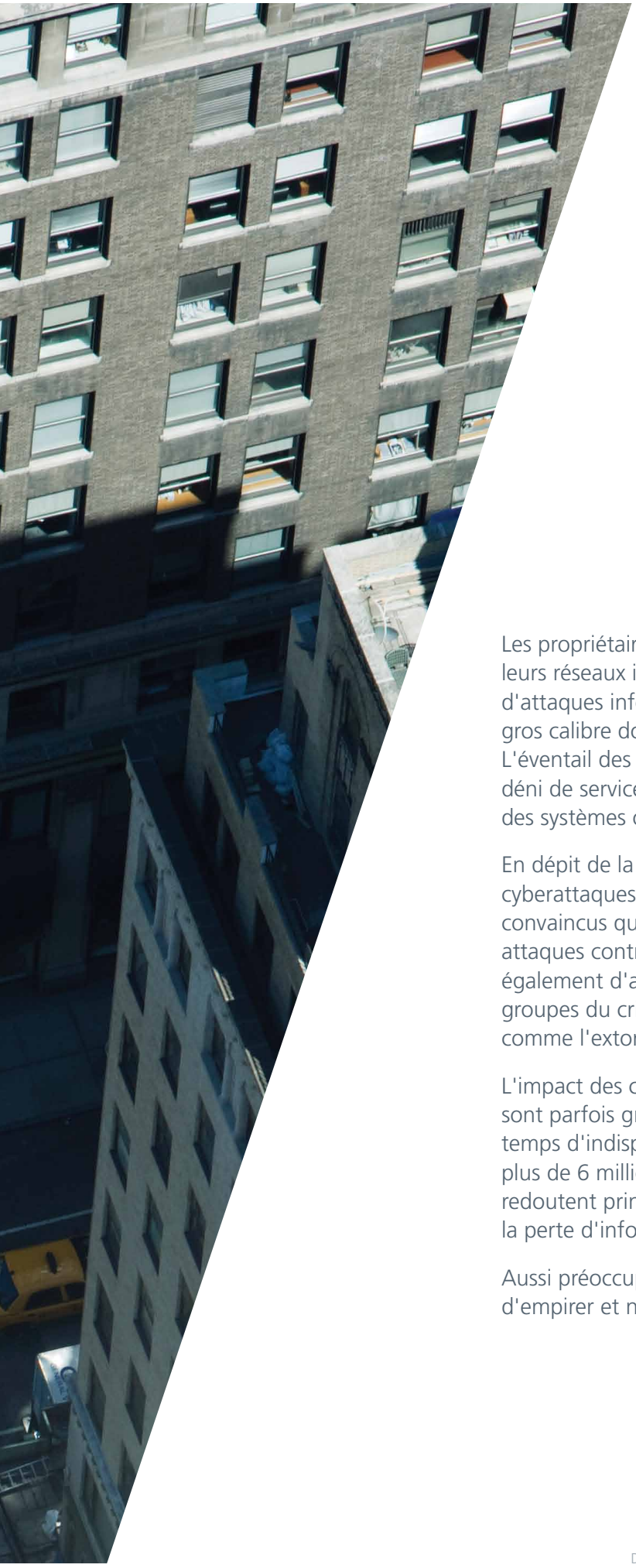
Les résultats de l'enquête recueillis pour les besoins de ce rapport permettent, pour la première fois, de brosser un tableau très complet des mesures mises en œuvre par les responsables de la sécurité des réseaux informatiques critiques pour contrer les cyberattaques, tenter de sécuriser leurs systèmes et collaborer avec les pouvoirs publics. Ce rapport a été rédigé par une équipe du programme Technology and Public Policy du CSIS (Center for Strategic and International Studies) à Washington, après une analyse des données recueillies, complétée par des études et des entretiens supplémentaires.

Les personnes interrogées sont des cadres dirigeants responsables des systèmes informatiques, de contrôle opérationnel ou de sécurité au sein de leur entreprise. La moitié d'entre eux exercent ces fonctions au niveau d'une division et un quart au niveau mondial.

L'objectif de l'enquête n'est pas tant de réaliser un sondage d'opinion basé sur des statistiques rigoureuses, des marges d'erreur et un échantillonnage précis, mais plutôt d'évaluer globalement le point de vue des cadres dirigeants et d'offrir un aperçu des différents avis d'un groupe significatif de décideurs[1].

Les entretiens menés par l'équipe du CSIS lui ont permis d'établir le contexte de l'étude, de vérifier les données recueillies et de brosser un tableau très complet des environnements réglementaires, des niveaux de menace et de vulnérabilité des sept secteurs d'activité passés à la loupe dans chaque pays ainsi que des meilleures pratiques adoptées de matière de sécurité. De nombreux cadres interrogés ont refusé de voir leur nom mentionné, certains ne voulant pas que celui-ci ou leurs propos soient cités. Les noms de ceux qui ont accepté d'être nommés figurent dans la section des remerciements.

# Une menace bien réelle



Les réseaux informatiques et les systèmes de contrôle font l'objet d'attaques informatiques répétées, souvent par des adversaires de gros calibre dotés de moyens considérables, tels des Etats étrangers.

Les propriétaires et opérateurs d'infrastructures critiques affirment que leurs réseaux informatiques et leurs systèmes de contrôle font l'objet d'attaques informatiques répétées, souvent par des adversaires de gros calibre dotés de moyens considérables, tels des Etats étrangers. L'éventail des attaques est impressionnant, qu'il s'agisse d'attaques par déni de service distribué en masse conçues pour mettre hors service des systèmes ou de tentatives furtives d'intrusion réseau.

En dépit de la difficulté à remonter à la véritable source des cyberattaques, la plupart des propriétaires et opérateurs sont convaincus que des Etats étrangers ont déjà été impliqués dans des attaques contre les infrastructures critiques de leur pays. Ils citent également d'autres types d'agresseurs, de simples vandales à des groupes du crime organisé. Les attaques à motivation lucrative comme l'extorsion et le vol de service sont répandues.

L'impact des cyberattaques est très variable mais leurs conséquences sont parfois graves, allant jusqu'à l'arrêt des opérations. Le coût des temps d'indisponibilité résultant d'attaques majeures s'élèverait à plus de 6 millions de dollars par jour. Outre le coût, les entreprises redoutent principalement le préjudice porté à la réputation, suivi de la perte d'informations personnelles sur la clientèle.

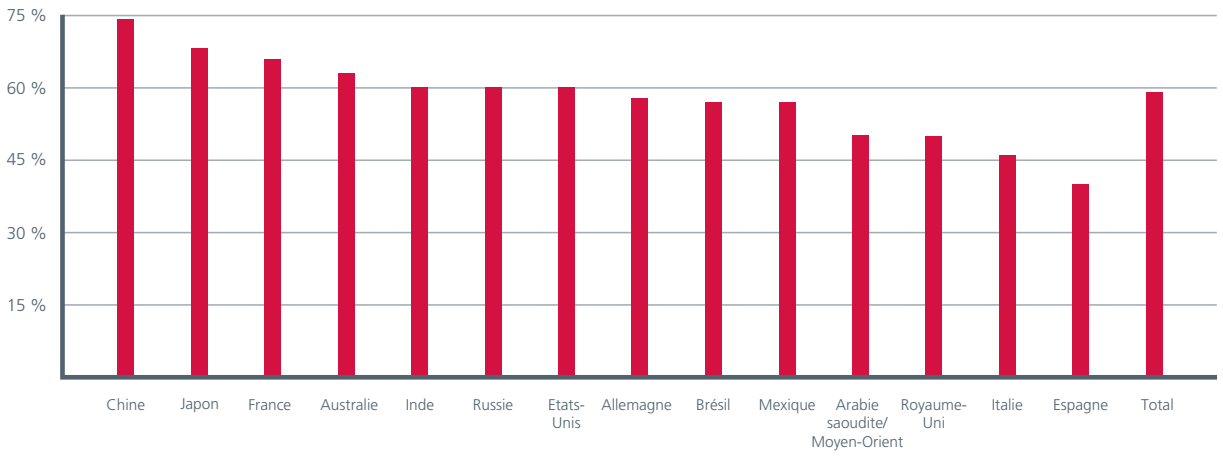
Aussi préoccupante soit-elle, la situation risque, selon les répondants, d'empirer et non de s'améliorer à l'avenir.

### Des cyberattaques graves et omniprésentes

Plus de la moitié des cadres dirigeants interrogés (54 %) déclarent avoir été confrontés à des « attaques par déni de service de grande envergure par un adversaire de haut niveau, à savoir le crime organisé, des terroristes ou un Etat (comme en Estonie et en Géorgie par exemple) ». La même proportion a été victime d'« infiltrations furtives » de leur réseau par ce type d'agresseur. GhostNet a notamment été cité : ce réseau d'espionnage de grande envergure lance des attaques de logiciels malveillants personnalisées afin de permettre aux pirates informatiques de s'introduire dans des réseaux appartenant à des organisations sans but lucratif, des agences gouvernementales ou des organismes internationaux dans des dizaines de pays, dans le but de contrôler ces réseaux et de télécharger d'importants volumes de données.

Une large majorité des répondants (59 %) est convaincue de l'implication de représentants de certains Etats étrangers dans ces infiltrations et attaques lancées contre les infrastructures critiques de leur pays.

Pourcentage de répondants convaincus que des Etats étrangers sont déjà impliqués dans des cyberattaques lancées contre les infrastructures critiques de leur pays



Une majorité des répondants est convaincue que des Etats étrangers sont déjà impliqués dans des cyberattaques lancées contre des infrastructures critiques.

En 2007, la conclusion du Rapport de criminologie virtuelle annuel de McAfee signalait que pas moins de 120 pays avaient ou étaient en train de développer une capacité offensive de cyberespionnage ou de cyberguerre. Au Royaume-Uni et en Allemagne, les autorités ont mis en garde les acteurs stratégiques du secteur privé que leurs réseaux étaient la cible d'intrusions par des services de renseignements étrangers. Aux Etats-Unis, les médias ont largement commenté les intrusions commises par des services de renseignements étrangers, souvent imputées à la Chine, visant plus particulièrement les secteurs de la défense et de l'énergie.

« L'existence d'entités étrangères menant des missions de reconnaissance (via Internet) sur notre infrastructure de transport d'électricité fait pas l'ombre d'un doute », déclare Michael Assante, directeur de la sécurité de North American Electric Reliability Corporation. « Elles cherchent vraisemblablement à grappiller des renseignements, à tenter de s'introduire (dans les réseaux informatiques) et à garder un accès constant à ceux-ci. »

**Des attaques fréquentes aux lourdes conséquences**

Près d'un tiers (29 %) des personnes interrogées déclarent avoir été victimes d'attaques par déni de service distribué à grande échelle plusieurs fois par mois et environ deux tiers d'entre elles (64 %) reconnaissent que ces attaques « ont eu un certain impact sur leurs opérations ».

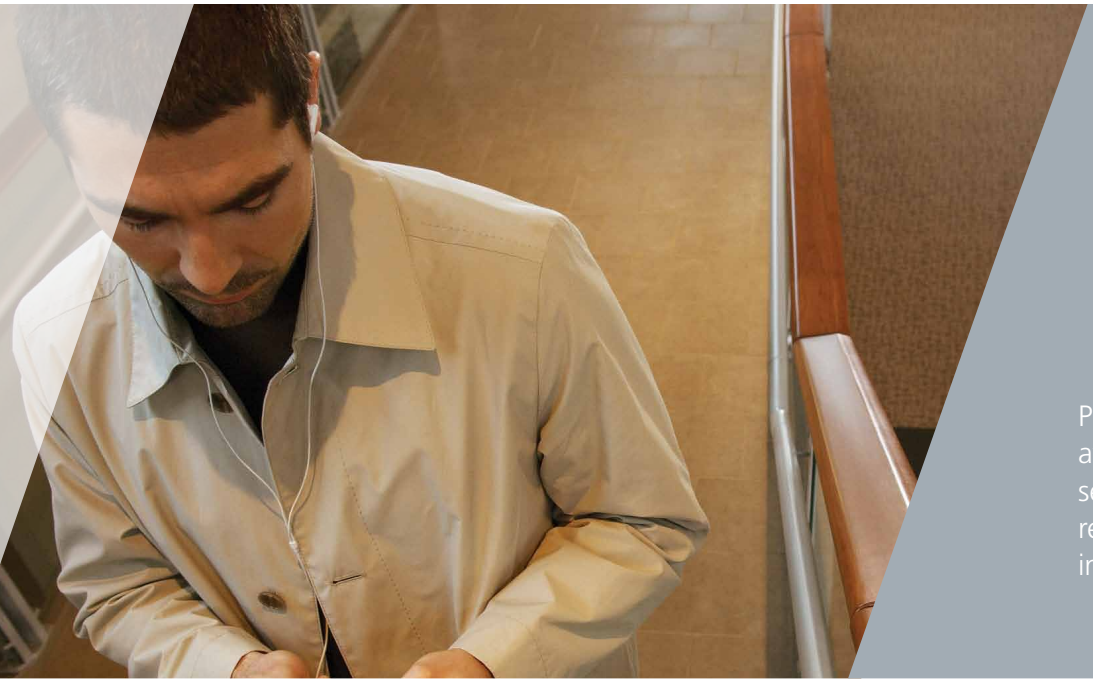
Les attaques par déni de service distribué utilisent des réseaux d'ordinateurs infectés, appartenant souvent à des individus ou des organisations ignorant que leurs systèmes avaient été compromis, afin de bombarder les réseaux de millions de fausses demandes d'informations via Internet. Les attaques de ce type sont menées par des réseaux de robots (botnets), c'est-à-dire des ordinateurs infectés par des logiciels malveillants (malwares) spécialement écrits à cette fin.

Dans l'environnement réseau d'aujourd'hui, les attaques par déni de service distribué sont techniquement plus faciles à détecter et à réprimer, notamment grâce à des services visant à minimiser les risques que les fournisseurs d'accès Internet (FAI) proposent à leurs clients, pour autant qu'ils en paient le prix.

« En général, en tant que fournisseurs d'accès Internet, nous partons du principe que nous sommes sont simplement chargés d'acheminer le trafic », déclare Adam Rice, directeur de la sécurité de Tata Communications, le plus important fournisseur de services Internet clé en main au monde. « Si vous êtes abonné au service (de réduction des risques), nous supprimerons la menace (d'attaque par déni de service distribué) avant qu'elle ne vous atteigne mais sans cela, les fournisseurs ont tendance à laisser passer. »

Selon Adam Rice, une action concertée de la part des « fournisseurs de niveau un », ceux qui détiennent et exploitent les dorsales Internet au niveau mondial, permettrait de mettre en place les mesures techniques nécessaires pour minimiser de telles attaques.

Comme l'ont fait remarquer d'autres experts, la difficulté réside dans le fait que la réduction de la menace pourrait être compliquée par des questions d'ordre réglementaire ou contractuel, à moins que la loi n'accorde une exclusion de responsabilité aux sociétés qui intercepteraient et détourneraient le trafic de déni de service distribué. Par ailleurs, les fournisseurs actifs sur plusieurs marchés nationaux peuvent être confrontés à des obligations légales différentes, parfois contradictoires, selon les juridictions.



Près de deux tiers des entreprises ayant subi des attaques par déni de service distribué de grande envergure reconnaissent que celles-ci ont eu un impact sur leurs opérations.

### Des agresseurs de l'ombre

Les instructions d'attaques diffusées aux réseaux de robots proviennent généralement d'ordinateurs infectés appartenant également à des tiers innocents, les véritables auteurs usant de fausses pistes et d'esquives pour dissimuler leurs traces. De plus, il est très facile de louer des réseaux de robots à des gangs de pirates. Remonter à la source de ces attaques par déni de service distribué relève par conséquent du tour de force. D'ailleurs, la véritable identité des auteurs des attaques lancées contre la Géorgie et l'Estonie reste sujette à controverse.

« Savoir la vérité et être en mesure d'en fournir la preuve sont deux choses très différentes », a déclaré un ancien représentant des forces de l'ordre américaines. « Même si vous parvenez à retrouver la machine responsable, vous n'en saurez pas plus sur l'identité de celui qui s'en est servi. »

Ce constat vaut également pour les infiltrations furtives des réseaux. Dans l'affaire GhostNet, des chercheurs ont trouvé des logiciels espions (spywares) conçus pour voler des mots de passe, des informations de connexion et des documents confidentiels sur des réseaux informatiques appartenant au bureau du chef spirituel tibétain, le dalaï-lama, une intrusion dont ils estiment le gouvernement chinois responsable. Cette accusation n'était pas uniquement fondée sur des éléments techniques mais aussi sur le fait que les données dérobées dans les réseaux compromis ont été exploitées par la suite par les autorités chinoises.

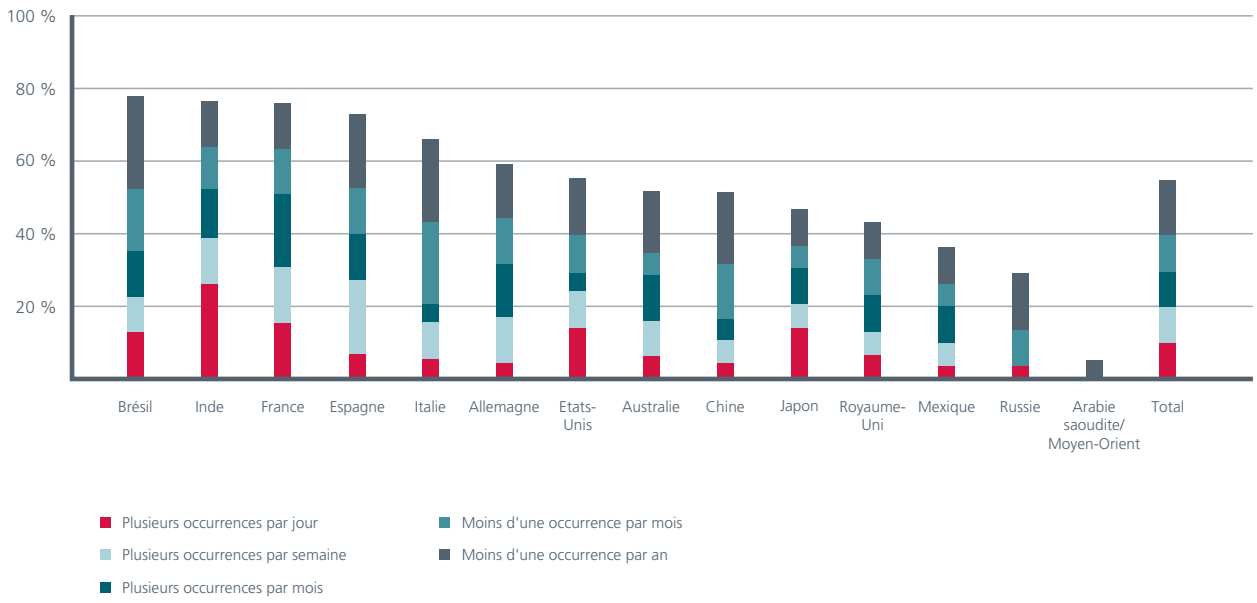
Compte tenu des difficultés à identifier les véritables auteurs des cyberattaques, les Etats agresseurs continuent d'abuser des avantages stratégiques du principe de « démenti plausible ». Toutefois, pour les responsables de la protection des réseaux critiques, les cyberconflits évoquent le concept hobbesien de la « guerre de tous contre tous ».

### Attaques par déni de service distribué : leur grande fréquence n'en fait pas pour autant le principal problème de sécurité

La forme d'attaque la plus répandue est l'infection par un ver ou un logiciel malveillant, à laquelle 89 % des personnes interrogées ont été confrontées. Plus de 70 % d'entre elles déclarent avoir été victimes d'autres types d'attaques, notamment des actes de vandalisme et des attaques par déni de service distribué de faible ampleur, des menaces émanant de membres du personnel, des vols ou fuites de données sensibles ainsi que des attaques par phishing ou pharming.

Les attaques évoluées sur le plan technique sont plus rares, même si elles restent plus répandues que les attaques par déni de service distribué à grande échelle. Plus de la moitié (57 %) des cadres informatiques signalent des attaques par empoisonnement du cache DNS (redirection du trafic web), et pour près de 50 % d'entre eux, celles-ci ont eu lieu plusieurs fois par mois. Un nombre similaire de répondants a été confronté à des attaques par injection de code SQL, qui permettent aux pirates d'accéder aux données du système central via un site web public. Dans ce cas-ci aussi, la moitié a subi plusieurs attaques par mois. Les attaques de ce type ont généralement un impact opérationnel plus important sur les systèmes compromis.

Pourcentage de répondants faisant état d'attaques par déni de service distribué de grande envergure et fréquence de ces attaques




### Généralisation du vol et des attaques à but lucratif

60 % des personnes interrogées ont été confrontées à des vols de service, près de 20 % plusieurs fois par mois. Les cas sont plus nombreux dans le secteur du pétrole/gaz, où trois quarts des répondants signalent ce type d'attaque. Ce secteur enregistre également le taux d'infiltrations furtives le plus élevé (71 % contre 54 % des répondants tous secteurs confondus), un tiers faisant état de plusieurs infiltrations par mois.

Notons toutefois que les variations des taux de victimes sont plus fortes entre les pays qu'entre les secteurs, ce qui laisse penser que les facteurs nationaux sont plus significatifs que les considérations sectorielles dans la détermination des taux d'attaques.

### Certains pays plus attaqués que d'autres

Plus de la moitié des cadres dirigeants indiens et français déclarent avoir été confrontés plusieurs fois par mois à des attaques par déni de service distribué de grande envergure. L'Espagne et le Brésil enregistrent également des taux de victimes élevés[2].

« Les attaques par déni de service distribué sont très courantes au Brésil, tout comme dans d'autres pays », affirme Anchises De Paula, analyste d'iDefense Labs basé au Brésil. Il ajoute que les fournisseurs d'accès Internet commençaient à mieux les gérer.

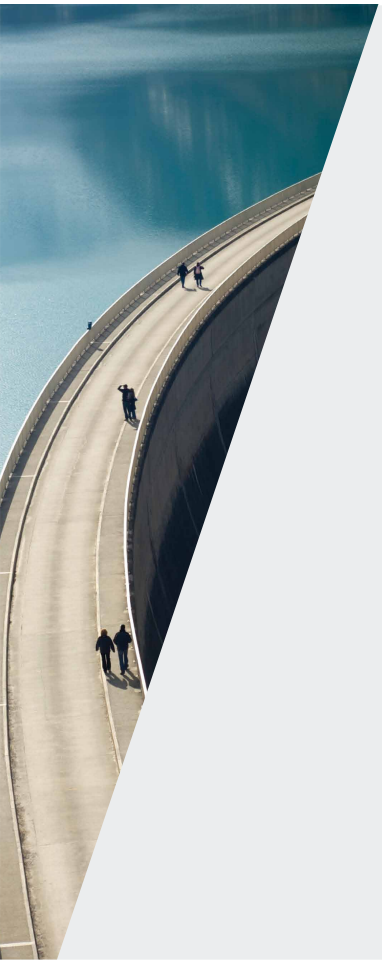
« Les attaques par déni de service distribué connaissent une popularité grandissante en raison de leur coût décroissant et de leur simplicité », fait remarquer Adam Rice. « Il suffit de quelques heures et d'une carte de crédit pour louer un réseau de robots et monter l'attaque. »

### Aucun secteur n'échappe aux attaques par déni de service distribué

En ce qui concerne les attaques par déni de service distribué à grande échelle, les variations sectorielles sont bien moins importantes qu'entre les pays, peut-être du fait que les facteurs nationaux influent davantage que les facteurs sectoriels sur les taux de victimes. Le secteur pétrolier et gazier est le plus touché, deux tiers des cadres dirigeants ayant été confrontés à de telles attaques et, pour un tiers, plusieurs fois par mois. Les moins frappés sont celui de la distribution d'eau et du traitement des eaux usées (43 % des répondants) ainsi que celui du transport (50 %).

### Des attaques au contrecoup sévère et variable selon les secteurs

Près de deux tiers des entreprises ayant subi des attaques par déni de service distribué de grande envergure reconnaissent qu'elles ont eu un impact sur leurs opérations. Celles-ci ne se contentent pas de bloquer l'accès à des sites web publics, elles perturbent également le fonctionnement de la messagerie électronique et des systèmes de téléphonie Internet, ainsi que d'autres fonctions opérationnelles essentielles.



### Le Web, un réseau d'extorsion

Un opérateur ou propriétaire d'infrastructures critiques sur cinq indique avoir été victime d'une tentative d'extorsion à la suite d'une cyberattaque ou d'une menace de cyberattaque au cours des deux dernières années. Aussi surprenante soit-elle, cette constatation concorde avec les témoignages des experts de plusieurs pays et secteurs. Pour certains, le chiffre réel est même probablement plus élevé. Selon eux, la plupart de ces affaires ne sont pas médiatisées, ni même divulguées, en raison du préjudice possible pour la réputation et d'autres craintes de la société victime.

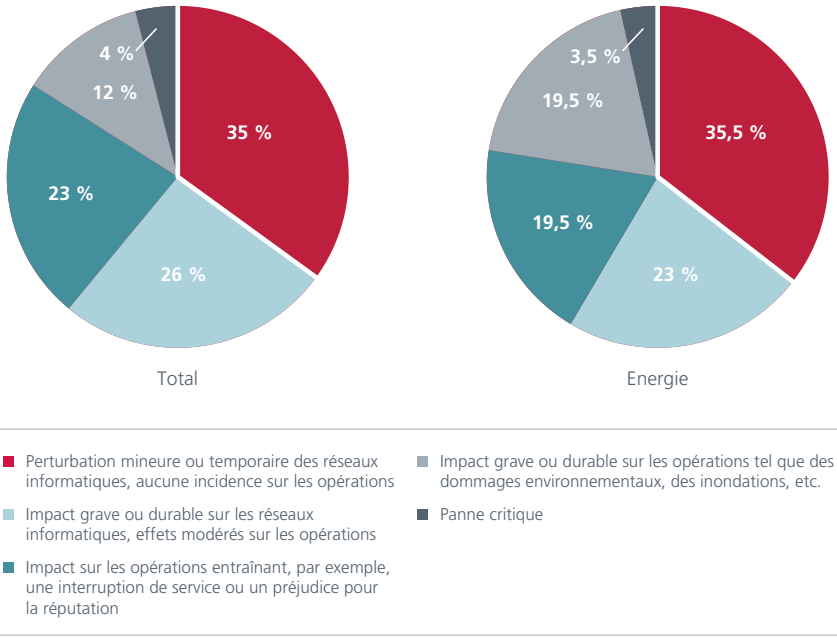
Les victimes les plus nombreuses sont à déplorer dans les secteurs de l'énergie (27 %) et du pétrole/gaz (31 %).

« L'extorsion est, selon moi, un phénomène très préoccupant lorsqu'elle vise l'interruption de systèmes d'alimentation électrique », déclare Michael Assante. Il estime que les tentatives d'extorsion réalisées dans le cadre d'attaques visant les réseaux d'entreprise peuvent être qualifiées de « mineures » en cela qu'elles présentent « un risque limité d'exposition pour l'extorqueur mais n'entraînent pas de pertes très importantes ». En revanche, les attaques lancées contre les infrastructures sont beaucoup plus sérieuses. « Lorsqu'on parle de couper l'électricité à toute une zone, la situation est entièrement différente. Le risque est, certes, plus grand pour l'extorqueur mais le préjudice financier sera bien plus conséquent. » En novembre 2009, les médias américains faisaient état de deux pannes de courant majeures au Brésil, en 2005 et 2007, attribuables à des pirates informatiques, sans doute dans le cadre d'une tentative d'extorsion de fonds.

En septembre 2009, Mario Azer, consultant en informatique pour la compagnie d'exploration pétrolière et gazière Pacific Energy Resources, basée à Long Beach en Californie, a reconnu avoir manipulé des systèmes informatiques à la suite du différend qui l'a opposé à la société concernant un paiement et un emploi futur. Il a modifié un logiciel de contrôle industriel spécialisé SCADA (Supervisory Control And Data Acquisition, télésurveillance et acquisition de données), conçu dans ce cas précis pour avertir les opérateurs en cas de fuites ou autres dommages causés aux pipelines sous-marins de plusieurs kilomètres reliant les derricks de la société au rivage.

Même si le secteur de la distribution d'eau et du traitement des eaux usées affiche un faible taux de victimes de tentatives d'extorsion (17 %), l'impact potentiel de ces menaces y est vivement ressenti.

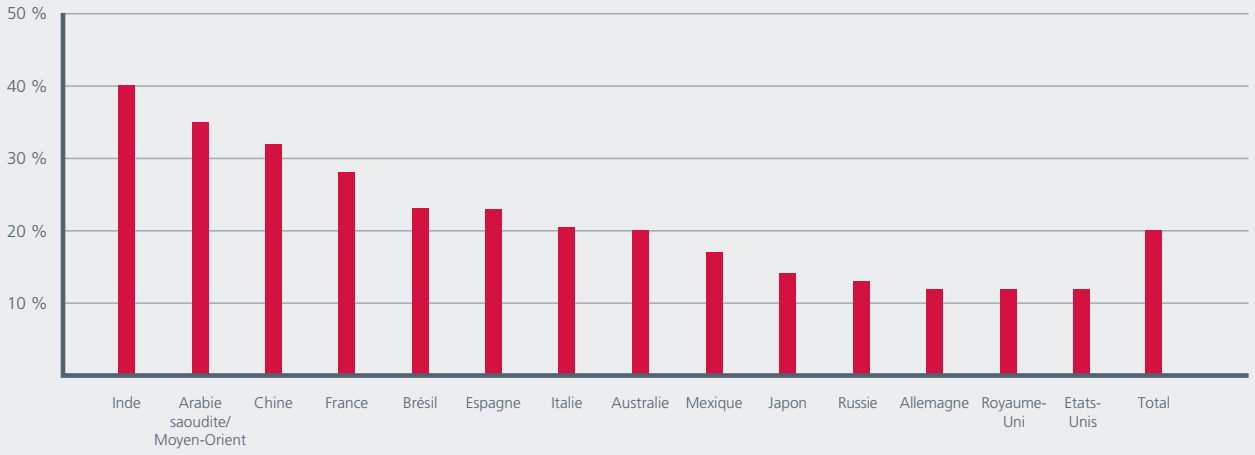
Impacts des attaques par déni de service distribué à grande échelle



« La majorité de la population américaine et la plupart de ses dirigeants considèrent l'accès à l'eau potable comme un acquis, voire un droit, depuis plus d'un siècle », déclare Aaron Levy de l'AMWA (Association of Metropolitan Water Agencies). « Une perte de confiance dans l'approvisionnement en eau potable pourrait, d'après des études, provoquer le chaos » dans les grandes villes et d'autres centres de population.

D'après notre étude, les manœuvres d'extorsion sont très répandues en Inde, en Arabie saoudite et au Moyen-Orient, en Chine et en France. Elles sont très rares aux Etats-Unis et au Royaume-Uni.

Pourcentage de répondants faisant état de tentatives d'extorsion au moyen d'une (menace d')attaque réseau au cours des deux dernières années




Près d'un cadre sur six estime que les attaques par déni de service distribué à grande échelle ont un impact « grave ou durable sur les opérations » ou qu'elles entraînent « une panne ou une défaillance critiques ».

Leurs répercussions sont particulièrement sérieuses pour les secteurs de l'énergie/électricité et de la distribution d'eau/du traitement des eaux usées.

Parmi les autres attaques à fort impact opérationnel, citons les infiltrations furtives de réseaux, les pertes ou fuites de données sensibles, l'empoisonnement du cache DNS et les injections de code SQL. Pour plus de 60 % des victimes, toutes ont une incidence sur le fonctionnement de l'entreprise. En ce qui concerne les pertes et les fuites de données sensibles, 15 % des répondants jugent leur impact grave et 4 %, critique.

D'après les cadres dirigeants interrogés, les conséquences indésirables des cyberattaques ne se limitent pas là. La plus redoutée est le préjudice porté à la réputation, suivi par la perte d'informations personnelles sur la clientèle. Il s'agit des deux préoccupations majeures dans le secteur bancaire.

**Principal mobile : l'argent, toujours l'argent**

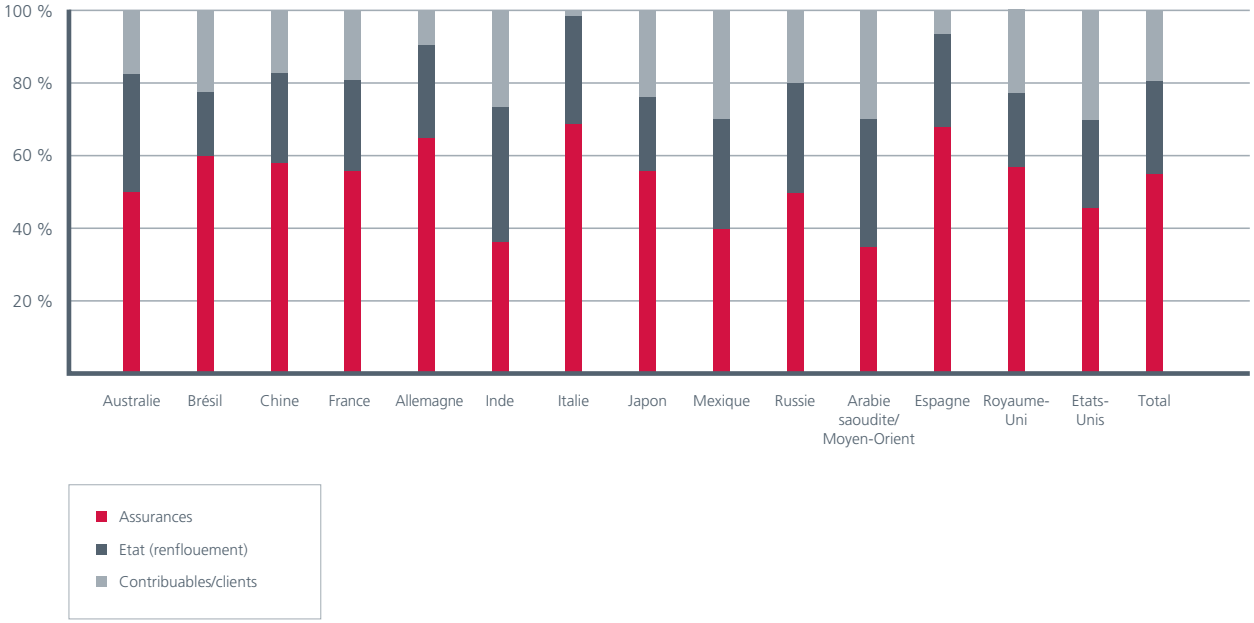
A la question concernant la cible la plus courante des cyberattaques, plus de la moitié des répondants (56 %) cite les données financières. Les informations de connexion et les mots de passe seraient les moins visés (21 % des attaques).

En revanche, dans les secteurs de l'énergie/électricité et du pétrole/gaz, ce sont les systèmes de contrôle opérationnel informatisés, tels que SCADA, qui sont le plus souvent attaqués (respectivement 55 et 56 % des cas dans ces deux secteurs).

**Les systèmes de contrôle opérationnel en butte aux assauts**

Les attaques menées contre les systèmes SCADA sont particulièrement graves car elles permettent aux pirates de contrôler directement les systèmes opérationnels, ce qui peut déboucher sur des pannes de courant à grande échelle ou des catastrophes écologiques d'origine humaine. (Voir page 22.)

Qui paiera la facture en cas d'incident de cybersécurité majeur dans votre secteur ?




En 2007, la chaîne CNN a diffusé une vidéo d'un test réalisé par des scientifiques de l'Idaho National Laboratory, au cours duquel un générateur électrique connecté à un système SCADA s'est pratiquement désintégré après avoir reçu des instructions piratées. La vidéo a permis d'illustrer de façon frappante les failles du système SCADA aux Etats-Unis et conduit à l'ouverture d'un débat au Congrès américain sur la cybersécurité du réseau de distribution électrique.

### Les coûts exorbitants des cyberattaques de grande envergure

Les données de l'enquête donnent à penser que les coûts d'un arrêt associé à un incident de sécurité majeur (occasionnant par exemple une indisponibilité critique de services pendant au moins 24 heures, des blessures ou pertes en vies humaines ou la faillite d'une société) pourraient être très élevés.

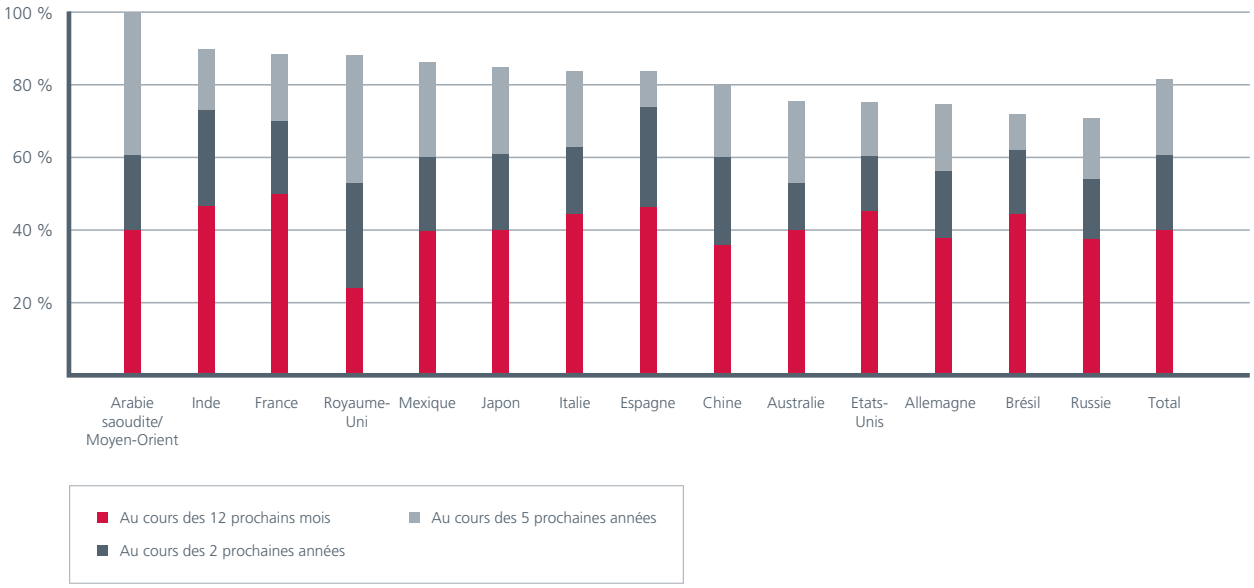
En moyenne, les répondants estiment qu'une interruption des activités pendant 24 heures à la suite d'une attaque majeure coûterait à leur entreprise 6,3 millions de dollars. C'est dans le secteur du pétrole/gaz que ce coût est le plus élevé, à savoir 8,4 millions de dollars en moyenne, et dans le secteur public ainsi que dans le secteur de la distribution d'eau et du traitement des eaux usées qu'il est le plus faible.

### Qui paiera la facture ?

A la question de savoir qui supportera les coûts d'une attaque informatique majeure, les réponses et les attentes varient considérablement. Plus de la moitié des répondants considèrent que ces coûts doivent être pris en charge par les assurances, près de 20 % d'entre eux, par le contribuable ou le client, et un peu plus du quart, par l'Etat. Les assurances ont été citées le plus souvent par les cadres dirigeants italiens, espagnols et allemands, et le moins souvent par les Indiens et les Saoudiens.

Les répondants du secteur de la distribution d'eau et du traitement des eaux usées sont pratiquement deux fois plus nombreux à penser que le coût doit être supporté par le client (35 % contre 19 % du total des répondants). Lorsque le secteur de la distribution d'eau affiche, comme ici, un tel écart par rapport à la moyenne, il faut se souvenir que son échantillon est très restreint. Toutefois, le pourcentage de cadres interrogés étant d'avis que la facture doit aller au client est également élevé dans les secteurs du transport (24 %) et des télécommunications (23 %). C'est dans le secteur du pétrole/gaz qu'il est le plus faible (12 %).

Quand vous attendez-vous à voir un incident de cybersécurité majeur affecter les infrastructures critiques de votre pays ?




Le coût moyen estimé d'une interruption des activités pendant 24 heures à la suite d'une attaque majeure s'élève à 6,3 millions de dollars.

De telles attentes s'avèreront peut-être optimistes. Comme l'a avancé un expert, elles risquent de changer à l'avenir dans la mesure où les entreprises vont tenter de limiter leur responsabilité face à la hausse du coût des cyberattaques.

« En Australie, (le consommateur) a eu de la chance jusqu'à présent étant donné que le problème ne le concernait pas », déclare Ajoy Ghosh, un cadre en sécurité de Logica, basé à Sydney. « Un particulier qui est victime d'une attaque par phishing (...) sait que la banque va le rembourser… Selon moi, la tendance risque un jour de s'inverser et ce sera à lui d'en assumer la responsabilité. »

Ajoy Ghosh, chargé de cours sur la cybercriminalité à l'University of Technology of Sydney, pense que les sociétés vont chercher à limiter leur responsabilité et que « le seul moyen d'y parvenir est de se décharger de cette responsabilité sur quelqu'un d'autre ; dans certains cas, ce quelqu'un sera l'Etat, dans d'autres l'assureur, mais selon moi, dans la grande majorité des cas, ce sera le consommateur ».

**Un risque de cyberattaques en hausse**

Loin de s'améliorer, la situation risque, au contraire, d'empirer. Les répondants sont presque deux fois plus nombreux à penser que la vulnérabilité de leur secteur aux cyberattaques a augmenté au cours de l'année écoulée plutôt qu'elle n'a diminué (37 % contre 21 %).

Fait significatif, deux cinquièmes des cadres informatiques s'attendent à un incident de cybersécurité majeur (avec interruption des activités de « 24 heures minimum, perte de vies humaines ou (...) faillite d'une société ») dans leur secteur au cours de l'année à venir. 80 % escomptent un incident de ce type au cours des cinq prochaines années. Ce pessimisme est particulièrement marqué dans les pays qui ont déjà été confrontés aux attaques les plus graves.

# Ressources et préparation face à la menace

Les compressions du personnel de sécurité engendrées par la conjoncture économique actuelle sont monnaie courante. Justifier commercialement la cybersécurité reste difficile.

La plupart des cadres informatiques estiment que leurs ressources de protection réseau sont suffisantes même si leur niveau de satisfaction diffère d'un pays à un autre. Toutefois, les compressions de ce personnel engendrées par la conjoncture économique actuelle sont également monnaie courante. Justifier commercialement la cybersécurité reste un défi.

Si les répondants sont généralement confiants dans leurs ressources, ils le sont moins en ce qui concerne leur niveau de préparation. Environ un tiers des personnes interrogées déclarent que leur secteur n'est pas suffisamment armé pour gérer des attaques majeures ou des infiltrations perpétrées par des adversaires de haut niveau. Ce manque de confiance est particulièrement marqué chez les Européens, qui doutent dans la capacité de leurs infrastructures bancaires à fonctionner en cas de cyberattaque majeure.

### Des ressources généralement jugées adéquates

D'une manière générale, les cadres informatiques estiment disposer des ressources appropriées pour protéger les réseaux informatiques de leur société. Près de deux tiers déclarent que ces ressources sont « parfaitement » ou « globalement » suffisantes. Un peu plus d'un tiers seulement pense qu'elles sont « insuffisantes » ou « relativement suffisantes ».

### Des pays et secteurs moins satisfaits que d'autres

Les cadres les moins satisfaits de leurs ressources proviennent d'Italie, du Japon et d'Arabie saoudite. Les plus satisfaits sont les Allemands, les Britanniques et les Australiens. Les niveaux de satisfaction sont globalement les plus élevés dans le secteur bancaire et les plus faibles dans le secteur du transport/transport en commun.

### La récession à l'origine de restrictions de ressources généralisées, parfois sévères

Deux tiers des cadres informatiques reconnaissent que la récession a entraîné des coupes dans le personnel en charge de la sécurité.

Un quart d'entre eux a vu ses ressources diminuer de 15 % ou plus. Les secteurs du pétrole/gaz et de l'énergie sont les plus concernés par ces réductions (trois quarts des répondants). En ce qui concerne les pays, ce sont l'Inde, l'Espagne, la France et le Mexique qui sont les plus touchés, et l'Australie la moins touchée.

### La sécurité joue un rôle déterminant dans les décisions d'investissement

La sécurité reste la priorité dans les décisions relatives aux stratégies et aux investissements informatiques, même en temps de crise. 92 % des répondants estiment que la sécurité est un facteur « crucial » ou « très important » lors des choix en matière de stratégies ou d'investissements informatiques. Pratiquement le même pourcentage (91 %) partage cette opinion concernant la fiabilité. Les deux autres critères suggérés, en l'occurrence l'efficacité et la disponibilité, sont considérés comme cruciaux ou très importants par trois quarts des cadres dirigeants.

Les cadres dirigeants chinois et américains sont les plus nombreux à juger la sécurité comme un critère de décision « crucial ».

### La justification commerciale de la cybersécurité passe par un rééquilibrage des priorités

En règle générale, le coût est considéré comme « le principal obstacle à la sécurisation des réseaux critiques », suivi de « l'absence de perception de l'ampleur du risque ».

Dans les secteurs de la distribution d'eau/du traitement des eaux usées et du pétrole/gaz, ce classement est inversé, l'absence de perception du risque étant généralement citée avant le coût. Des spécialistes en sécurité de plusieurs secteurs estiment qu'il est toujours difficile de justifier commercialement un investissement en cybersécurité dans la mesure où il est fréquent que la direction ne mesure pas l'ampleur de la menace ou la nécessité d'une solution.

« Le premier obstacle est, selon moi, l'incapacité des responsables de la sécurité à attirer l'attention sur l'urgence du problème et à persuader les décideurs que la menace est bien concrète », déclare un expert en sécurité. Il ajoute que cette situation est en partie due au fait que la sécurité n'est pas encore devenue un élément différenciateur clé sur le marché pour les secteurs critiques.

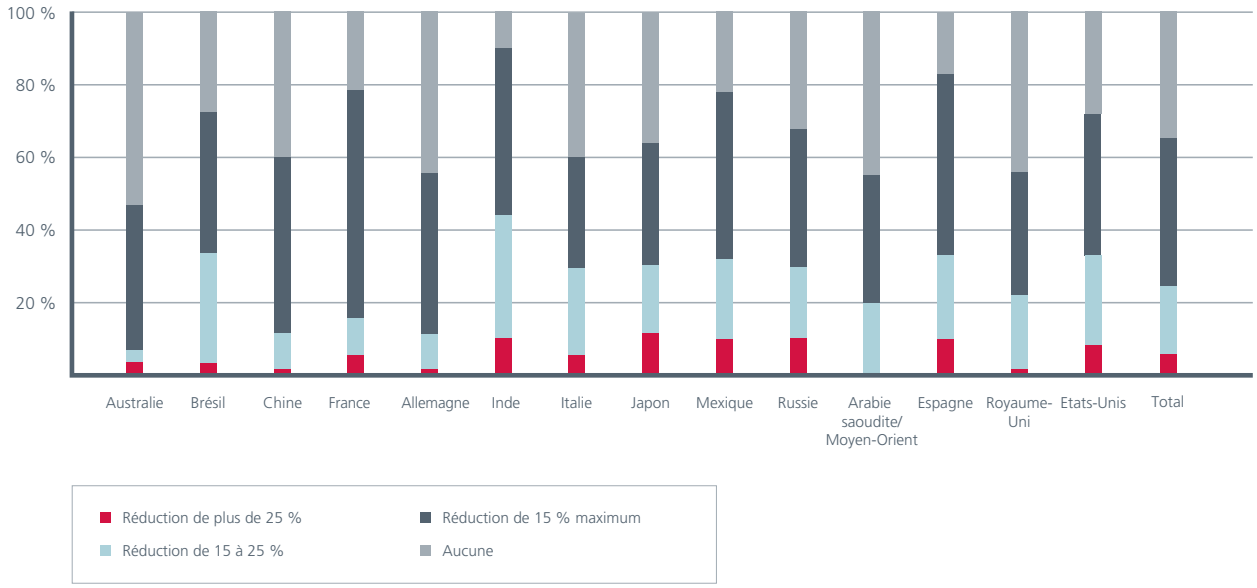
Les experts s'accordent à dire que les attaques terroristes du 11 septembre ont contribué à une meilleure conscientisation aux problèmes de cybersécurité aux Etats-Unis et ailleurs et qu'elles ont incité les Etats à renforcer leurs infrastructures critiques. Mais ils sont également d'avis qu'il reste encore beaucoup de chemin à parcourir...

« La prise en compte de la cybersécurité est une notion relativement récente pour les directeurs de services d'utilité publique et leurs responsables de la sécurité », déclare Aaron Levy de l'Association of Metropolitan Water Agencies. « Tout le monde s'efforce actuellement de combler le retard », ajoute un spécialiste du secteur des transports.

Malheureusement, c'est en forgeant qu'on devient forgeron. En d'autres termes, il faut souvent une attaque sérieuse pour convaincre la direction de la réalité de la menace et de la nécessité de s'en protéger. « Les sociétés bien organisées sur le plan de la cybersécurité sont généralement celles qui ont été confrontées à un problème grave dans le passé », affirme ce spécialiste.

Cela dit, le responsable de la sécurité d'un des plus grands fournisseurs d'accès Internet et de télécommunications nous a confié que les clients commençaient à accorder davantage d'attention à

Réductions des ressources en sécurité provoquées par la récession




la sécurité et à la considérer comme un facteur de différenciation sur le marché. « C'est aujourd'hui le client qui décide », déclare Adam Rice de la société Tata Communications. « La sécurité n'est plus la dernière chose dont on se souvient au moment de signer le contrat. Elle passe au premier plan... elle est désormais une nécessité absolue pour tous les clients. Ils nous appellent, posent des questions pointues, veulent visiter les centres de données et avoir le droit de s'y rendre sans prévenir... Ils nous font part de leurs exigences et nous sommes tenus de les satisfaire. »

En dépit de tout cela, justifier un investissement en cybersécurité d'un point de vue commercial reste un défi. « Personne ne veut payer tant qu'il n'y a pas péril en la demeure », indique Adam Rice. « Pour le directeur de la sécurité, le meilleur moyen de démontrer l'utilité de la solution au reste de la direction est d'apporter la preuve (...) du préjudice que peuvent causer les problèmes de sécurité en termes de revenus (...) et de démontrer comment un euro dépensé aujourd'hui peut faire gagner à la société des millions demain. »

Tout dépend de la position du responsable de la sécurité dans l'organisation. « Si le directeur de la sécurité ne rend pas directement compte au PDG, l'information ne remontera probablement pas jusqu'à ce dernier. »

Plus de trois quarts (77 %) des cadres dirigeants en informatique et en sécurité interrogés déclarent que leur société possède un directeur de la sécurité informatique. Près de la moitié (46 %) indiquent que ce directeur dépend directement du PDG.

Selon plusieurs experts, les autorités pourraient avoir un rôle à jouer en proposant des mesures incitatives ou avantages de nature à renforcer la sécurité. Bien que les effets de la réglementation soient complexes (ce point est abordé plus en détail au chapitre 4), certains envisagent d'autres types d'actions gouvernementales susceptibles de favoriser une politique incitative en matière de sécurité.

Selon Michael Hayden, général à la retraite, « le cyberespace pourrait s'apparenter à un tabouret à trois pieds représentant respectivement la convivialité, la sécurité et la confidentialité (…) et à ce jour, toute notre créativité s'est concentrée sur la convivialité ».

« Comme pour n'importe quel tabouret de ce type, s'il manque un pied, tout ce qu'il vous reste, c'est du bois de chauffage », déclare-t-il, ajoutant qu'il fallait rééquilibrer la priorité donnée à la convivialité par rapport aux deux autres critères.

### Une confiance variable dans l'état de préparation

Environ un tiers des cadres informatiques interrogés déclarent que leur secteur n'est « pas préparé du tout » ou « pas très préparé » à faire face aux attaques ou infiltrations perpétrées par des adversaires aux capacités évoluées. Parmi ceux qui ont été confrontés à de telles situations, ce pourcentage atteint 41 %.

Il existe toutefois des différences notables d'un pays à l'autre. En Arabie saoudite, la très grande majorité des répondants (90 %) pense que le secteur n'est pas préparé (« pas du tout préparé » ou « pas très préparé »). Dans la plupart des pays, ceux qui ont été confrontés à des attaques évoluées sont généralement plus pessimistes quant au niveau de préparation de leur secteur (68 % des Indiens et 75 % des Mexicains).

Les pays où le taux de confiance quant à la préparation aux attaques de grande envergure est le plus élevé sont l'Allemagne (78 %) et le Royaume-Uni (64 %).

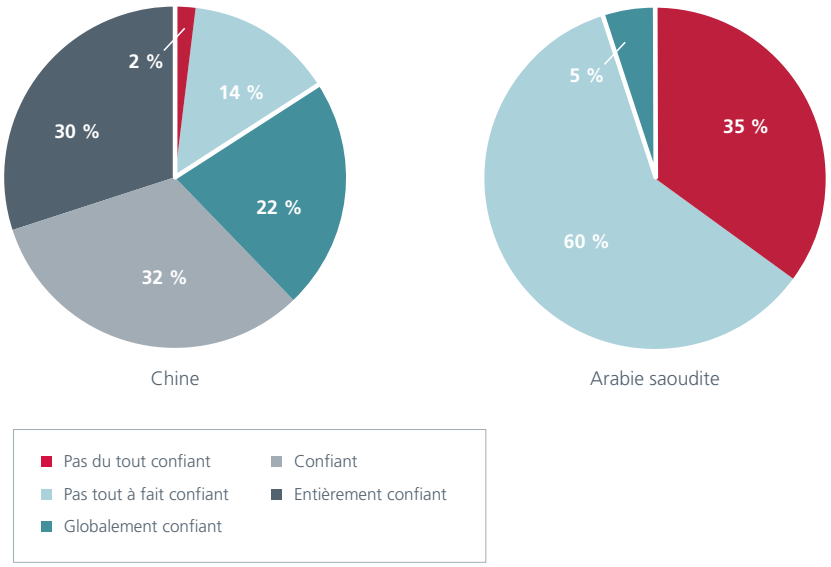
A l'exception des attaques par déni de service distribué de grande envergure, les cadres dirigeants jugent généralement leur secteur mieux préparé contre les autres formes d'attaques, un quart d'entre eux seulement estimant que leur secteur n'y est pas préparé.

Face à l'éventail global des menaces, les Américains, les Britanniques et les Australiens classent systématiquement leurs secteurs parmi les mieux armés face aux attaques. Tous ces pays possèdent des programmes de soutien gouvernemental reconnus à l'intention des propriétaires et opérateurs d'infrastructures critiques.

### Les systèmes bancaires et téléphoniques sur la sellette en cas d'attaque

Les cadres informatiques doutent également de la capacité de leurs propres fournisseurs d'infrastructures critiques à garantir un service fiable lors d'une attaque informatique majeure. A cet égard, les banques ou autres fournisseurs de services financiers sont citées par 30 % d'entre eux, et les opérateurs de télécommunications, par 31 %. C'est en Europe que la confiance dans la résilience du système bancaire est la moins grande, et plus particulièrement en Italie, en France et en Espagne.

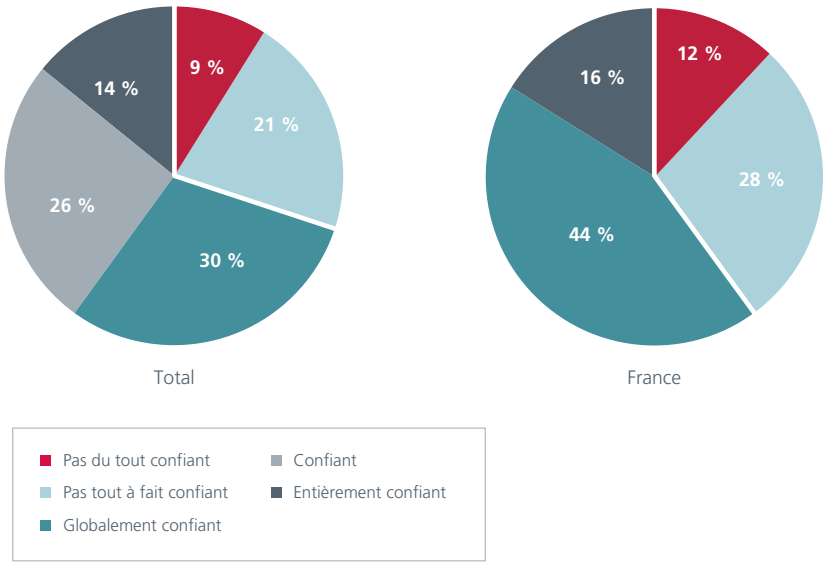
Niveau de confiance dans la continuité des services publics en cas de cyberattaque majeure




Au cours des attaques par déni de service distribué lancées contre l'Estonie en 2007, les sites web de nombreuses banques du pays ont été mis hors service, même si celles-ci ont déclaré par la suite que leurs systèmes opérationnels n'avaient pas été compromis. Des spécialistes en sécurité de différents secteurs et pays reconnaissent que les services bancaires et financiers présentent généralement les niveaux de sécurité les plus élevés. Ce secteur est également confronté à la « loi de Sutton », qui doit son nom à un célèbre braqueur de banque. Interrogé sur les raisons qui le poussaient à attaquer les banques, Willie Sutton aurait répondu « parce que c'est là qu'est l'argent ». Selon ce principe, ce secteur attisera toujours la convoitise des auteurs d'attaques informatiques motivés par l'appât du gain.

Les services publics bénéficient d'une meilleure confiance que la plupart des autres secteurs. Pourtant, seuls 37 % des répondants pensent que leurs pouvoirs publics seraient à même d'assurer leurs services en cas de cyberattaque majeure. C'est en Arabie saoudite que cette confiance est la plus faible et en Chine qu'elle est la plus élevée.

Niveau de confiance dans la continuité des services bancaires et financiers en cas de cyberattaque majeure



# Mesures de sécurité mises en place pour contrer la menace

## Adoption peu généralisée de certaines mesures de sécurité clés

Les cadres dirigeants en informatique et en sécurité ont répondu à une série de questions détaillées sur une vingtaine de mesures de sécurité différentes (technologies, stratégies et procédures) ainsi que sur leurs types d'utilisation.

Les cadres responsables des systèmes SCADA ou ICS (Industrial Control System) de leur organisation ont également répondu à des questions similaires sur les mesures de sécurité mises en œuvre sur ces réseaux. Les données recueillies à propos des systèmes SCADA/ICS, bien qu'elles portent sur un plus petit échantillon, sont saisissantes. Plus de trois quarts des responsables de ces systèmes déclarent que ceux-ci sont connectés à Internet ou à un autre réseau IP et près de la moitié d'entre eux admettent que cette situation crée un « problème de sécurité non résolu ».

Les autres réponses, prises individuellement, montrent que certaines mesures de sécurité élémentaires sont loin d'être en place.

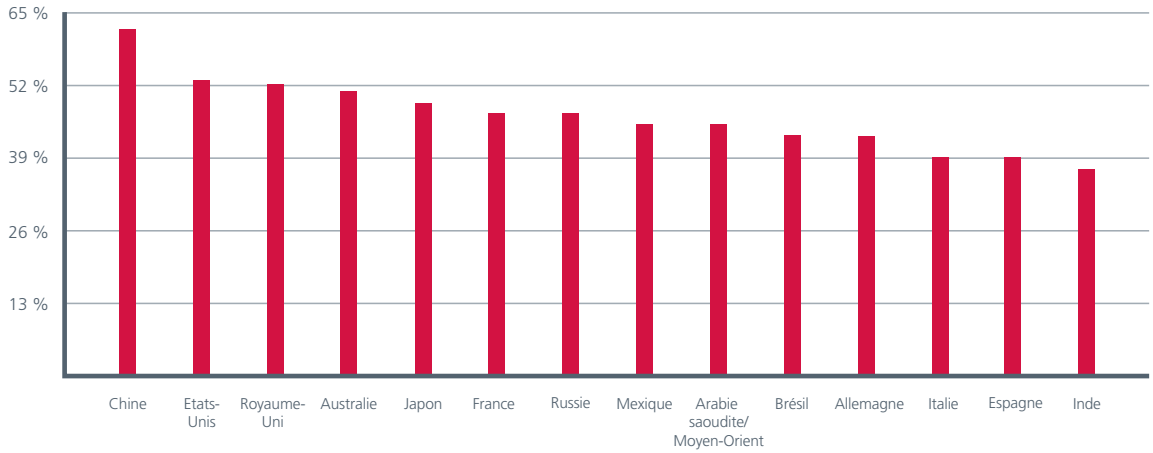
L'agrégation de ces données permet d'identifier les pays et les secteurs affichant les taux d'adoption le plus élevé et le plus faible de ces mesures en général. Ces observations ne constituent pas nécessairement une mesure de la qualité (bonne ou mauvaise) de la sécurité dans un secteur ou un pays donné. Elles permettent plutôt de mettre en lumière les pratiques de sécurité qui n'entrent pas dans le cadre de l'autoévaluation subjective des répondants et d'établir le taux objectif de déploiement de mesures de sécurité clés.

En se fondant sur cette mesure, c'est la Chine qui enregistre le plus fort taux d'adoption de mesures de sécurité (62 %), suivie de loin par les Etats-Unis, le Royaume-Uni et l'Australie, dont les taux varient entre 50 et 53 %.

L'Italie, l'Espagne et l'Inde présentent les taux d'adoption les plus faibles, avec des valeurs toutes inférieures à 40 %. Les autres pays, à savoir le Japon, la Russie, la France, l'Arabie saoudite, le Mexique, le Brésil et l'Allemagne, affichent tous des taux compris entre 40 et 49 %.

Les secteurs bancaire et de l'énergie arrivent en tête de peloton en termes d'adoption de mesures de sécurité, alors que le secteur de la distribution d'eau et du traitement des eaux usées se classe en dernière position.

Taux d'adoption de mesures de sécurité d'après les réponses des cadres




### Taux d'adoption de mesures de sécurité

Les cadres dirigeants en informatique et en sécurité ont dû répondre à des questions concernant 27 mesures de sécurité différentes : dix technologies de sécurité, six stratégies de sécurité, cinq méthodes différentes de chiffrement et six modes d'authentification obligatoire. Ce taux d'adoption mesure essentiellement le nombre de réponses positives concernant l'utilisation d'une mesure de sécurité donnée.

Chaque organisation possède sa propre stratégie en matière de sécurité, et la plupart des mesures de sécurité sur lesquelles les cadres dirigeants ont été interrogés peuvent être utilisées de multiples façons. C'est la raison pour laquelle le taux d'adoption de mesures de sécurité ne doit pas être nécessairement considéré comme une mesure de la qualité, bonne ou mauvaise, de la sécurité dans un secteur ou un pays donné. Il permet, en revanche, d'établir un jugement comparatif concernant le taux d'adoption de mesures de sécurité clés par différents secteurs et pays.
Il s'agit d'une mesure approximative puisque chaque technologie, pratique ou stratégie bénéficie d'une pondération identique, quelle que soit son efficacité. Elle n'en demeure pas moins objective.

### D'après les réponses des cadres, la Chine est le pays où l'adoption de mesures de sécurité est la plus forte (62 %).

Ses différents taux d'adoption, quelle que soit la mesure, sont supérieurs à n'importe quel autre pays. Viennent ensuite les Etats-Unis (53 %), l'Australie (51 %) et le Royaume-Uni (52 %).

L'Italie, l'Espagne et l'Inde ont les taux d'adoption globaux les plus bas, avec des valeurs toutes inférieures à 40 %. Les autres pays, à savoir le Japon, la Russie, la France, l'Arabie saoudite, le Mexique, le Brésil et l'Allemagne, affichent tous des taux compris entre 40 et 49 %.

### De hauts taux d'adoption limitent-ils les probabilités de réussite des attaques ?

Cette question est primordiale mais les réponses fournies par l'enquête sont mitigées. D'une part, la Chine, en première position dans l'adoption des mesures de sécurité, présente effectivement un taux de victimes d'attaques inférieur à celui des pays en queue de peloton, comme l'Inde. D'autres données laissent également penser que les pays où l'adoption de mesures de sécurité est réduite peuvent être affectés de diverses façons. Le système mondial de renseignements sur les menaces de McAfee, par exemple, surveille le trafic électronique malveillant émanant d'ordinateurs compromis et intégrés à des réseaux de robots à la suite de leur infection. Selon ces données, l'Inde, qui enregistre le niveau d'adoption de mesures le plus bas, bat tous les records en termes de trafic malveillant en Asie puisque ce dernier dépasse celui de la Russie et de la Chine réunies.

En revanche, le bilan global de la sécurité en Chine n'est pas tellement meilleur que celui de nombreux autres pays affichant un taux d'adoption moindre. La Chine n'est pas particulièrement épargnée par les attaques de grande envergure et les responsables chinois interrogés ne se considèrent pas beaucoup mieux préparés que dans d'autres pays.

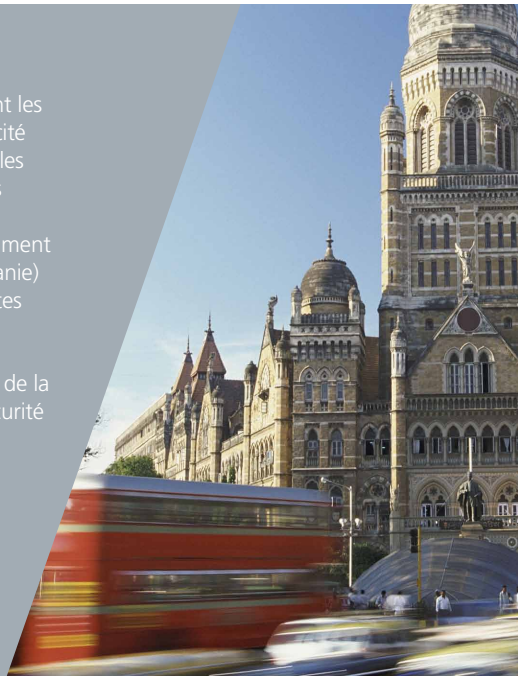
### Adoption peu généralisée de certaines mesures clés

La technologie de sécurité la moins adoptée est celle des listes d'autorisation d'applications, mise en œuvre par moins d'un cinquième (19 %) des organisations sur les réseaux informatiques et SCADA/ICS. D'autres technologies de sécurité plus évoluées, comme les systèmes de gestion des événements et des informations de sécurité ainsi que les outils de détection des anomalies et des rôles, sont utilisées respectivement par 43 et 40 % des sociétés interrogées.

## Chine et Inde : des résultats contrastés

Quels facteurs peuvent expliquer la différence énorme en termes d'adoption de mesures de sécurité de ces deux puissances asiatiques ? Les répondants chinois et indiens considèrent que le niveau de réglementation est très élevé dans leur pays. En Inde plus que dans n'importe quel pays, les cadres dirigeants déclarent que leur cybersécurité est soumise à la législation et aux réglementations (97 %), la Chine venant en deuxième position avec l'Allemagne (92 %). Les attitudes envers les pouvoirs publics varient toutefois considérablement. Parmi les entreprises chinoises soumises à des réglementations, 91 % ont changé leurs processus d'entreprise pour se mettre en conformité tandis qu'en Inde, seules 66 % l'ont fait. En outre, l'Inde est l'une des moins bien classées en termes de participation à des partenariats sous l'égide des pouvoirs publics dans le domaine des infrastructures critiques tandis que la Chine occupe la première place.

Les cadres dirigeants chinois présentent également les niveaux de confiance les plus élevés dans la capacité de leur pouvoirs publics à prévenir et décourager les attaques informatiques. Les informations fournies par le système mondial de renseignements sur les menaces de McAfee montrent que l'Inde a récemment remplacé la Chine (ainsi que la Russie et la Roumanie) comme terrain de chasse de prédilection des pirates informatiques pour le recrutement d'ordinateurs infectés en vue de la constitution de réseaux de robots. Il pourrait s'agir d'une autre conséquence de la disparité en termes d'adoption de mesures de sécurité entre les deux pays.



D'après les réponses des cadres, la Chine est le pays où l'adoption de mesures de sécurité est la plus forte.

Aux dires des experts, il se peut que les entreprises n'ont pas toujours conscience des avantages de certains outils récents ou que ces derniers ne conviennent qu'aux grandes entreprises.

Pour autant, certaines mesures élémentaires ne sont pas plus largement mises en œuvre. Seuls 57 % des cadres dirigeants déclarent que leur entreprise applique régulièrement des patchs et des mises à jour. Le déploiement régulier de patchs est plus répandu en Arabie saoudite (80 %), en Russie (77 %), en Australie (73 %), alors qu'il l'est peu au Brésil (37 %).

Seul un tiers des cadres interrogés affirme que leur organisation possède des stratégies « qui limitent ou interdisent l'utilisation des clés USB ou d'autres supports amovibles ». Outre le risque de téléchargement, vol ou sortie illicite de données, de tels supports, même lorsqu'ils sont utilisés sans intention malveillante, peuvent facilement être à l'origine de la propagation de virus et d'autres logiciels malveillants, même sur des systèmes protégés par un pare-feu. Les mesures d'interdiction des clés USB et d'autres supports similaires sont largement adoptées en Arabie saoudite (65 %) et en Russie (50 %). C'est en Espagne (13 %) et au Brésil (20 %) qu'elles sont les moins appliquées.

### Autres mesures plus répandues

La mesure de sécurité la plus couramment mise en place est l'utilisation de pare-feux entre des réseaux privés et publics (77 % toutes entreprises confondues et 65 % pour celles qui utilisent des systèmes SCADA ou ICS).

Les services de renseignements et de surveillance des menaces affichent le taux d'adoption le plus élevé en Inde (57 %), en Chine (54 %) et au Japon (54 %), et le plus faible en Arabie saoudite (20 %), en Russie (23 %) et en Italie (20 %).

### Variations sensibles dans l'utilisation du chiffrement

Comme pratiquement toutes les mesures, c'est la Chine qui se classe première dans la mise en œuvre du chiffrement. La seule exception concerne l'utilisation du chiffrement pour protéger les données sur CD et autres supports amovibles, la Chine (48 %) se classant alors derrière les Etats-Unis (56 %), le Japon et le Royaume-Uni (avec tous deux 54 %). L'Inde présente des taux d'adoption plus bas que la moyenne pour cinq des six utilisations du chiffrement. Cette constatation vaut également pour l'Italie et l'Espagne.

### Le secteur de la distribution d'eau et du traitement des eaux usées à la traîne

Le taux d'adoption de mesures de sécurité est le plus élevé dans les secteurs des services bancaires/financiers et de l'énergie (tous deux de 50 %). Le taux le plus bas est à mettre au compte du secteur de la distribution d'eau et du traitement des eaux usées (38 %). Tous les autres secteurs affichent des taux de 40 % et plus.

Le secteur de la distribution d'eau et du traitement des eaux usées présente le plus faible niveau d'adoption de mesures de sécurité visant à protéger les systèmes SCADA/ICS, sans doute parce qu'il possède également le pourcentage de connexion le plus bas entre les systèmes SCADA et les réseaux IP (55 % contre 76 % en général).

Lorsque vous analysez ces données, tenez compte du fait que l'échantillon de dirigeants du secteur de l'eau interrogés est très petit par rapport à l'échantillon global des entreprises dotées de systèmes SCADA/ICS (seulement 11 sur 143).

80 % ont admis que les systèmes SCADA sont connectés à des réseaux IP ou à Internet en dépit du risque impliqué.

**Sécurité des systèmes SCADA**

Nous avons également créé une échelle des taux d'adoption pour les systèmes SCADA et ICS, sur la base d'une liste de 16 mesures d'authentification et de sécurité implémentées par les responsables de ces systèmes. (Ces chiffres doivent être interprétés avec prudence en raison de la petite taille de l'échantillon. En effet, seuls 143 répondants sur 600 étaient responsables de systèmes SCADA au sein de leur entreprise et ont été interrogés sur ceux-ci.)

Pour les systèmes SCADA/ICS, c'est une fois encore la Chine qui enregistre le plus haut taux d'adoption de mesures de sécurité (74 %), loin devant l'Australie (57 %) et le Brésil (54 %). L'écart entre les pays est surprenant. Les taux d'adoption sont les plus bas en Inde et en Espagne (toutes deux 29 %), suivies du Royaume-Uni (31 %), ce qui signifie que les opérateurs de systèmes SCADA/ICS chinois ont adopté trois fois plus de mesures de sécurité clés que leurs homologues indiens et espagnols.

Dans la plage intermédiaire figurent les Etats-Unis et le Japon (50 %), suivis par la France, la Russie, l'Allemagne et l'Arabie saoudite (40 % et plus), puis par l'Italie et le Mexique (respectivement 38 et 35 %).

Certains outils comme les listes d'autorisation d'applications et les solutions de gestion des événements et des informations de sécurité sont plus largement implémentés dans les systèmes SCADA/ICS que dans les réseaux IP.

Les cadres dirigeants rendent compte de hauts niveaux de connexion des systèmes SCADA à des réseaux IP, y compris Internet, malgré la prise de conscience généralisée des risques posés.

76 % des responsables de systèmes SCADA/ICS interrogés admettent que leurs réseaux sont « connectés à un réseau IP ou à Internet », et dans près de la moitié des sociétés connectées (47 %), la connexion pose un « problème de sécurité non résolu ».

Selon un cadre doté d'une longue expérience en matière de sécurité informatique, les connexions aux réseaux IP représentent un risque car elles peuvent permettre à des utilisateurs non autorisés d'accéder à des systèmes contrôlant les infrastructures critiques. « La conception initiale de SCADA ne prévoyait pas que les systèmes de contrôle seraient exposés à des réseaux auxquels des utilisateurs non habilités bénéficient d'une forme quelconque d'accès. » Le logiciel des systèmes SCADA a été écrit « il y a quelque temps déjà et n'a pas été modifié depuis ». Les systèmes « ne sont pas (exécutés) sur les plates-formes les plus récentes et comportent dès lors des vulnérabilités identifiées au fil du temps ».

Dans la mesure où ces systèmes associent souvent du matériel et des logiciels, ils ne peuvent pas être mis à jour comme un logiciel normal, et les remplacer constituerait « une opération extrêmement complexe et coûteuse », déclare l'expert. Il n'existe « aucun mécanisme permettant de réviser le système et de le modifier en cas de détection de vulnérabilités ».

Un expert en cybersécurité du secteur de l'électricité déclare que les systèmes SCADA ont été « développés comme des environnements techniques », dotés de peu de fonctionnalités de sécurité et qu'ils sont « généralement ouverts et difficiles à sécuriser ».

Certains experts estiment que les réseaux SCADA/ICS ne devraient jamais être connectés à Internet. « Les systèmes de contrôle devraient être une infrastructure dédiée, non connectée à Internet », explique un spécialiste du secteur des transports. Selon lui, l'« aspect pratique » est parfois la seule véritable raison de la connexion des réseaux ICS à Internet.

Il ajoute : « Le ver Conficker, qui s'est propagé via Internet, a tiré la sonnette d'alarme à certains égards. Le fait qu'il se soit propagé même là où on ne l'attendait pas a soulevé bien des questions. »

Toutefois, les experts estiment également qu'il existe aujourd'hui une bien meilleure prise de conscience des failles des systèmes SCADA, fait confirmé par les données de l'enquête.

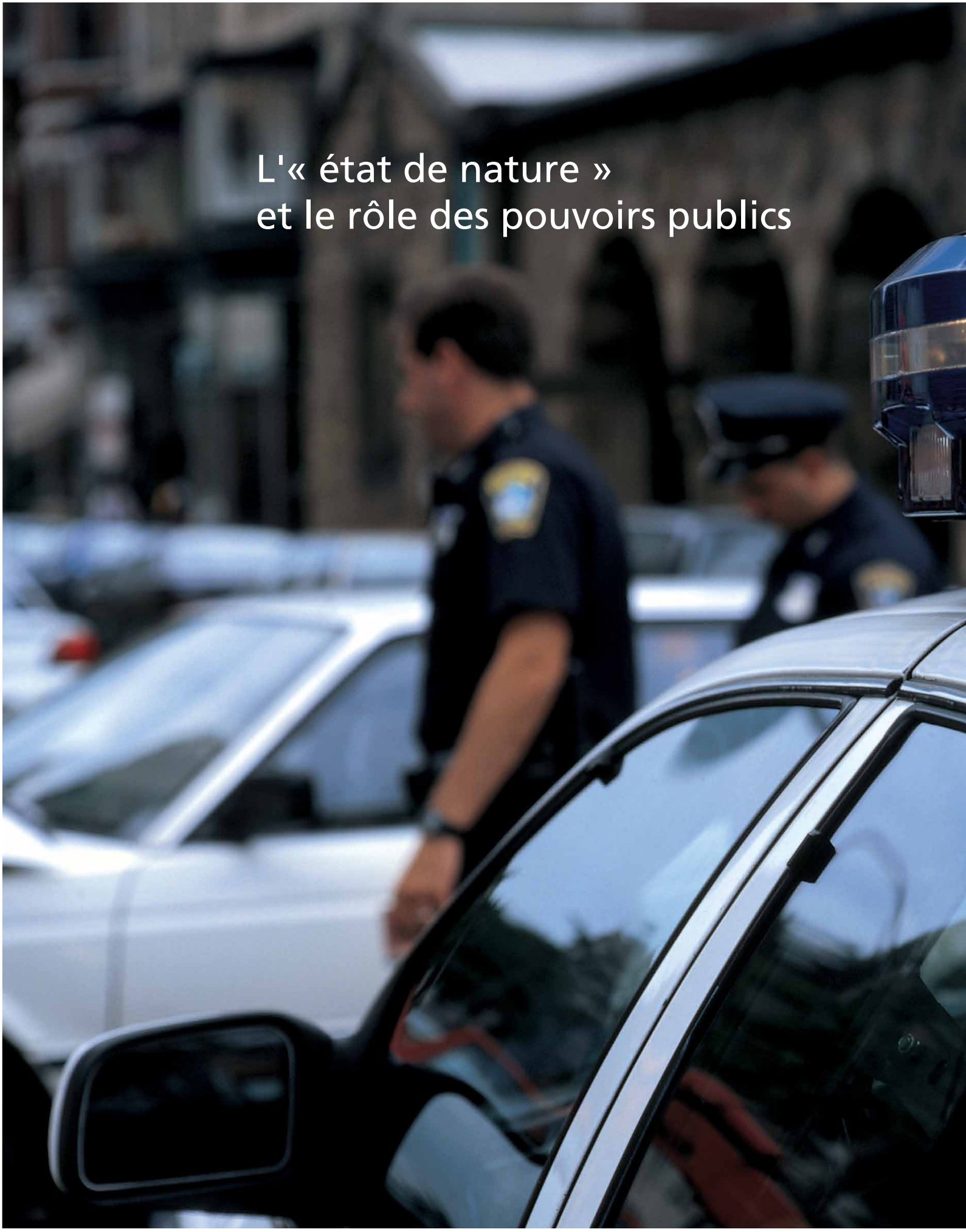
Selon le spécialiste du secteur des transports : « En toute honnêteté, cinq ans plus tôt, si vous vous rendiez dans n'importe quelle grande organisation de notre secteur ou d'autres d'ailleurs et que vous discutiez avec l'équipe chargée de la cybersécurité... il est fort probable qu'il aurait ignoré jusqu'à l'existence de ces systèmes de contrôle, leur objet et leur fonctionnement, car ils sortaient de leur cadre de responsabilité et de celui des directeurs informatiques. Ils relevaient en fait exclusivement du personnel en charge des opérations qui n'accordait aucune attention à la cybersécurité. »

Il conclut en disant : « sans risque de me tromper, je pense qu'à l'heure actuelle, tout le monde s'efforce actuellement de combler le retard ».

92 % des cadres responsables des systèmes SCADA déclarent que ceux-ci font l'objet d'une forme quelconque de surveillance. La mesure la plus largement adoptée est la mise en place d'outils d'analyse du comportement au niveau du réseau (62 % au total), avec la Chine (100 %), le Royaume-Uni (78 %) et le Mexique (75 %) en tête de liste. 59 % des répondants utilisent des journaux d'audit, surtout en Allemagne (90 %) et en Chine (82 %).

Seuls 8 % admettent ne pas surveiller les nouvelles connexions IP aux systèmes SCADA/ICS.

# L'« état de nature » et le rôle des pouvoirs publics



Les cadres dirigeants en informatique considèrent les Etats-Unis comme l'un des pays les plus « susceptibles d'être impliqués » dans des cyberattaques contre des pays étrangers.

Aujourd'hui, le cyberespace se trouve majoritairement dans ce que Hobbes appelait l'état de nature : une « guerre de tous contre tous ». Hobbes pensait que seuls les lois et l'Etat étaient capables de mettre un terme à cette guerre permanente entre les hommes. Dans le cyberespace toutefois, le rôle des pouvoirs publics est plus compliqué. La majorité des infrastructures critiques à travers le monde sont entre les mains d'entreprises privées, souvent actives dans plusieurs pays. Pour ces entreprises, les Etats sont des partenaires, certes, mais aussi des régulateurs et des policiers, des propriétaires, des maîtres d'œuvre et des clients. Parfois aussi, ils se transforment en adversaires, en agents infiltrés ou même en agresseurs.

Même lorsque l'Etat adopte le rôle de défenseur, c'est-à-dire lorsqu'il s'efforce de prévenir les attaques et d'améliorer la sécurité, certains cadres dirigeants en informatique et en sécurité sont plutôt sceptiques quant à leur capacité à dissuader ces attaques ou à protéger les entreprises, bien que les attitudes varient largement d'un pays à l'autre.

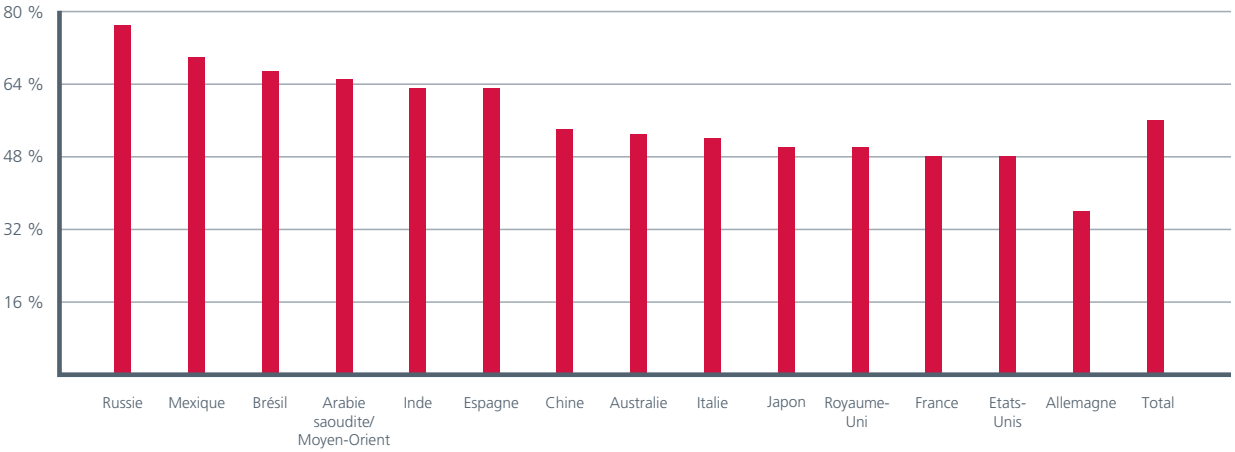
Il est toutefois un domaine où les initiatives officielles sont vues d'un bon œil comme ayant un effet généralement positif : celui de la réglementation. Les taux d'exécution des audits et de conformité à ces réglementations, l'impact effectif de ces dernières sur la sécurité ou encore les perceptions vis-à-vis de leur efficacité sont très différents selon les pays.

De nombreux Etats encouragent la coopération en matière de cybersécurité entre les propriétaires et les opérateurs d'infrastructures critiques, mais il apparaît que la participation aux initiatives varie fortement.

Les cadres chinois évoquent une coopération exceptionnellement étroite avec l'Etat, ainsi qu'une forte réglementation et un haut degré de confiance dans les pouvoirs publics. La Chine émerge ainsi comme une tête de pont en termes d'engagement de l'Etat dans la collaboration avec les secteurs d'activité.

Dans le monde, les cadres dirigeants en informatique et en sécurité manifestent clairement des sentiments très ambivalents envers les Etats-Unis. C'est la nation la plus souvent citée en modèle en matière de gestion de la cybersécurité. En même temps, des cadres dirigeants de nombreux pays, y compris grand nombre de nations alliées, considèrent les Etats-Unis comme l'un des pays les plus « susceptibles d'être impliqués » dans des cyberattaques contre des pays étrangers, juste devant la Chine.

Pourcentage de répondants estimant que les lois actuellement en vigueur dans leur pays sont insuffisantes pour contrer les cyberattaques




### Les doutes sur la capacité des autorités et des lois à décourager les attaques

Plus de la moitié de tous les cadres dirigeants interrogés estiment que la législation de leur pays est insuffisante pour dissuader les cyberattaques. Plus des trois quarts des Russes sont de cet avis, partagé d'ailleurs par une vaste majorité des Mexicains et Brésiliens. Ce sont les Allemands qui ont la plus grande confiance dans le pouvoir dissuasif de leurs lois, suivis par la France et les Etats-Unis.

Dans certains des pays que nous venons d'évoquer, beaucoup doutent de la capacité des pouvoirs publics à prévenir et à décourager les attaques. Un pourcentage impressionnant d'entre eux (45 %) estime que leurs pouvoirs publics ne sont « pas très » ou « pas du tout » à même de prévenir et de dissuader les cyberattaques. Dans des nations comme le Brésil et l'Italie, les deux tiers ou plus pensent que leurs pouvoirs publics n'en sont « pas très » ou « pas du tout » capables. Le Mexique, l'Arabie saoudite, l'Allemagne et l'Espagne sont aussi au nombre des pays dont la majorité envisage les facultés de prévention et de dissuasion de leurs autorités de manière défavorable. Aux Etats-Unis, par contre, seuls 27 % des cadres dirigeants ont une mauvaise opinion de la capacité de leurs pouvoirs publics en la matière ; en Chine, le vote de défiance frôle les 30 % seulement.

« Pour l'instant, le shérif est absent », pour reprendre l'analogie avancée par le général à la retraite Michael Hayden, qui vient de mettre un terme à sa longue carrière dans les services de renseignements américains en tant que directeur de la CIA. Selon lui, le cyberspace est un peu comme le Far West... « Tout le monde doit se défendre par soi-même, donc tout le monde est armé. » Mais dans le « cyberdomaine », c'est un peu comme si l'on attendait de chaque citoyen qu'il organise sa propre défense nationale. « Il ne nous viendrait pas à l'idée de nous rendre dans un bureau de poste et de demander aux préposés quelles armes ils utilisent pour assurer leur propre défense... pourtant, c'est un peu ce qui se passe en matière de cybersécurité », affirme Michael Hayden.

### La majorité pense que les réglementations officielles améliorent la sécurité

Un grand nombre d'experts s'accordent à dire que les pouvoirs publics doivent consentir davantage d'efforts pour améliorer la cybersécurité des infrastructures critiques. Pour l'instant, toutefois, le bilan est mitigé. Les approches sont aussi nombreuses que variées, leur impact est très inégal, et les cadres informatiques des divers pays les accueillent avec plus ou moins d'enthousiasme ou de scepticisme.

Dans l'ensemble, 86 % des cadres indiquent que leur cybersécurité est soumise de l'une ou l'autre manière à une réglementation imposée soit par la loi, soit par les autorités publiques. Près de trois quarts (74 %) affirment que leur organisation a « mis en œuvre de nouvelles politiques, procédures, meilleures pratiques ou mesures techniques » en vertu de la législation ou

Une forte majorité de cadres informatiques estime que les réglementations et/ou la législation ont contribué à améliorer la cybersécurité.

de la réglementation. Les variations nationales sont considérables, avec deux pourcentages largement en dehors des moyennes aux deux extrêmes du spectre : en Chine, 91 % des organisations ont modifié leurs politiques à la suite des réglementations officielles, contre seulement 56 % en Espagne. Dans la moyenne, en Inde, en Allemagne, en Italie et en Australie, il apparaît que moins de 70 % ont modifié leurs procédures.

Pour 42 % des cadres interrogés, la réglementation officielle n'a eu « aucun effet significatif », ou aurait même « accaparé des ressources qui auraient pu servir à améliorer la sécurité » ; par opposition, 58 % estiment qu'elle a « amélioré la politique de l'entreprise et renforcé la sécurité ». Dans des pays dont les approches nationales varient pourtant fortement (le Brésil, l'Espagne, la Chine, le Mexique, l'Allemagne et le Japon), de 60 à 70 % s'accordent à reconnaître que la réglementation a amélioré la sécurité. Le scepticisme s'est révélé le plus fort en Italie et en Australie, où la majorité a mis en doute la valeur des mesures réglementaires de leurs pouvoirs publics.

La confiance dans l'efficacité de la réglementation est particulièrement faible dans le secteur de l'eau, où seulement 24 % des personnes interrogées reconnaissent qu'elle a accru la sécurité. Une fois encore, même si les chiffres de ce secteur d'activité sont un extrême statistique, il n'en reste pas moins que le petit nombre de répondants est à prendre en compte.

**Participation et partenariat**

En ce qui concerne la coopération en matière de cybersécurité instiguée par les pouvoirs publics, on constate de fortes variations parmi les propriétaires et les opérateurs d'infrastructures critiques.

De manière générale, la participation à des partenariats sous l'égide des pouvoirs publics est faible. A la question de savoir s'ils étaient impliqués dans la mise au point de lois ou règlements, environ un tiers (35 %) des cadres dirigeants déclarent que leur organisation était active au sein d'un organisme de partenariat entre secteur public et privé. Cette participation est plus intense dans les organisations plus horizontales telles que les associations de partage d'informations propres à certains secteurs, où plus de la moitié des répondants (53 %) affirment qu'ils étaient membres.

Cependant, la participation varie fortement selon les pays. Elle est la plus élevée en Chine, où 61 % des cadres dirigeants affirment appartenir à une organisation travaillant en partenariat avec les autorités. Les taux de participation sont les plus faibles au Brésil (22 %) et inférieurs à 30 % au Japon, en Allemagne, en Italie, en Inde et en Espagne.

Il est néanmoins possible que ces taux de participation ne constituent pas des indicateurs totalement fiables du succès de ces initiatives. Même aux Etats-Unis, où la participation à des organismes de partenariat est relativement forte, avec 42 %, les données recueillies lors des entrevues donnent à penser que de nombreuses entreprises craignent encore que le partage d'informations ne se fasse à sens unique.

### La Chine tête de pont en matière d'implication de l'Etat vis-à-vis des secteurs d'activité

Dans l'ensemble, un peu moins de la moitié (49 %) des cadres dirigeants en informatique et en sécurité affirme avoir été soumis à un audit d'une agence officielle dans le domaine de la conformité aux lois et réglementations sur la cybersécurité. Il existe toutefois des variations très fortes dans les taux d'audit selon les pays. Ainsi, la Chine et l'Arabie saoudite se placent très loin en tête, avec respectivement 83 % et 73 %. Le Brésil, l'Australie et la France affichent des taux d'audit supérieurs à 50 %. Ils sont les plus bas en Russie (30 %) et en Espagne (32 %).

Les cadres chinois évoquent également un niveau élevé d'activité réglementaire et législative par les autorités, avec 92 % affirmant qu'ils y sont soumis — un chiffre comparable à celui de l'Allemagne qui enregistre le deuxième taux le plus élevé mis à part l'Inde, avec 97 %.

Le pays où les cadres dirigeants signalent les niveaux les plus bas d'activité réglementaire est les Etats-Unis, où 72 % affirment qu'ils sont soumis à une réglementation de leur cybersécurité, comparé à une moyenne de 86 %.

### Les Etats-Unis vus comme un modèle

Sans doute pour cette raison, les cadres dirigeants en informatique et en sécurité ont le plus fréquemment identifié les Etats-Unis comme pays autre que le leur qu'ils considéraient comme un modèle en matière de cybersécurité, avec 44 % des répondants partageant ce point de vue. Suivent dans la liste des modèles nationaux les plus populaires l'Allemagne (22 %) et le Royaume-Uni (18 %). Le modèle américain est particulièrement apprécié en Chine (78 %) et au Mexique (72 %). Sa popularité est la plus faible en Allemagne (31 %).

Les données recueillies lors des entretiens suggèrent que la mise en avant du modèle américain doit sans doute plus à l'attention qu'ont accordée les médias et certains dirigeants politiques en vue aux efforts consentis par ce pays en la matière, plutôt qu'à la manière dont les autorités d'outre-Atlantique gèrent ce problème. De fait, peu de nations semblent les émuler à cet égard.

### Sources de scepticisme concernant la valeur des réglementations

Il existe clairement une méfiance assez répandue chez les cadres dirigeants quant à l'impact des réglementations et des législations. Ce n'est sans doute pas surprenant. Se baser sur des réponses à une enquête pour déterminer les attitudes vis-à-vis des réglementations peut se révéler problématique. Peu de cadres en appellent à plus de régulation. Toutefois, certaines idées fondamentales se dégagent.

Les personnes interrogées ont mis en évidence trois domaines qui les préoccupent plus particulièrement :

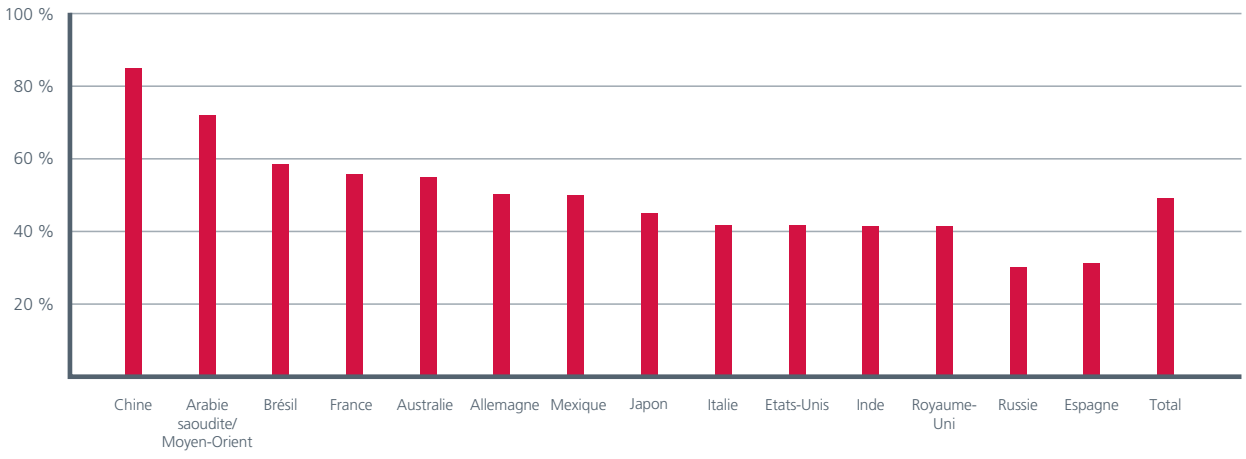
- Un manque de confiance dans les connaissances des autorités sur le mode de fonctionnement d'un secteur d'activité
- La possibilité que des réglementations maladroites puissent niveler la sécurité par le bas dans divers secteurs
- Le risque que la divulgation obligatoire des incidents de sécurité (par exemple en cas de compromission de données personnelles) n'entraîne les politiques et les ressources dans des directions contraires aux objectifs effectivement poursuivis

Le scepticisme est particulièrement répandu dans le secteur de la distribution et du traitement des eaux usées, où 77 % des personnes interrogées affirment que les lois et les réglementations ont soit « accaparé des ressources qui auraient pu servir à améliorer la sécurité » ou n'ont eu aucun effet. Les cadres de ce secteur affichent aussi le degré de confiance le plus bas dans la capacité de leurs pouvoirs publics à prévenir ou à décourager les cyberattaques.

Un expert en sécurité américain du secteur de la distribution et du traitement de l'eau affirme que les exigences réglementaires se font très fortement ressentir, particulièrement dans le cas de plus petites structures dans un secteur fort diversifié. « Nos gars sur le terrain se trouvent coincés dans un scénario où ils doivent toujours parer au plus pressé en essayant de répondre aux nombreuses exigences variées imposées par les réglementations, au lieu de planifier la sécurité de manière coordonnée. Essayer de contenter un trop grand nombre de maîtres finit par rendre les gens marteau. Cela consomme des ressources et cela laisse au final au responsable (la décision) de savoir comment les risques vont être gérés. »

Selon ce spécialiste, lui et ses collègues ont « souvent l'impression d'être des laissés-pour-compte » dans les forums sur la sécurité au niveau fédéral où tous les secteurs d'activité sont représentés. « Très souvent, nous ne bénéficions pas du même respect, pas à un niveau personnel mais à un niveau tactique ou stratégique, que les autres secteurs », explique-t-il.

Pourcentage de répondants subissant des audits par des agences officielles en vertu de lois et/ou de réglementations




Toutefois, le scepticisme vis-à-vis des réglementations ne se limite pas au secteur de l'eau, et les entretiens révèlent que celui-ci naît de préoccupations plus répandues.

« Ici, aux Etats-Unis, il existe un manque de confiance dans les connaissances des pouvoirs publics quant aux mesures à prendre et quant au fonctionnement des diverses infrastructures », explique un spécialiste de la sécurité dans le secteur du transport. Selon lui, beaucoup « craignent que les réglementations n'entraînent énormément d'opérations très couteuses, pour une augmentation minime voire nulle de la sécurité ».

Les experts avancent aussi que dans des secteurs où les opérateurs sont très diversifiés, les réglementations, particulièrement si elles sont appliquées sans discernement, peuvent involontairement niveler les exigences vers le bas. L'introduction d'une norme dans un secteur très diversifié peut renforcer la sécurité chez certains mais définir un plancher qui ôterait à d'autres entreprises technologiquement plus avancées toute motivation à implémenter des mesures plus rigoureuses alors qu'elles auraient aisément pu le faire. « J'ai entendu parler d'organisations qui ont fait marche arrière en matière de gestion de la sécurité de l'entreprise pour répondre spécifiquement aux exigences de la réglementation », déclare un spécialiste de la sécurité dans le secteur de la distribution d'électricité.

Beaucoup craignent que la plupart des réglementations n'entraînent « énormément d'opérations très couteuses, pour une augmentation minime voire nulle de la sécurité ».

Les cadres affirment que, mis à part l'arrêt des opérations, les conséquences d'une cyberattaque qu'ils craignent le plus sont les atteintes à la réputation. Des témoignages suggèrent que les lois imposant la divulgation de certains incidents de sécurité pourraient inciter les entreprises à effectuer des investissements et à prendre des décisions stratégiques de nature à réduire le nombre d'incidents susceptibles d'être rapportés, plutôt qu'à renforcer la sécurité globale de l'entreprise.

Au Japon, par exemple, un fonctionnaire a remarqué que les obligations de signaler des incidents liés à la sécurité des informations aux autorités a donné lieu à des plaintes, selon lesquelles « la charge administrative pour la personne responsable de la sécurité dépasse la (gravité de la) menace » que représentent ces incidents.

**Les Etats-Unis aussi considérés comme l'un des pays les plus vulnérables aux cyberattaques**

50 % des cadres dirigeants en informatique et en sécurité identifient également les Etats-Unis comme l'un des trois pays « les plus vulnérables aux cyberattaques sur les infrastructures critiques dans leur secteur », avant tout autre pays. La Chine arrive en seconde position (34 %), suivie de la Russie (27 %).

Les perceptions de la vulnérabilité américaine sont particulièrement répandues en Chine (où 80 % ont indiqué les Etats-Unis dans la liste des trois nations les plus vulnérables), au Mexique (73 %), ainsi qu'au Brésil et en Russie (70 %).

La Chine est principalement jugée vulnérable par les cadres des régions géographiquement proches, les Indiens (57 %), les Japonais (56 %) et les Australiens (43 %) s'étant montrés plus enclins que la moyenne à la citer parmi les trois nations les plus vulnérables.

Selon certains experts, les Etats-Unis sont considérés comme vulnérables parce qu'ils sont techniquement plus avancés, et donc plus dépendants des réseaux informatiques que pratiquement toutes les autres nations. D'autres argumentent toutefois que la vulnérabilité américaine aux cyberattaques n'est pas un cas isolé et qu'il est fort possible qu'elle soit exagérée.

**Les Etats-Unis et la Chine perçus comme des agresseurs potentiels en cas de cyberguerre**

Comme nous le faisons remarquer dans la première partie, une large majorité des cadres dirigeants en informatique et en sécurité pensent que des Etats étrangers ont déjà été impliqués dans des attaques contre des réseaux dans leur secteur d'activité. Lorsqu'on leur demande de citer le pays « dont ils craignent qu'il soit le plus susceptible d'être impliqué dans des attaques de réseaux contre leur pays/ secteur d'activité », 36 % ont pointé du doigt les Etats-Unis et 33 %, la Chine. C'est bien plus que les autres pays parmi les six proposés aux répondants (qui avaient par ailleurs la possibilité de spécifier une réponse différente). En troisième position, mais loin derrière, vient la Russie avec seulement 12 %. Aucun des trois autres pays, le Royaume-Uni, la France et l'Allemagne, n'ont franchi la barre des 6 %.

Les pays perçus comme des agresseurs potentiels varient en fonction des secteurs d'activité. Parmi les cadres de l'administration publique, par exemple, la Chine dépasse les Etats-Unis au titre de pays le plus susceptible d'être impliqué dans des cyberattaques. Dans le secteur de l'énergie, le premier pays cité est la Russie, tandis que la Chine et les Etats-Unis sont au coude à coude dans les télécommunications.

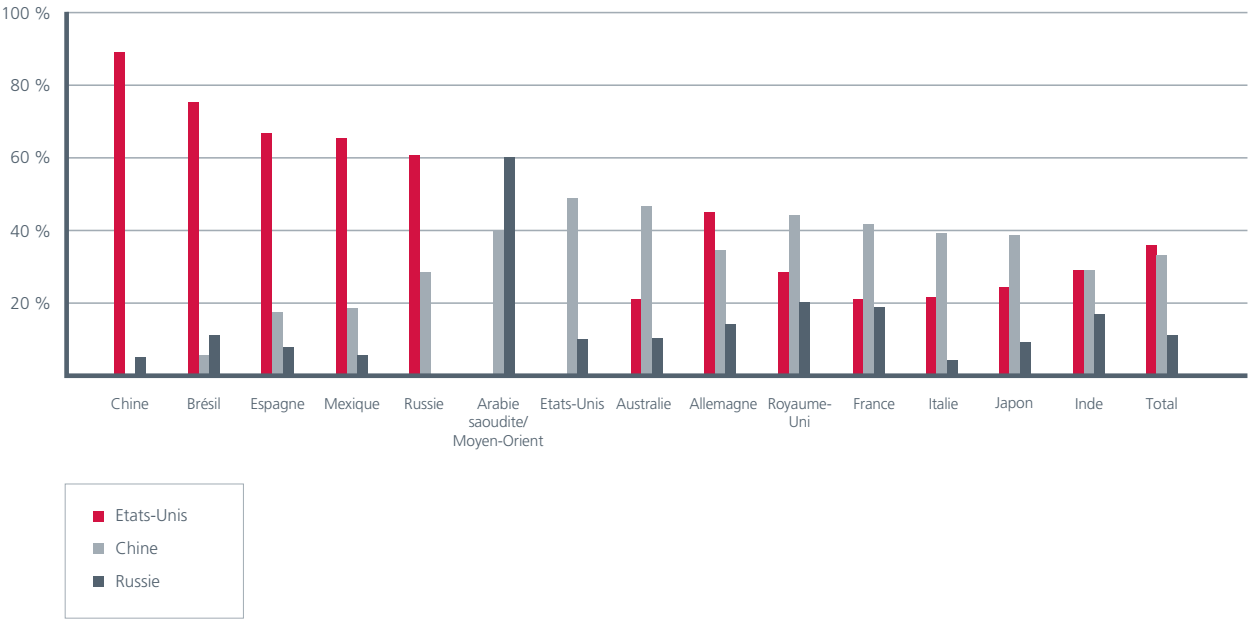
« Les agresseurs auxquels nous sommes confrontés (en Australie) sont des agresseurs économiques (...) cela dépend largement du secteur concerné », explique Ajoy Ghosh, cadre australien dans le domaine de la sécurité. « Le secteur minier considère la Chine comme une plus grande menace (...) Dans le domaine de la défense, les concurrents sont l'Europe et les Etats-Unis. »

Les Etats-Unis sont considérés comme le principal agresseur potentiel par une grande majorité des cadres dirigeants dans des pays où la méfiance envers les intentions américaines est habituelle : la Chine (89 %), le Brésil (76 %), l'Espagne (67 %), le Mexique (65 %) et la Russie (61 %). Mais même chez un allié traditionnel de l'Amérique tel que l'Allemagne, 45 % la désignent comme nation la plus susceptible d'être responsable d'attaques, tandis que seulement 34 % citent la Chine — alors que le gouvernement allemand a publiquement critiqué cette dernière pour mener des opérations informatiques d'espionnage sur les réseaux visant des actifs nationaux stratégiques.

« (Ce résultat) est sans doute moins choquant qu'il n'y paraît », observe le Michael Hayden. « Il se peut qu'il soit un simple reflet de la capacité et — en toute franchise — de la taille intrinsèques de nos agences de renseignements américaines. » Le gouvernement américain s'est également engagé dans une série de longs débats publics, pour une très large part non résolus, portant sur les politiques à adopter afin d'organiser ses capacités d'attaque et de défense de réseaux. Ces longues discussions sur la place publique ont peut-être agi comme une chambre d'écho des préoccupations concernant la capacité américaine, selon le général.

Bien que le débat américain ait trouvé un bien plus large écho auprès des médias, les autorités russes ont elles aussi lancé cette année un train de mesures législatives destinées à octroyer aux pouvoirs publics une plus grande liberté d'action contre les attaques et menaces. Ainsi, un nouveau projet de loi entend donner à Moscou l'autorité nécessaire pour définir les actes de cyberguerre et y réagir. Cette nouvelle loi « affirme pour l'essentiel que s'il peut déterminer qu'il est la cible d'un gouvernement d'un autre Etat dans le cadre d'une cyberattaque, quelle qu'elle soit, il peut traiter cette attaque comme un acte de guerre », explique Kimberly Zenz, spécialiste de la Russie auprès d'iDefense Labs.

Pourcentage des répondants citant les Etats-Unis, la Chine ou la Russie comme pays « le plus susceptible » de mener des cyberattaques contre des pays étrangers




Considérées dans leur ensemble, les nouvelles lois codifient de nouveaux pouvoirs d'une portée considérable pour le Kremlin, affirme-t-elle. « S'il subit un incident majeur, il peut à lui seul pointer du doigt le pays qu'il estime responsable et prendre des mesures unilatérales à très haut niveau sans nécessiter de preuve ou d'accord extérieurs. »

La Chine a elle aussi révélé publiquement des informations à propos de son programme de guerre informatique. Une étude de la littérature militaire chinoise ouverte au public, menée en 2009 par la Commission d'étude sino-américaine sur l'économie et la sécurité a conclu que « la doctrine de campagne (chinoise) identifie l'établissement précoce de la dominance en matière d'informations sur un ennemi comme l'une des principales priorités opérationnelles en cas de conflit ». Le rapport signale qu'une nouvelle stratégie baptisée Integrated Network Electronic Warfare (guerre intégrée exploitant l'électronique et les réseaux) semblait destinée à remplir ce rôle, en associant des techniques de cyberguerre et autres technologies électroniques belliqueuses avec des opérations cinétiques.

Malgré ces discussions, il existe des limites claires à la transparence. Tant la Russie que la Chine ont fait face à des accusations bien documentées (mais catégoriquement démenties), alléguant qu'elles faisaient cause commune avec des hackers nationalistes. Ces trois pays ont clairement l'intention de continuer à bénéficier, dans une plus ou moins large mesure, de l'avantage stratégique qu'offre le « démenti plausible » dans le cyberespace.

### Comment pouvons-nous échapper à l'« état de nature » ?

Tant que les grands Etats acceptent que règne une liberté d'action plus ou moins sans entraves dans le cyberespace, celui-ci restera le Far West. Entre-temps, les propriétaires et opérateurs des infrastructures critiques qui composent ce nouveau champ de bataille continueront à se trouver dans la ligne de mire et devront donc peut-être se doter eux-mêmes de leur propre arsenal de défense.

# Une meilleure sécurité à l'aube de la cyberguerre

En ce qui concerne les stratégies qui permettraient d'améliorer la cybersécurité, les données recueillies n'ont pas fourni de réponses faciles.

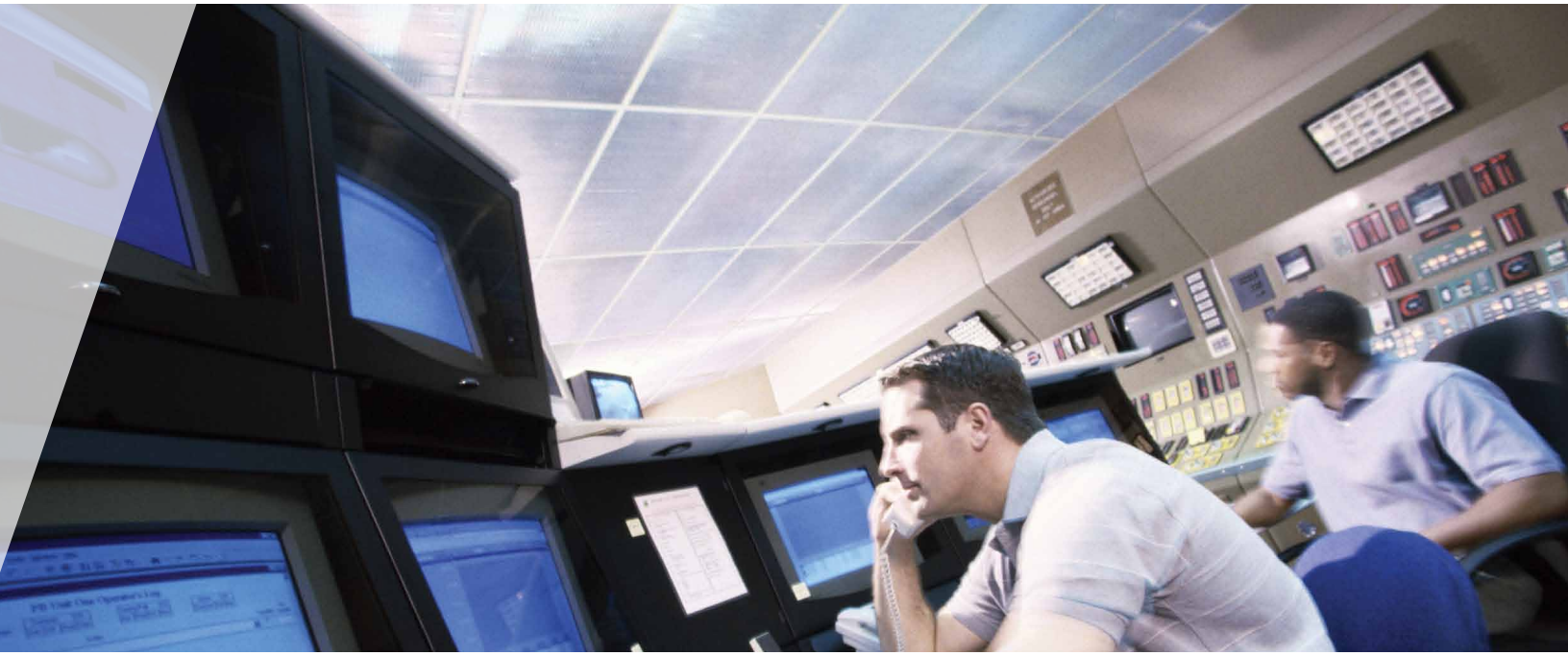
En ce qui concerne les stratégies qui permettraient d'améliorer la cybersécurité des infrastructures critiques, les données de l'enquête et des entretiens n'ont pas fourni de réponses faciles.

Les propriétaires et opérateurs d'infrastructures critiques indiquent que la sécurité est une priorité absolue à leurs yeux, ce qui semble amplement étayé par la large palette de mesures de sécurité qu'ils mettent en œuvre. Mais même les secteurs et les pays où les taux de déploiement de mesures de sécurité à l'efficacité attestée sont élevés ne sont pas à l'abri des attaques.

« Il n'existe pas de modèle de protection identifiable qui tienne la distance par rapport à l'évolution et à la sophistication des cybermenaces », affirme Michael Assante, du secteur de l'électricité. De plus, les technologies innovantes, de l'informatique dématérialisée aux réseaux de distribution et compteurs intelligents en passant par la connectivité SCADA, continuent à créer de nouvelles vulnérabilités.

Les pouvoirs publics sont eux aussi à la recherche de la meilleure approche en termes de cybersécurité pour leurs infrastructures. Deux défis particuliers sont communs à ces deux groupes :

- La modification d'anciennes organisations et structures publiques pour faire face aux cybermenaces visant les infrastructures critiques
- L'identification de méthodes efficaces pour partager des informations sensibles sur les menaces et les vulnérabilités avec les propriétaires et opérateurs, et pour déployer des mesures intelligentes visant à aider les infrastructures critiques à se défendre de façon autonome



### Certaines technologies de sécurité essentielles restent sous-utilisées

Les standards d'authentification en particulier méritent d'être améliorés, et l'adoption des technologies biométriques est réduite. La sécurité des réseaux dépend de plus en plus de la capacité à détecter et à bloquer les utilisateurs dont les comptes manifestent des anomalies de comportement ou outrepassent leurs droits définis. De plus, les auteurs d'attaques ciblent davantage les utilisateurs à titre individuel au travers du phishing et d'autres techniques. Cette évolution signifie que l'authentification des utilisateurs et de leurs privilèges prend une importance croissante.

Pourtant, plus de la moitié des cadres dirigeants (57 %) déclarent que leur organisation n'emploie que des noms d'utilisateur et des mots de passe pour authentifier les connexions à leur réseau. Les autres ont recours à des techniques d'authentification plus robustes, comme la biométrie ou les tokens (jetons), soit seules soit en combinaison. Dans l'ensemble, 16 % seulement affirment utiliser des technologies biométriques, un taux d'adoption assez bas que certains experts attribuent à une résistance culturelle dans de nombreux pays. Les tokens sont deux fois plus fréquents. Il existe des inconvénients, des défis techniques et des facteurs de coûts qui entrent en jeu dans l'emploi de la biométrie et des tokens, affirment les experts, et les combinaisons mot de passe/nom de connexion peuvent présenter des degrés d'efficacité très variables, suivant la force des mots de passe utilisés et la technologie de chiffrement adoptée. Toutefois, des niveaux de sécurité supplémentaires sont clairement préférables à l'unique recours aux noms d'utilisateur et mots de passe, qui sont souvent faciles à deviner, à voler ou à compromettre de l'une ou l'autre manière.

De même, sur le plan mondial, environ la moitié des cadres dirigeants seulement utilisent régulièrement le chiffrement dans la plupart des circonstances, bien que cette technologie soit mise en œuvre plus fréquemment (61 %) pour la transmission de données en ligne. Ce pourcentage semble aussi assez bas, particulièrement au vu de l'emploi de plus en plus répandu des périphériques mobiles. Pamela Warren, experte en cybersécurité chez McAfee, estime que « si vous possédez des périphériques mobiles et qu'ils contiennent des données sensibles, vous devez absolument envisager de chiffrer ces données ».

### Les vulnérabilités continuent de se multiplier

Le recours de plus en plus fréquent à des réseaux IP pour les systèmes SCADA et d'autres systèmes de contrôle opérationnel créent des vulnérabilités uniques et inquiétantes. Les cadres dirigeants qui gèrent des systèmes SCADA/ICS rendent compte de hauts niveaux de connexion de ces systèmes à des réseaux IP, y compris Internet, tout en reconnaissant que ces connexions donnaient lieu à des problèmes de sécurité. Des experts sectoriels ont exprimé leur forte inquiétude quant aux implications sur la sécurité de cette évolution, et les spécialistes en sécurité informatique insistent sur la nécessité d'apporter les mesures nécessaires pour corriger cette vulnérabilité.

L'accès à distance à des systèmes de contrôle « représente un grave danger », affirme Phyllis Schneck, Vice-Présidente de la division Threat Intelligence de McAfee. « Nous devons soit les protéger de façon appropriée, soit les déplacer vers des réseaux plus privés et ne pas utiliser ce réseau ouvert qu'est Internet », ajoute Mme. Schneck, qui est également membre de la Commission sur la cybersécurité du CSIS pour la 44e Présidence des Etats-Unis.

Plus de la moitié des cadres dirigeants déclarent que leur organisation n'emploie que des noms d'utilisateur et des mots de passe pour authentifier les connexions à leur réseau.

« La virtualisation de logiciels anciens par-dessus des logiciels plus récents procure un certain niveau de protection, ce qui permet aux protocoles et à l'accès réseau au moins de transiter par des piles logicielles plus évoluées », ajoute un vétéran de la sécurité informatique. Selon lui, les propriétaires et opérateurs doivent « dresser autant de barrières que possible entre eux et l'agresseur potentiel ».

« L'objectif (pour une sécurisation rapide des systèmes SCADA) ne devrait pas nécessairement être de mettre à l'arrêt (ou) de remplacer ces systèmes, mais de placer devant eux des technologies de blocage, dans la mesure du possible, et d'imposer des critères beaucoup plus rigoureux pour l'acceptation de nouveaux systèmes à l'avenir. »

### Le risque lié à SCADA aggravé par les plates-formes de services « intelligentes »

De nouvelles plates-formes de fourniture de services comme les « compteurs électriques intelligents » avec interopérabilité ou les transactions bancaires sur les périphériques mobiles engendrent de nouvelles vulnérabilités mais aussi de nouvelles opportunités. « Les réseaux de distribution intelligents vont certainement créer de nouvelles vulnérabilités, mais cela ne signifie pas que tout le système de distribution d'énergie sera plus fragile à l'avenir », explique l'ancien responsable de la cybersécurité du ministère américain de l'Energie, Christopher « Rocky » Campione. Il ajoute qu'ils procurent de nombreux avantages et améliorations en termes d'efficacité et de fiabilité.

Reste à voir si les économies réalisées compensent les risques encourus. L'un des défis dans le développement des compteurs intelligents est de parvenir à maîtriser suffisamment les coûts pour permettre une adoption à grande échelle. Les implications de ce type de pression sur la sécurité sont inquiétantes. « Quel niveau de sécurité pouvez-vous escompter si le coût à l'unité doit être inférieur à cent dollars ? », demande un expert.

Dans un environnement en évolution rapide, les cadres dirigeants en informatique et en sécurité sont confrontés à des choix difficiles concernant la sécurité, avec peu d'éléments d'informations en main, affirme M. Campione. « Vous devez prendre des décisions qui tiennent compte des opportunités, des risques et de la sécurité, mais sans pour cela vous enliser dans des analyses interminables. Vous ne disposez jamais de toutes les données avant de trancher. » Dans un tel environnement, on ignore quelle attention sera portée aux compromis de sécurité nécessaires aux réseaux de distribution intelligents.

### Les nouveaux défis de sécurité de l'informatique dématérialisée

Les systèmes dématérialisés permettent aux entreprises de louer des infrastructures de serveur et des services logiciels, externalisant ainsi de fait leurs besoins informatiques. Suivant les services et les données qui sont externalisés, de nouvelles mesures de sécurité peuvent être intégrées, mais de nouvelles vulnérabilités peuvent aussi apparaître.

De nombreux Etats n'ont guère progressé en matière d'organisation à cet égard, et, dans certains cas, sont clairement à la traîne.

L'informatique dématérialisée permet aux petites entreprises de mettre en œuvre des mesures de sécurité qui ne seraient pas autrement à leur portée. Et pourtant, « j'ai une peur bleue de l'informatique dématérialisée », affirme un expert de longue date de la sécurité informatique. « Pas parce que j'ai connaissance de problèmes particuliers qui lui sont propres, mais parce que, si l'on se penche un peu sur le passé, chaque fois que nous avons adopté une nouvelle technologie, nous avons été incapables de prévoir et d'appréhender les attaques potentielles auxquelles elle pouvait prêter le flanc. »

« Nous créons des systèmes toujours plus complexes et, qui plus est, qui doivent pouvoir fournir des services à d'autres systèmes à faible interdépendance et offrant une authentification laissant à désirer », conclut-il.

Selon Pamela Warren, pour corriger les vulnérabilités, les entreprises et les pouvoirs publics devraient « envisager les types de données dont on autoriserait la transmission via Internet et choisir le modèle d'informatique dématérialisée idéal qui leur convient le mieux, valider le modèle de sécurité et les pratiques du fournisseur de services, et établir des lignes directrices pour la responsabilité des différentes parties en matière d'hébergement ».

**La nécessité pour les pouvoirs publics de s'organiser plus efficacement pour faire face aux cybermenaces**

Un sujet qui revient régulièrement sur le tapis lors des entretiens avec les experts de différents secteurs et pays est la façon dont les pouvoirs publics s'organisent pour aborder les nouvelles menaces. Il s'agit de modèles courants ; tous les pays concernés par l'enquête, par exemple, avaient établi des équipes d'intervention informatique d'urgence pour gérer les réponses aux incidents, même si aux dires des cadres interrogés, leur efficacité varie. Cependant, de nombreux Etats n'ont guère progressé en matière d'organisation à cet égard, et certains pays sont très clairement à la traîne.

Au Brésil, par exemple, le gouvernement fédéral a instauré en août 2009 le Groupe de travail sur la sécurité des informations et la protection des infrastructures critiques, sous l'égide de son ministère de la Sécurité de l'information et des communications. Le groupe s'attelle à l'établissement de plans d'intervention d'urgence et étudie le problème de la sécurité des informations, selon Anchises de Paula, analyste brésilien auprès d'iDefense Labs.

En Australie, un livre blanc du ministère de la Défense publié en 2009 a annoncé l'établissement d'un Centre national d'opérations pour la cybersécurité, dans le cadre du service de renseignements australien (Defense Signals Directorate), mais de nombreux détails du projet n'ont pas encore été révélés.

Un spécialiste en cybersécurité australien affirme que son gouvernement a longtemps étudié les modèles américain et britannique, entre autres, dans le cadre de la récente révision de sa politique de cybersécurité. « Il y a une lutte d'influence entre les membres de l'administration qui penchent pour le modèle américain et ceux qui préfèrent le modèle britannique », affirme-t-il.


Comme les infrastructures critiques font le plus souvent déjà l'objet de réglementations dans de nombreux pays, ces types de changements peuvent causer des problèmes aux propriétaires et opérateurs, qui se trouvent confrontés à des exigences réglementaires redondantes ou contradictoires, ou à d'autres obligations officielles concernant la cybersécurité. Les cadres sont généralement plus à l'aise vis-à-vis des organismes de réglementation existants et accueillent avec méfiance ou inquiétude de nouvelles contraintes réglementaires ou des changements dans la réglementation. Ces organismes de réglementation manquent cependant souvent de compétences pointues en matière de cybersécurité.

Des spécialistes en sécurité américains du secteur de la distribution et du traitement de l'eau, par exemple, nous ont dit avoir une excellente relation avec leur organisme régulateur, l'Environmental Protection Agency, mais ils reconnaissent qu'il n'est pas réaliste de s'attendre à les voir réglementer aussi la cybersécurité. « Il est impossible que l'EPA puisse avoir un quelconque pouvoir de réglementation sur la cyberinfrastructure du pays », déclare l'un d'eux.

L'existence ou la création de plusieurs agences disposant d'autorité réglementaire, de pouvoirs d'investigation ou de responsabilités en termes de cybersécurité peut également entraîner des frictions bureaucratiques au sein de l'administration publique.

Par exemple, Kimberly Zenz affirme que les conflits de territoire sur la question de la cybersécurité font rage à Moscou. « Il existe énormément de luttes intestines au sein des organes gouvernementaux russes. Les sujets de querelle ne manquent pas. Tous les organes fédéraux, même au sein d'un ministère, sont divisés par un conflit permanent. »

Aux Etats-Unis, les frictions au sein de l'exécutif sont reflétées et amplifiées par les conflits entre les comités de contrôle du Congrès. « Capitol Hill ignore tout des problèmes de cybersécurité aux Etats-Unis », déclare l'ancien responsable du ministère de l'Energie, Christopher Campione. « Il se produit un phénomène d'enlisement », ajoute-t-il, concluant que l'origine du problème est la manière dont l'administration reçoit ses fonds. « Si, en tant que législateur, vous (allouez des fonds) au bureau du directeur informatique central (d'une agence), l'argent va finir à Washington, ou du moins il finira par être dépensé par des gens à Washington. Si vous octroyez de l'argent à un sous-département quelconque, alors il finit sa course en Virginie... ou à Pittsburgh ou peu importe, enfin à l'endroit où vous souhaitez qu'il aille », déclare M. Campione.

« Au Congrès, les dépenses sont largement motivées par des considérations géographiques. » Il ajoute que « c'est pour cette raison que toutes ces administrations ont tant de mal à consolider leurs systèmes informatiques ».

### Le partage d'informations semble mieux fonctionner horizontalement

D'après les cadres dirigeants, les niveaux de participation sont plus élevés dans les structures de partage d'informations intersectorielles plus horizontales, bien que selon les pays, les types d'organisation et les niveaux de participation divergent.

Le partage d'informations entre éditeurs de logiciels de sécurité, par exemple, « a fait d'énormes progrès, franchissant des obstacles tels que la méfiance mutuelle, (les problèmes juridiques de propriété intellectuelle) ou les questions de concurrence », explique Phyllis Schneck de McAfee. Elle affirme que les différents acteurs du secteur « collaborent efficacement (...) particulièrement dans un contexte de crise ».

Une variété d'approches encore plus grande caractérise l'organisation des forums de partage d'informations entre pouvoirs publics et secteur privé, et il existe une grande variation entre nations en termes de taux de participation. Mais ici, du moins au cours des entretiens, nous avons pu dégager une doléance commune : les autorités sont peu enclines à partager des informations sensibles concernant les menaces et les vulnérabilités.

Le responsable de la sécurité d'un grand opérateur de télécommunications déclare que sa société entretient des relations avec les forces de l'ordre de plus d'une centaine de pays où elle est active. Toutefois, lorsqu'il faut partager des informations de sécurité concernant l'infrastructure nationale critique, « (je ne reçois jamais) des informations aussi complètes que je le souhaiterais. J'attends des autorités qu'elles nous éclairent sur ce que nous ne pouvons pas obtenir par ailleurs : des renseignements précis sur la nature des menaces, des indications sur les domaines où nous pourrions mieux exploiter nos ressources, sur la base d'une analyse plus détaillée des menaces que ce dont nous sommes capables. Ils ne manquent pourtant pas de services de sécurité et d'autres types d'outils. »

Or, c'est exactement le type d'information que les pouvoirs publics gardent le plus jalousement, en partie parce qu'ils ne voient pas vraiment comment partager en toute fiabilité les renseignements avec les propriétaires et opérateurs d'infrastructures critiques sans les divulguer aussi à leurs adversaires.

Pour cette raison, les niveaux de participation élevés dans les organismes de partage d'information sous la houlette des pouvoirs publics ne sont probablement pas un indicateur fiable de leur réussite. Certains pays adoptent clairement une approche plus exclusive du partage d'informations que d'autres.

### Secret et sécurité

« Aux Etats-Unis et en Europe, un peu plus d'efforts sont consentis » par les organismes pour partager des informations, selon ce responsable de la sécurité, « mais au moment où il s'agit de recevoir des renseignements vraiment utiles de la part des autorités, tels que des avertissements ou des conseils quant à l'usage des ressources, nous ne recevons rien, d'aucun gouvernement ». Aux Etats-Unis, où les cadres signalent une participation supérieure à la moyenne dans des groupes de partage d'informations avec les autorités, des initiatives ont été prises pour résoudre ces problèmes, par l'octroi de droits d'accès spéciaux à certains dirigeants de secteurs critiques, mais les progrès en la matière sont inégaux.

« Une ou deux personnes (dans une entreprise donnée) bénéficient d'autorisations spéciales », signale M. Campione, « mais ces personnes ne sont pas forcément les plus pertinentes ». Ces autorisations doivent-elles être octroyées à un cadre supérieur, qui ne disposera peut-être pas des compétences techniques nécessaires pour interpréter les informations qui lui ont été communiquées? Ou vont-elles à un collaborateur plus expérimenté techniquement mais à un échelon inférieur de la hiérarchie, qui ne bénéficie sans doute pas de l'autorité requise pour gérer des problèmes qu'il ne peut pas révéler à d'autres ?

Une autre approche, prônée par Pamela Warren de McAfee, est de rendre accessibles davantage d'informations à un niveau « sensible mais pas top secret », des informations qui « pourraient être partagées parmi les membres d'une communauté de confiance », y compris avec ceux dépourvus d'autorisations officielles. « Le problème vient en partie du fait que nous gardons trop de renseignements secrets », affirme l'ancien haut fonctionnaire du ministère de l'Energie.

En Australie, le cadre en sécurité Ajoy Ghosh affirme que le nouveau Centre d'opérations pour la cybersécurité allait avoir une capacité opérationnelle, la faculté de « tâter du terrain » aux côtés des propriétaires et opérateurs d'infrastructures critiques. Aux Etats-Unis, par contre, les agences favorisent une approche plus axée sur l'établissement de normes.

En Chine, on relève une relation exceptionnellement proche entre les secteurs d'activité critiques et l'Etat.

En Russie, selon Kimberly Zenz, les pouvoirs publics optent pour une approche plus informelle. Bien qu'il n'existe pas de plan national de cyberexercice et peu de dispositions institutionnelles en matière de partage d'informations ou de partenariats, certains fonctionnaires publics « entretiennent des relations très étroites avec les fournisseurs d'accès Internet (...) et parmi ceux-ci, certains ont des connaissances très pointues en matière de réseaux » et leur tiennent lieu de sources d'informations, selon elle.

En Chine, on relève une relation exceptionnellement proche entre les secteurs privé et public, au vu des niveaux élevés de participation et d'approbation vis-à-vis des initiatives instiguées par les pouvoirs publics révélés par l'enquête. Le général Hayden fait remarquer que la Chine étant « un pays plus autoritaire, il est probablement plus aisé pour eux d'adopter cette attitude (...) Sans doute que la population est plus habituée aux exigences que pose la sécurité (...) au vu de tous les aspects de la vie et de la culture chinoises », et du fait que l'emploi d'Internet, même s'il est important et en croissance, est encore largement réservé à « une très petite fraction privilégiée » de la population.

La difficulté d'une collaboration efficace avec les acteurs des divers secteurs économiques est encore accentuée par la nature très mouvante des menaces. Un spécialiste de la sécurité dans le secteur du transport nous explique : « la valeur de l'expertise opérationnelle chute rapidement (une fois qu'un cadre rejoint) l'administration. C'est un problème majeur auquel est confronté le secteur lorsqu'il doit composer avec les différentes agences dont il relève. »

De fait, le même problème mine les efforts visant à ouvrir avec le grand public un dialogue réaliste sur la sécurité. Les débats publics sur les questions de sécurité sont toujours délicats, mais ils sont particulièrement épineux dans le cyberdomaine, avance le général Hayden. « Vous faites un ou deux pas en avant et c'est 95 % du public qui est distancé du point de vue technologique (...) puis les partisans de la protection de la vie privée interviennent et, tout à coup, le dialogue devient très difficile... Culturellement, c'est très compliqué pour nous. »

**Conclusion**

L'enquête montre que les réseaux informatiques, particulièrement les réseaux IP, sont désormais essentiels pour les propriétaires et opérateurs d'infrastructures critiques. Dans le climat économique actuel, ces propriétaires et opérateurs, qui recourent à l'informatique pour une meilleure efficience, seront de plus en plus dépendants vis-à-vis des réseaux, tant en ce qui concerne les systèmes opérationnels que les systèmes d'administration. Les données recueillies par l'enquête et les entretiens montrent que ces systèmes critiques (y compris ceux de nature opérationnelle comme les systèmes SCADA/ICS) fonctionnent dans un environnement à hauts risques et sont confrontés à une longue série de menaces, qui peuvent parfois être assorties de coûts exorbitants. Toutefois, ces données suggèrent également que de nombreuses initiatives peuvent être prises pour les protéger, notamment par l'adoption plus large de mesures de sécurité essentielles.

Si le cyberespace est le Far West, il est temps que le shérif se réveille. Les questions de gouvernance sont au centre de tous les débats sur la sécurité des réseaux dans le cadre des infrastructures critiques. Les commentaires n'ont pas manqué, par exemple sur les obstacles juridiques à l'emploi plus répandu de certaines mesures techniques pour contrer les attaques par déni de service distribué. Les experts ont également évoqué les difficultés qui attendent les traités et les autres initiatives dans ce domaine.

Pour les propriétaires et opérateurs, selon l'enquête, la relation qu'ils entretiennent avec les pouvoirs publics est un facteur déterminant sur leur gestion de la sécurité. Pour les pouvoirs publics, cette relation est cruciale pour la défense du patrimoine national. En l'absence d'une solution technologique miracle, de nombreux cadres dirigeants voient la réglementation, malgré ses inconvénients, comme un moyen de renforcer la sécurité. Et au-delà de la simple réglementation, l'enquête indique que dans certains pays, dont la Chine est l'exemple le plus frappant, un lien étroit entre les pouvoirs publics et les propriétaires et opérateurs contribue à l'amélioration de la sécurité.

# Remerciements

Les chercheurs et auteurs du CSIS ont eu des entretiens formels et informels avec des dizaines de personnes dans le cadre de leur analyse de l'énorme quantité de données rassemblées pour les besoins de ce rapport. Un grand nombre d'entre elles ont accepté d'être interrogées et citées officiellement, mais certaines ont refusé que l'on mentionne leur nom, même dans les remerciements où elles ne pouvaient pas être liées directement à l'un ou l'autre propos. Nous sommes éminemment reconnaissants à toutes les personnes, qu'elles soient citées ou anonymes, qui nous ont fait si généreusement don de leur temps et de leurs avis compétents. Nous remercions tout particulièrement James Lewis pour ses conseils et Denise Zheng, qui a gardé le projet sur les rails. Bien évidemment, les auteurs sont pleinement responsables de toutes erreurs ou omissions.

Stewart Baker, membre invité distingué du CSIS, partenaire chez Steptoe & Johnson

Shaun Waterman, chercheur et rédacteur pour le CSIS

George Ivanov, chercheur auprès du CSIS

**Michael Assante**
Vice-président et directeur de la sécurité,
North American Electric Reliability Corporation

**David Aucsmith**
Directeur, Microsoft Institute for
Advanced Technology in Governments

**Christopher « Rocky » Campione**
Ancien haut responsable de la cybersécurité,
ministère américain de l'Energie

**John Carlson**
Vice-président directeur, BITS,
division de Financial Services Roundtable

**Claudia Copeland**
Spécialiste en ressources et politique environnementale,
Congressional Research Service

**Dan Corcoran**
Responsable de la sécurité des informations de groupe,
division Consumer Group d'Intuit

**Kristen Dennison**
Analyste en renseignements sur les menaces, iDefense Labs

**Ajoy Ghosh**
Cadre dirigeant en sécurité auprès de Logica et chargé de cours sur la cybercriminalité à l'University of Technology, Sidney

**Général Michael Hayden** (à la retraite)
Ancien directeur de la CIA (Central Intelligence Agency) ;
ancien adjoint du Directeur du renseignement national ;
ancien directeur de la NSA (National Security Agency)

**Rick Howard**
Directeur des renseignements sur la sécurité, iDefense Labs

**Aaron Levy**
Directeur de la stratégie de sécurité,
Association of Metropolitan Water Agencies

**Anchises De Paula**
Analyste en renseignements sur les menaces, iDefense Labs, Brésil

**Karl Rauscher**
Membre distingué de l'EastWest Institute ; membre de Bell Labs

**Adam Rice**
Directeur de la sécurité à l'international, Tata Communications

**Phyllis Schneck**
Vice-Présidente de la division Threat Intelligence, McAfee ;
membre de la Commission sur la cybersécurité du CSIS pour la 44e Présidence des Etats-Unis

**Paul Smocer**
Vice-président, BITS, division de Financial Services Roundtable

**Pamela Warren**
Stratégiste en cybercriminalité, directrice d'initiatives entre le secteur public et le secteur des télécommunications, McAfee

**Tom Wills**
Financial Services Information Sharing and Analysis Center et iDefense Labs

**Kimberly Zenz**
Analyste en renseignements sur les menaces, iDefense Labs

**Notes**

1 L'enquête a été menée en septembre 2009 par la société d'études de marché britannique Vanson Bourne, Ltd. Les répondants sont issus de panels de cadres informatiques que la société organise dans différents secteurs et pays dans le cadre de ses recherches. Parmi les 600 personnes interrogées, 100 résidaient aux Etats-Unis ; 50 résidaient au Japon, en Chine, en Allemagne, en France, au Royaume-Uni et en Italie ; 30 en Russie, en Espagne, en Australie, au Brésil, au Mexique et en Inde ; 20 en Arabie saoudite. Les secteurs d'activité les mieux représentés étaient la banque et la finance ainsi que la fonction publique, avec 145 répondants dans chaque catégorie. Le plus petit nombre de répondants, avec seulement 23 sur 600, relevait du secteur de la distribution et du traitement des eaux usées. D'autres secteurs (pétrole/gaz, énergie/électricité, transports/transports en commun et télécommunications) comptaient de 59 à 82 répondants.

Au vu de la taille de l'échantillon, nous avons tiré des conclusions sur les tendances et les variations entre les divers secteurs et entre les divers pays, mais pas concernant les secteurs au sein des pays.

Lorsque les questions se sont adressées uniquement aux personnes ayant des responsabilités au niveau des systèmes opérationnels, 143 des 600 répondants au total, les tailles d'échantillons se sont réduites et même les variations entre pays devenaient difficiles à évaluer de manière fiable. Lorsque la prudence s'impose quant à la fiabilité des données, ce fait est signalé dans le texte.

De manière générale, nous avons essayé d'aborder lors des entretiens les éléments de données les plus surprenants et les plus intéressants mis en lumière par l'enquête. Dans les cas où les données recueilles à l'occasion des entretiens remettent en cause les données de l'enquête ou en suggèrent une interprétation différente, cela est précisé.

2 Certains aspects des données relevées par l'enquête auprès des répondants russes ne correspondaient pas à ce que nous apprenions lors des entretiens. Ainsi, seuls 30 % des cadres dirigeants russes rendaient compte d'attaques par déni de service distribué à grande échelle, avec 3 % seulement subissant des attaques multiples tous les mois — le taux le plus bas de toutes les nations. « Les attaques par déni de service distribué représentent un réel problème en Russie », affirme Kimberly Zenz, spécialiste russe auprès d'iDefense Labs. « Tout le monde se fait attaquer, c'est si facile de louer un réseau de robots là-bas ! ». Mme Zenz affirme que les attaques contre les sites web de concurrents, même entre des points de vente locaux dans des petites villes, sont légion. Le secteur des services financiers est souvent pris pour cible dans le cadre d'attaques par déni de service distribué et de tentatives d'extorsion, ajoute-t-elle.

Cette anomalie apparente dans les données peut être due en partie à la formulation de la question. Elle prenait comme exemple d'attaques à grande échelle les campagnes de déni de service distribué contre l'Estonie et la Géorgie, des attaques qui ont été largement imputées à la Russie. Cela peut avoir eu une incidence sur les réponses des répondants russes. Toutefois, à la question portant sur les attaques par déni de service distribué « de bas niveau », sans référence à l'Estonie ou à la Géorgie, 73 % des Russes ont affirmé avoir subi des attaques, un chiffre qui correspond nettement mieux aux données de l'ensemble des répondants (72 %).

## Les auteurs

Stewart Baker est membre invité distingué du CSIS (Center for Strategic and International Studies) et partenaire au sein du cabinet d'avocats Steptoe & Johnson de Washington. De 2005 à 2009, il a été sous-secrétaire aux affaires politiques au sein du ministère américain de la Sécurité intérieure. Avant cela, il a été avocat-conseil de la commission Silverman-Robb, chargée d'enquêter sur les manquements des services de renseignements américains concernant les armes de destruction massive irakiennes. De 1992 à 1994, il a été avocat-conseil pour la NSA (National Security Agency).

Journaliste et consultant pour les questions de sécurité intérieure et de terrorisme, Shaun Waterman a été engagé par le CSIS pour réaliser cette enquête et en rédiger le rapport. Actuellement journaliste free-lance pour le Washington Times et d'autres journaux et magazines, il a été, de 2000 à 2009, correspondant et rédacteur en chef de l'agence de presse United Press International à Washington.

George Ivanov est chercheur au sein du CSIS. Il est titulaire d'une maîtrise en sciences internationales et politique technologique de la George Washington University.

Pour plus d'informations sur le CSIS, visitez son site à l'adresse :
www.csis.org

## A propos de McAfee

Basé à Santa Clara en Californie, McAfee, Inc. est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. McAfee consacre tous ses efforts à trouver des réponses aux plus grands défis de sécurité de notre époque. A cette fin, notre société fournit dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes et des réseaux et permettent aux utilisateurs de se connecter, de surfer ou d'effectuer leurs achats sur Internet en toute sécurité. Avec le soutien d'une équipe de recherche saluée par de nombreux prix, McAfee crée des produits innovants à l'intention des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses.

Pour plus d'informations, visitez notre site à l'adresse :
www.mcafee.com/fr

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr



7795rpt_cip_0110