Comment un projet d'envergure tel que le Smart Port City contribue au développement d'un territoire numérique de confiance ?

Intervention de Jean-Marie Dumon, Délégué Général adjoint du GICAN

Tout d'abord, laissez-moi vous exprimer la joie de retrouver, même virtuellement, le ***monde portuaire***. C'est un ***lieu d'enjeux majeurs pour notre pays*** et j'ai pu le mesurer tout au long de ma vie professionnelle en tant :

- Qu'ancien marin et hydrographe, donc praticien des ports mondiaux,
- Qu'ancien président de la Grande Commission Nautique donc ayant accompagné les projets de développements associés de vos espaces,
- Au cours de mes années au MEDEF aussi, au plus près des territoires, et valorisant le dynamisme des entreprises portuaires,
- Et bien entendu actuellement au GICAN, pour soutenir au quotidien l'industrie navale dans toutes ses dimensions.

La question qui est posée renvoie à la ***notion de « territoire de confiance ».*** Ce vocable recouvre ***un des 5 projets fédérateurs majeurs de la filière des industries de la sécurité***, telle que dénommée au sein du Conseil National de l'Industrie. Le GICAN en est un des membres fondateurs, du fait de son implication historique au sein du Conseil des Industries de la Confiance et de la Sécurité (CICS). Nous avons, avec d'autres, la paternité de cette notion que nous avons imposée au CICS en substitut du seul vocable de Smart City. Et nous militons pour exprimer le fait que ***le secteur maritime et portuaire est mâture en matière de cybersécurité*** et porte des projets pilotes particulièrement démonstratifs pour les enjeux de filière.
Pourquoi « territoire de confiance » ? Parce que ***cette notion de territoire élargit le concept, lui restitue sa dynamique, sa logique de flux, d'espaces successifs et hétérogènes*** et oblige à réfléchir depuis le large dans ses trois dimensions jusqu'à l'Hinterland le plus éloigné.
Je crois que votre ambition, au Havre, est bien celle-ci, et se veut une ***approche globale du « smart and secure ».***
Ce qui nous rassemble avec le GICAN, c'est bien entendu ***le navire***, qui est et doit rester ***au centre de la démarche*** sous peine de manquer de pertinence.
En fait, nous sommes passés d'une situation où nous pensions que les cyberattaques ne concernaient pas les navires, puisqu'ils étaient faits pour être en mer, couper du lien terrestre, que l'impact économique pour les armateurs ou assureurs était considéré comme négligeable et que seuls les navires militaires méritaient que l'on s'occupe de leur sort mais dans une dimension d'agression ou de réponse dans un environnement de cyberguerre haut du spectre et centrée sur des points névralgiques.
Tout cela appartient au passé, nous le savons. ***Le cyberespace s'est densifié et l'hyperconnectivité s'accroit à bord des navires et à terre***, avec une logique similaire. Cette explosion de systèmes collaboratifs a complexifié les réponses cyber et démultiplié les angles d'attaque.
Après avoir mis au centre du débat le navire, il faut y adjoindre la ***digitalisation croissante des activités***. De ce point de vue, un chantier naval figure parmi les activités industrielles les plus complexes à gérer et fait face à cette réalité.

La réponse est de s'engager résolument vers l'industrie du futur avec deux marqueurs :

- ***La mise en place d'un jumeau numérique*** utile dans toutes les phases de conception, d'utilisation, de maintenance et de gestion du navire
- L***a cybersécurisation et le cybermanagement de ce jumeau dès le design***.

Les ***entreprises du secteur naval*** sont donc devenues de plus en plus des ***productrices de solutions cyber*** adaptées au monde maritime, tout en étant des entités très ***consommatrices de solutions cyber pour protéger leurs activités***. Ces entreprises sont établies au sein d'***écosystèmes portuaires***, et donc intègrent nativement cette dimension. Le fait que certains ports ne possèdent pas de chantiers navals d'importance ne remet pas en cause la très bonne perception des enjeux cyber portuaires par nos entreprises. ***Le dialogue avec les armateurs et les assureurs*** est aussi essentiel car les conséquences économiques des attaques cyber sont de plus en plus lourdes et ont des effets systémiques délétères. Il faut passer d'une logique d'un coût cyber à celui d'un profit grâce à la cyber.

Le ***GICAN*** joue son rôle d'engagement sur le sujet cybermaritime, comme je l'ai déjà exprimé, au travers de la stratégie des filières industrielles (Sécurité et Mer), des actions dès la première heure qu'il mène au sein du comité France Maritime, en tant que ***pilier du conseil cyber du monde maritime (C2M2)***, siège de la gouvernance de la cybersécurité, au côté des acteurs portuaires et de l'Etat.

Le GICAN se réjouit de la naissance de l'Association France Cyber Maritime, elle la rejoindra pour représenter le collège industriel. Le GICAN soutient le projet sous-jacent de CERT-Maritime et encourage la dimension européenne de la démarche.

Pour conclure, le projet Smart Port City nous parle.

Il met l'innovation en avant et nous considérons que c'est une priorité car les offres attractives de solutions ne peuvent exister si l'on ne consacre pas suffisamment à l'innovation pour renouveler et développer. Le raccourcissement des cycles impose une réactivité grandissante en la matière.

La transformation et l'accompagnement du changement ne doivent pas être négligés et vous l'avez bien en tête. C'est particulièrement utile pour les petites structures, les PME, qu'il faut convaincre, car elles ont déjà de multiples tâches à accomplir au quotidien et la prise en compte de la cyber ou la proactivité au sein de projets d'envergure ou de démarches type « smart » n'apparaissent pas forcément nécessaires pour elle.

Le besoin de fédérer et de mobiliser l'écosystème est indispensable. Nous le voyons au sein du Conseil cyber du domaine maritime et le fait que les acteurs économiques, sociaux, les collectivités et l'Etat tirent dans le même sens rend la logique de territoire pertinente.

Enfin, et ce n'est pas le moindre, ***l'importance des données (les datas) est au carrefour de votre démarche*** et rejoint notre vision de la numérisation des activités et de la prise en compte efficace de la cybersécurité.