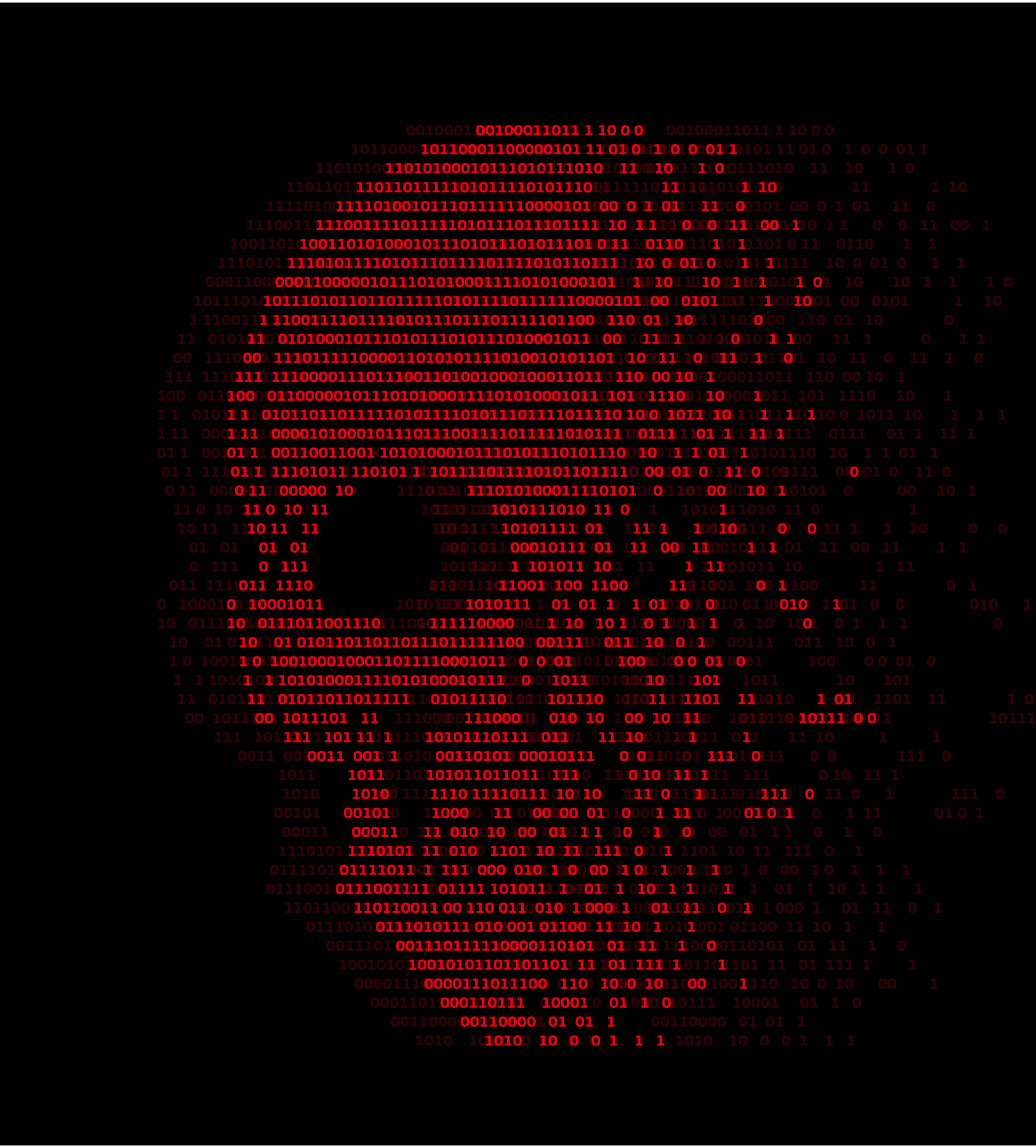

LA CYBERSÉCURITÉ

Du Bureau des Légendes au bureau

OLIVIER MELLINA-GOTTARDO (96)
secrétaire général Hub One

Aux lecteurs qui s'imagineraient encore que la cybersécurité est l'affaire de spécialistes ou de militaires, ce dossier espère faire partager la conviction que la cybersécurité doit devenir l'affaire de tous, dans tous les secteurs de la vie économique et citoyenne.

La cybercriminalité existe parce que l'innovation numérique a transformé notre environnement : nos entreprises et nos biens personnels n'ont pas attendu le numérique pour être la cible de criminels cherchant à se livrer à de l'espionnage, du sabotage, des actes de vol, de destruction ou de manipulation de l'information, etc. Mais le numérique offre simplement un moyen de plus de s'y livrer et les capacités d'attaque sont à la portée d'ingénieurs pas forcément spécialisés, formés par exemple dans nos écoles, ce qui appelle des questions d'éthique dans nos formations initiales et nos métiers.

Ce dossier, sans aucune prétention d'exhaustivité, met des coups de projecteur çà et là sur des domaines économiques où le risque cyber s'illustre : l'industrie et les usines, notamment quand elles se digitalisent et se dotent de capteurs connectés industriels et des réseaux qui les sous-tendent ; la santé face au dilemme d'un fort besoin d'e-santé, mais aussi de protection absolue des données (avec l'exemple du Service de santé des armées qui travaille sur les terrains doublement sensibles des données de défense et de santé) ; voire l'aérien où on ne peut pas complètement écarter le risque cyber dans le détournement d'aéronefs. Plus généralement, toute entreprise possédant aujourd'hui un système d'information accessible notamment à distance est exposée de fait à un risque supplémentaire (cyber) d'espionnage ou de vol de données (bases de données clients, etc.). Enfin, plus proche de notre quotidien, ce sont des objets devenus aussi courants que des maisons avec alarme connectée, des voitures, et pas forcément encore autonomes, qui portent un risque cyber.

Comment le monde économique s'organise-il ? Si les très grandes entreprises se dotent déjà de moyens de surveillance cyber comme les SOC (centres opérationnels de sécurité) et suivent les directives et recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), le paysage de la cybersécurité de demain reste à écrire, avec notamment des questions sur le rôle que l'intelligence artificielle pourra jouer dans les moyens de défense accessibles à toutes les entreprises.