LA FRANCE FACE À LA MONTÉE DE LA CYBERCRIMINALITÉ

Avec l'essor des technologies numériques, la France est confrontée à une augmentation des cyberattaques visant ses infrastructures critiques, telles que les hôpitaux, les systèmes de transport et les réseaux énergétiques. Les cybercriminels utilisent des techniques de plus en plus sophistiquées pour perturber les services essentiels et compromettre la sécurité nationale.

La cybercriminalité se définit comme l'ensemble des infractions criminelles menées au moyen des réseaux informatiques ou d'Internet, visant à accéder illégalement à des données, à manipuler des systèmes ou à réaliser des actes frauduleux. Elle englobe des pratiques variées, telles que le vol de données personnelles, le piratage de systèmes informatiques, les attaques par rançongiciel et la fraude en ligne. Ce phénomène représente un enjeu majeur pour la sécurité numérique et la protection des informations, tant pour les institutions publiques que pour les entreprises et les particuliers. Quant à la cybersécurité, c'est l'ensemble des pratiques, technologies et processus visant à protéger les systèmes informatiques, les réseaux et les données contre les accès non autorisés, les attaques malveillantes et les dommages. Elle comprend la gestion des risques, la mise en œuvre de mesures de protection et la détection d'intrusions afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations dans le cyberespace. Elle est cruciale pour préserver la confiance dans les infrastructures numériques des gouvernements, des entreprises et des individus. Tel est l'enjeu du sujet de notre espèce.

Cet article a le mérite de mettre l'accent sur les types de menaces actuelles et les stratégies instaurées pour renforcer la cybersécurité des infrastructures vitales sur le territoire français.

À la lumière de tout ce qui précède, il convient d'analyser d'une part, les menaces croissantes sur les infrastructures critiques (I) et d'autre part, les mesures de protection à leur profit (II).

I-LES MENACES CROISSANTES SUR LES INFRASTRUCTURES CRITIQUES

En France, ces menaces s'expliquent par diverses attaques avec des exemples à l'appui (A) et qui, par la suite, vont engendrer des conséquences pour la sécurité nationale (B).

A-TYPES DE CYBERATTAQUES ET EXEMPLES DE CIBLES EN FRANCE

Dans le cas d'espèce, on a trois types de cyberattaques avec des exemples qui sont :

- D'abord, ***le ransomware et la paralysie des hôpitaux*** : En 2021, l'hôpital de Dax et plusieurs autres établissements de santé ont été victimes d'attaques par ransomware, où les données ont été chiffrées et les services bloqués. Ces incidents ont obligé les hôpitaux à rediriger les patients et à revenir temporairement à des méthodes papier pour le suivi des soins, perturbant gravement les soins médicaux.
- Ensuite, ***les attaques sur le secteur énergétique*** : En 2022, le gestionnaire de réseau électrique Enedis a été ciblé par des attaques visant à compromettre le système de distribution électrique. Bien que la sécurité des données n'ait pas été compromise, cet incident montre à quel point ce secteur reste une cible privilégiée, car une coupure de courant pourrait paralyser une région entière et affecter les entreprises et les foyers.
- Enfin, ***la piraterie des réseaux de transport*** : Les réseaux de transports publics, notamment ceux des grandes villes comme **Paris**, sont également à risque. En 2023, un incident touchant les systèmes de billetterie de la RATP a montré que le secteur du transport est vulnérable aux cyberattaques qui perturbent le service et affectent des milliers de voyageurs.

Des faits qui auront un impact sur la sécurité nationale en question.

B-LES CONSÉQUENCES POUR LA SÉCURITÉ NATIONALE

Comme conséquences, on a :

- ***Les menaces sur la continuité des services publics*** : c'est-à-dire que les cyberattaques visant les infrastructures critiques peuvent perturber des services essentiels, ce qui peut par la suite, mettre en danger la vie des citoyens, comme cela a été le cas avec les attaques contre les hôpitaux. En bloquant les données, les attaquants risquent d'empêcher l'accès rapide aux informations médicales, retardant des interventions urgentes.

- ***Le piratage de données personnelles*** : Les hôpitaux et les infrastructures de santé, par exemple, gèrent des millions de données sensibles. Une faille de sécurité pourrait permettre le vol de données de santé, exposant les patients à des risques de fraude ou de violation de la vie privée. Question très critique dans un contexte où les systèmes de santé sont déjà sous pression.

- ***L'impact économique*** : Il faut noter que les cyberattaques ont aussi un coût économique colossal. Par exemple, les ransomwares nécessitent souvent de longues périodes de récupération et des investissements en sécurité pour éviter les incidents futurs. En 2021, les coûts associés aux attaques sur les hôpitaux français ont été estimés à plusieurs millions d'euros en réparation, formation et sécurisation.

Dans le but de lutter contre la cybercriminalité en renforçant la sécurité nationale, des dispositifs de protection de ces infrastructures vitales sont élaborés à l'initiative du privé et du public.

II-LES MESURES DE PROTECTION DES INFRASTRUCTURES CRITIQUES

Ces mécanismes se traduisent non seulement par la mise en place des actions gouvernementales et des initiatives de coopération internationale (A)), mais aussi par des innovations et du renforcement de la résilience des infrastructures vitales (B).

A-LES ACTIONS GOUVERNEMENTALES ET INITIATIVES DE COOPÉRATION INTERNATIONALE

En 2021, la France a alloué un budget de près d'un milliard d'euros pour la cybersécurité dans le cadre du plan "France Relance". Cet investissement permet de renforcer la cybersécurité des administrations publiques, mais aussi de former des experts en sécurité numérique pour répondre aux besoins croissants.

Toujours dans cette même dynamique, l'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) qui pilote les réponses aux cyberattaques en France, travaille avec les secteurs public et privé pour protéger les infrastructures critiques. En 2022, elle a développé des simulations d'attaques avec les hôpitaux pour les préparer aux incidents réels.

La France collabore également avec ses voisins de l'UE pour harmoniser les normes de sécurité et partager des informations sur les menaces en temps réel. Dans le cadre du programme européen ***Cyber Shield***, les États membres travaillent ensemble pour déployer des équipes de cybersécurité capables de réagir rapidement aux incidents transnationaux.

En outre de ces actions privées/publiques, il y a eu aussi des innovations et des stratégies de renforcement contribuant à la résilience des infrastructures critiques face à la cybercriminalité.

B-LES INNOVATIONS ET LE RENFORCEMENT DE LA RÉSILIENCE DES INFRASTRUCTURES CRITIQUES

À cet effet, des entreprises comme ***Orange Cyberdefense*** et ***Thales*** mettent en œuvre des technologies avancées (l'IA et les outils d'apprentissage automatique) pour détecter les anomalies dans les systèmes critiques en temps réel. En 2023, Thales a lancé un programme de surveillance prédictive pour anticiper les comportements suspects dans les systèmes de transport et d'énergie.

Les protocoles de cybersécurité évoluent constamment pour s'adapter aux nouvelles menaces. D'où des audits de sécurité réguliers et la mise en place de systèmes de protection en couches (firewalls, détection d'intrusion, sauvegardes) qui sont désormais requis pour toutes les infrastructures critiques, c'est-à-dire les hôpitaux, l'énergie et les transports ou mobilités.

Au-delà des outils techniques, la formation des équipes est indispensable pour une sécurité efficace et efficiente. En 2023, une campagne nationale de sensibilisation aux risques cyber a été lancée pour inciter les professionnels à adopter des pratiques de sécurité rigoureuses, comme la gestion des mots de passe et l'identification des e-mails de phishing.

En somme, la cybercriminalité, posant des défis importants en matière de sécurité nationale, de protection des données sensibles et nécessitant des réponses techniques, légales et éducatives pour prévenir, détecter et réagir aux menaces, la sécurité des infrastructures critiques est un potentiel enjeu majeur pour la France, confrontée à des cyberattaques de plus en plus fréquentes et sophistiquées. Protéger ces systèmes demande donc une mobilisation continue des ressources humaines, financières et technologiques, ainsi qu'une collaboration étroite avec les partenaires européens. En renforçant la cybersécurité, la France peut non seulement protéger ses citoyens, mais aussi assurer la résilience et la continuité de ses services essentiels à long terme.

Auteur anonyme