L'industrie 4.0, cheval de Troie d'une cybersécurité intégrée ?

Une occasion historique à saisir

Florian MANET
Colonel de la Gendarmerie nationale
Commandant la Section de Recherches de Bretagne
Chercheur associé à la chaire de géopolitique de Rennes School of Business

L'Industrie 4.0 révolutionne la production industrielle au sein de chaînes de valeur interconnectées. Elle interroge sur la pleine maîtrise par l'homme de cet écosystème numérique complexe. Le capitaine d'industrie est-il encore maître dans son propre navire ?

Le terme d'« Industrie 4.0 » est apparu pour la première fois sous la plume du professeur Wolfgang Wahlster, directeur du Centre allemand pour la Recherche sur l'Intelligence Artificielle. Le 1er avril 2011, il publia un article intitulé *« Industry 4.0 : With the Internet of Things on the Way to Fourth Industrial Revolution »*. D'emblée, ce concept fait référence à la quatrième révolution industrielle qui repose sur la numérisation. D'où, par ailleurs, la sémantique « 4.0 » empruntée aux sciences de l'information.

Un ré-enchantement de la production par la numérisation des process ?

Dès lors, l'industrie s'est appropriée, avec succès, ce concept novateur qui, aujourd'hui, connaît des réalisations concrètes de plus en plus nombreuses. Un phénomène global de numérisation de l'espace industriel tant au niveau de la production que des process mis en œuvre a redessiné les équilibres globaux. Ainsi, il embrasse toute la chaîne de production :

- Conception du produit (usine virtuelle, continuité numérique),
- Contrôle et pilotage (automatisation des flux et des équipements : usines/lignes connectées, capteurs/Internet des Objets, logistique automatisée),
- Procédés de fabrication (machine intelligente, fabrication additive, robots collaboratifs ou cobotiques)
- Maintenance conditionnelle (*big data*, télé-maintenance),
- Organisation du travail (opérateur assisté, organisation apprenante).

La *smart industry* apparaît comme un lieu porteur de valeurs qu'il convient de partager. Mieux encore, la production elle-même s'inscrit dans un dialogue constant avec le client désireux d'obtenir un bien sur-mesure dont il peut suivre à distance la réalisation et en influer le cours à sa guise. Ce dispositif industriel est intégré dans un maillage serré d'interconnexions. L'Internet des Objets fait interagir les objets connectés, équipements ou process au sein de la chaîne de production. Plus largement, par la mise en réseau des systèmes d'information, cette *smart industry* s'insère étroitement dans l'ensemble de l'écosystème

industriel l'environnant aussi bien en amont comme en aval.

La donnée, moteur de performance collective

Oeuvre collaborative, ce processus industriel exploite les possibilités infinies qu'offrent les nouvelles technologies de l'information. À ce titre, la donnée devient le centre de gravité d'un système en recherche d'une performance accrue et d'une production centrée sur le client.

Clé de voûte, la donnée est valorisée par trois innovations majeures :
- L'informatique avancée ou décisionnelle avec les machines apprenantes, l'exploitation du *big data* et du *cloud*,
- Les objets connectés avec la possibilité de faire le lien avec des objets physiques et d'autres numériques,
- La robotique avancée avec des robots collaboratifs.

Au total, le principe d'une entité « *smart* » se fonde sur l'utilisation et l'exploitation des données et des algorithmes afin d'appliquer des processus intelligents qui pourraient, ensuite, être exécutées, évaluées et améliorées. Ces entités sont conçues *nativement* pour détenir la capacité d'apprendre et de prendre des décisions en autonomie.

Des risques 4.0, corolaires de l'interconnexion digitale ?

Cette révolution industrielle induit un changement fondamental de paradigme, source d'opportunités, mais aussi de risques émergents. La littérature explicitant le concept est prolifique. Toutefois, l'évaluation des risques liés aux technologies digitales interconnectées mérite d'être encore approfondie en décortiquant méthodiquement ce changement d'ère. Loin de ne présenter que des impacts environnementaux ou productifs, l'Industrie 4.0 génère aussi une révolution sociale au cœur des chaînes de production et d'approvisionnement. Décloisonnant l'espace industriel à l'extrême, elle contribue, malgré elle, à le rapprocher d'acteurs malveillants qui exploiteront, sans état d'âme, les opportunités offertes par ce progrès technologique. Au total, cette réorganisation industrielle suscite un nouveau modèle économique dont le maillon… fort doit demeurer l'Homme, garant de la résilience collective. À ce titre, la *smart factory* constitue une formidable opportunité pour renforcer la cybersécurité. Alors, considérons ce concept comme le cheval de Troie d'une cybernétique sécure !

Une révolution managériale en marche ?

L'Industrie 4.0 engendre une révolution managériale au sein des organisations industrielles. Pièce maîtresse, le directeur du site est à la croisée des chemins de la traditionnelle verticalité qui donne du sens à l'action et d'une horizontalité de plus en plus prégnante qui souligne la dimension collaborative de la chaîne de production intelligente. Ce contexte exige un niveau élevé de compréhension des mécanismes digitaux et de leurs impacts sur la production industrielle. Pour ce faire, le dirigeant s'appuie sur des fonctions support ou expertes telles le *Chief Digital Officier* (CDO). Responsable de la transformation numérique, le directeur du digital produit des études d'impact sur les nouvelles technologies et sur leur adaptation aux besoins. Il supervise la bonne mise en œuvre de la stratégie numérique et de sa coordination avec la stratégie globale de l'entreprise. Par ailleurs, il veille à la cohérence des interconnexions établies par les acteurs du site avec l'écosystème. Il s'efforce d'anticiper les risques et de construire des plans de continuité d'activités adaptées aux scénarii de crise. Dans les faits, il s'en suit un partage du pouvoir entre le directeur et le CDO. La complémentarité et la qualité des relations entre ces deux figures essentielles conditionnent la réussite globale de l'entreprise. Affectant les relations managériales, cette révolution s'accompagne corrélativement d'un effort essentiel de communication et de partage avec l'ensemble des collaborateurs qu'il faut embarquer dans ce tout numérique.

De plus, la *smart factory* suppose une très forte agilité des salariés, acteurs essentiels du dialogue Homme-Machine et Machine-Machine. L'enjeu majeur est aussi la constitution d'une ressource humaine hautement qualifiée et la qualité d'une formation continue, incluant une forte dimension de cybersécurité. L'effort de formation est capital pour la conduite des projets industriels. En effet, l'homme reste au cœur d'un système complexe : il donne du sens et de la cohérence aux données collectées. Son esprit d'analyse facilite la prise de décision. Mais, avouons-le, il demeure un maillon fragile susceptible de contribuer, bien souvent malgré lui, à la compromission des systèmes numériques.

La cybercriminalité, valeur dominante du portefeuille risque

À l'avenir, les gestionnaires de risque auront un portefeuille où le volet cyber prédominera. Au-delà des atteintes physiques sur les collaborateurs et sur les infrastructures. En retour, cette tendance est susceptible d'impacter les solutions d'assurance face à des évènements de sureté caractérisés par un préjudice exceptionnel. Cristallisant les enjeux de souveraineté, la valeur de la donnée épouse le contour de la nécessaire maîtrise de son identité personnelle, de la propriété intellectuelle et du savoir-faire sans négliger la réputation de l'entreprise. Le montant des rançons exigées par des cybercriminels est illustratif des réalités d'un capitalisme criminel dont l'enjeu contemporain semble être la souveraineté de la donnée quelle qu'elle soit.

Le spectre du cyber-chaos, horizon inéluctable ?

Peu importe le mode opératoire, l'effet produit se traduit immanquablement sous la forme d'un déni de service. La ligne de production est arrêtée, les serveurs de *control and command* ne sont plus opérants, le fichier clients ou la dernière innovation ont disparu. Fruit d'une interconnexion recherchée à dessein, cet écosystème interdépendant peut se trouver amputé et perturbé. Le rançongiciel NOT PETYA est illustratif des effets produits sur la logistique mondiale et du caractère irrémédiable d'un tel déni de service opéré sur 50 000 terminaux portuaires contraints à une reprise manuelle sur 600 sites répartis dans 130 pays. Les pertes directes supportées par l'opérateur s'élèvent à plus de 300 millions de dollars. Quel est le montant global de la facture pour l'ensemble des victimes collatérales de ce dérèglement logistique ?

Une Sagesse 4.0 ?

Cette quatrième révolution industrielle revêt des impacts socio-économiques, organisationnels, juridiques et sécuritaires. Source d'innovations, elle invite, avant tout, à promouvoir une approche intégrée au sein des organisations interconnectées. Dans ce contexte de complexification des chaînes de production, les capacités humaines peuvent être dépassées et inaptes à saisir les facteurs pertinents dans l'action ainsi que dans la prise de décision. Ainsi, le danger majeur pourrait provenir d'une confiance absolue dans la technologie sans en identifier les limites et vulnérabilités. Cette situation invite à un partage d'expérience avec d'autres secteurs d'activité complexe tels le nucléaire, la pétrochimie ou l'aviation qui sont, eux aussi, confrontés à des problèmes de performance humaine. Au fil des expériences, ils ont développé des méthodes d'analyse et des protocoles de prise de décision raisonnée dans le cadre d'une gestion intégrée des risques. L'homme y a toute sa place.

Finalement, l'Industrie 4.0 est en soi une Sagesse.

Les opinions exprimées ci-après sont celles de son auteur. Elles n'engagent aucunement la Gendarmerie nationale.