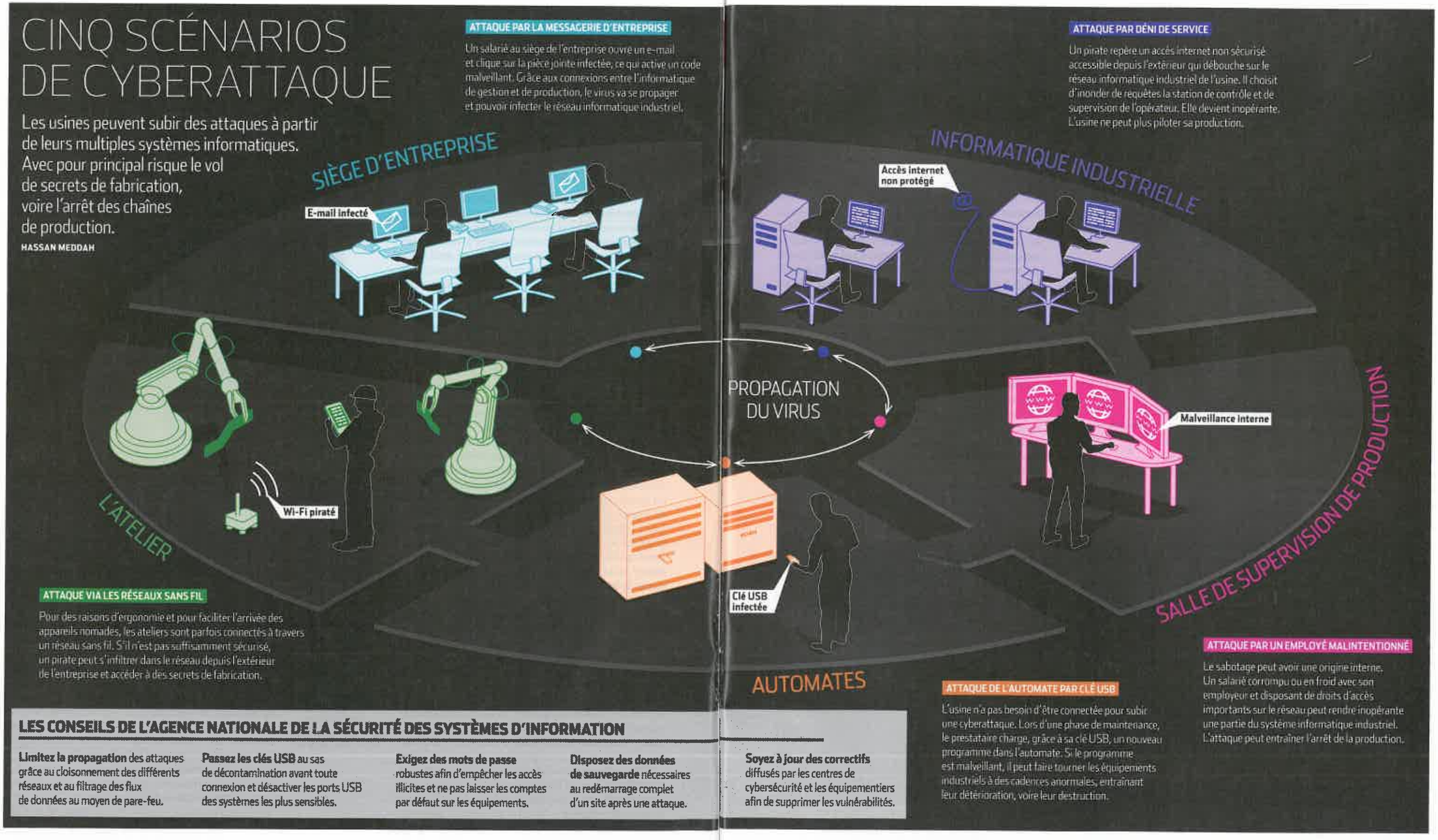
CINQ SCÉNARIOS DE CYBERATTAQUE

Les usines peuvent subir des attaques à partir de leurs multiples systèmes informatiques. Avec pour principal risque le vol de secrets de fabrication, voire l'arrêt des chaînes de production.

HASSAN MEDDAH



ATTAQUE PAR LA MESSAGERIE D'ENTREPRISE

Un salarié au siège de l'entreprise ouvre un e-mail et clique sur la pièce jointe infectée, ce qui active un code malveillant. Grâce aux connexions entre l'informatique de gestion et de production, le virus va se propager et pouvoir infecter le réseau informatique industriel.

ATTAQUE PAR DÉNI DE SERVICE

Un pirate repère un accès internet non sécurisé accessible depuis l'extérieur qui débouche sur le réseau informatique industriel de l'usine. Il choisit d'inonder de requêtes la station de contrôle et de supervision de l'opérateur. Elle devient inopérante. L'usine ne peut plus piloter sa production.

ATTAQUE VIA LES RÉSEAUX SANS FIL

Pour des raisons d'ergonomie et pour faciliter l'arrivée des appareils nomades, les ateliers sont parfois connectés à travers un réseau sans fil. S'il n'est pas suffisamment sécurisé, un pirate peut s'infiltrer dans le réseau depuis l'extérieur de l'entreprise et accéder à des secrets de fabrication.

ATTAQUE DE L'AUTOMATE PAR CLÉ USB

L'usine n'a pas besoin d'être connectée pour subir une cyberattaque. Lors d'une phase de maintenance, le prestataire charge, grâce à sa clé USB, un nouveau programme dans l'automate. Si le programme est malveillant, il peut faire tourner les équipements industriels à des cadences anormales, entraînant leur détérioration, voire leur destruction.

ATTAQUE PAR UN EMPLOYÉ MALINTENTIONNÉ

Le sabotage peut avoir une origine interne. Un salarié corrompu ou en froid avec son employeur et disposant de droits d'accès importants sur le réseau peut rendre inopérante une partie du système informatique industriel. L'attaque peut entraîner l'arrêt de la production.

LES CONSEILS DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Limitez la propagation des attaques grâce au cloisonnement des différents réseaux et au filtrage des flux de données au moyen de pare-feu.

Passez les clés USB au sas de décontamination avant toute connexion et désactiver les ports USB des systèmes les plus sensibles.

Exigez des mots de passe robustes afin d'empêcher les accès illicites et ne pas laisser les comptes par défaut sur les équipements.

Disposez des données de sauvegarde nécessaires au redémarrage complet d'un site après une attaque.

Soyez à jour des correctifs diffusés par les centres de cybersécurité et les équipementiers afin de supprimer les vulnérabilités.

INFOGRAPHIE FLORENT ROBERT POUR L'USINE NOUVELLE