Newsletter n°67 - 22 septembre 2023

□□ Éditorial

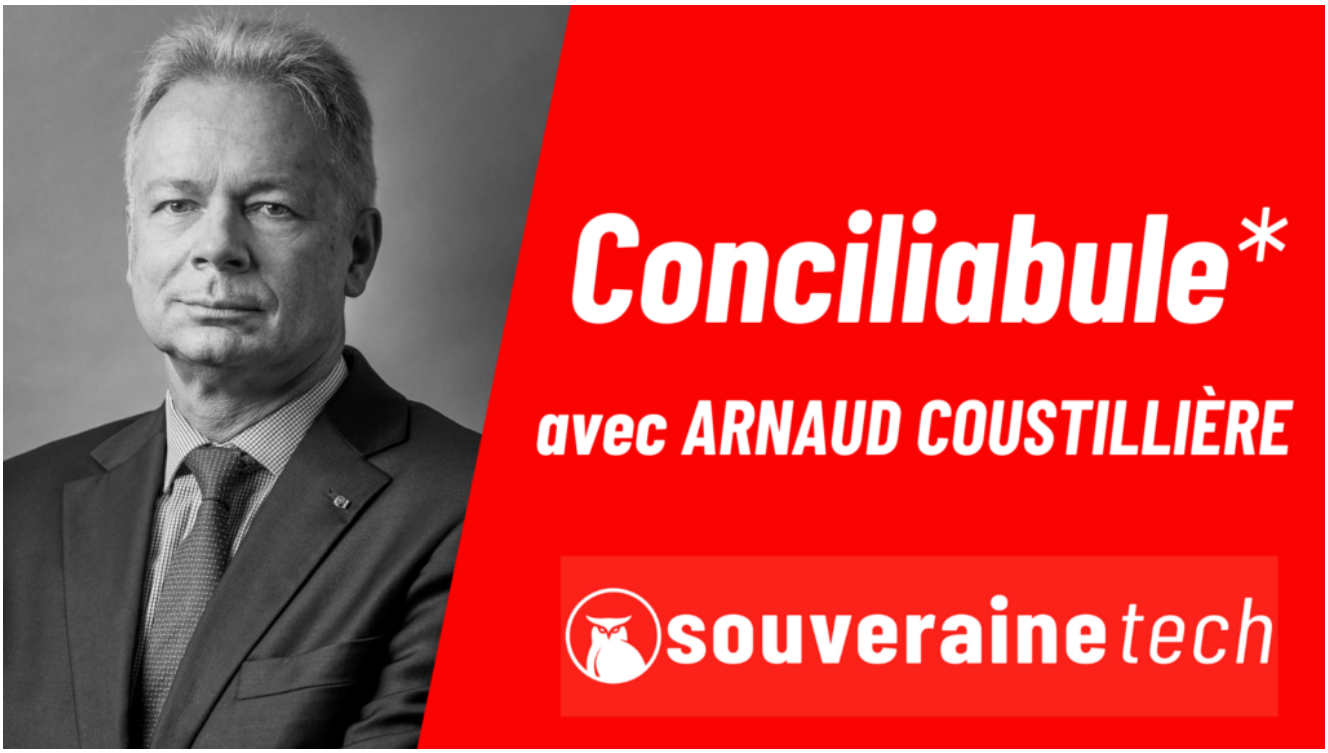
J’aurais aimé l’être

Depuis Saint-Malo, bien des agitations nationales mues par nos petits courants de pensée semblent vaines. Un vague sentiment s’en dégage comme une écume : la discorde nous empêchera d’avancer, et la discorde, chez un peuple comme le nôtre, cela ressemble furieusement à une mer d’orgueil. Je profite du fait que nous recevions aujourd’hui un marin, non pour faire des phrases*, mais pour exprimer en votre nom à tous ce besoin de grands vents pour l’intelligence française *(*ça y ressemble un peu quand même)*. Je peux le dire, parmi les vies que j’aurais aimé avoir, il y a celle de marin. Il est probable que je l’idéalise. Mais j’y devine encore aujourd’hui la possibilité d’être soi autant que l’indispensable rouage d’un ensemble efficace et rutilant. Derrière mes histoires de souveraineté technologique, et ce colloque qui arrive comme un continent dont j’approche, c’est d’abord à cela que je songe. Un orchestre mouvant et organisé, composé de joyeux drilles fiables, polis par l’effort et la discipline, ivres de concorde et de fierté, et bien décidés à s’engager…

Pardon, j’oubliais le plus important : un Pacha qu’on ait envie de suivre par gros temps.

Bertrand Leblanc-Barbedienne

Nous recevons aujourd'hui, vendredi 22 septembre 2023, le Vice-amiral d'escadre (2S) Arnaud Coustillière, qui est président du Pôle d'Excellence Cyber.



On peut comparer les grands fonds au dark web

□□ Conciliabule

Avertissement *: Souveraine Tech revendique par vocation une approche transpartisane. Seule nous oblige la défense des intérêts supérieurs de notre pays. Nous proposons ainsi un lieu de « disputatio » ouvert aux grandes figures actives de tous horizons. La parole y est naturellement libre et n'engage que ceux qui la prennent ici. Cependant, nous sommes bien conscients des enjeux en présence, et peu dupes des habiles moyens d'influence plus ou moins visibles parfois mis en œuvre, et dont tout un chacun peut faire l'objet, ici comme ailleurs. Nous tenons la capacité de discernement de notre lectorat en une telle estime que nous le laissons seul juge de l'adéquation entre le dire et l'agir de nos invités.*

NB : Arnaud Coustillière tient à préciser qu'il s'exprime ici à titre personnel et que ses propos n'engagent que lui.

1/ La moitié de l'activité numérique mondiale sera bientôt dévolue à la sécurisation de l'autre ? Que pensez-vous de cette assertion ?

Je ne sais pas dire si elle est exacte, mais elle restitue bien le contexte global de très forte augmentation du niveau de menace et de sophistication des attaques. Elle frappe les esprits et interroge les acteurs de l'IT sur leurs priorités. Comme dans le monde réel, il ne peut y avoir de développement sans confiance et sécurité.

En premier lieu, la sécurité doit être conçue « by design », intégrée dès la conception dans l'architecture, elle concerne donc tous les acteurs de la chaine IT, avec une responsabilité forte des éditeurs de logiciel, notamment des plus grands qui ont des millions d'usagers. Quand vous achetez un produit manufacturé, vous avez des organismes de certification qui garantissent la « non dangerosité » du produit. Dans le numérique on doit faire confiance à l'éditeur, y compris dans sa stratégie et tempo de mise à jour… Cet état de fait n'est pas très vertueux… et fait reposer la sécurité by design sur les éditeurs privés, motivés souvent par d'autres priorités que la sécurité. C'est l'origine de tous les débats actuels autour de la « supply chain » qui est devenue un maillon faible. L'Appel de Paris lancé par la France en 2018 pointe bien ce point, tout comme le CIGREF qui représente les plus grandes entreprises françaises utilisatrices. Même si la situation n'est pas satisfaisante, les éditeurs comme les utilisateurs en sont de plus en plus conscients et deviennent plus exigeants ; la règlementation elle aussi évolue.

En second lieu, il y a la chaine Cyber en charge d'anticiper, de détecter, de corriger et de réagir face aux attaques ; il est vrai que face à une menace qui devient de plus en plus «

industrielle » elle est amenée à de plus en plus se renforcer, à la fois en personnel qualifié avec de nouveaux métiers, mais aussi par le recours accru à de l'automatisation et l'emploi de big data, d'OSINT, d'IA, prochainement de puissances de calcul démultipliées par le quantique, pour traquer la menace le plus en amont possible, mais aussi au cœur des systèmes à protéger.

Les deux points clefs pour moi sont les places respectives entre des « actions humaines à forte valeur ajoutée » versus une « automatisation accrue pour traiter tout le reste ».

2/ Quel rôle la Bretagne joue-t-elle vis-à-vis de Paris dans la course à l' »excellence cyber » ? Voyez-vous une place particulière pour Saint-Malo, notamment au regard de son histoire ?

En 2013/14 vous avez eu la rencontre de deux politiques publiques qui ont propulsé la Bretagne au cœur du cyber régalien, loin devant les autres régions.

La première est liée aux suites du Livre blanc sur la sécurité et la défense nationales de 2008, puis celui de 2013, ils ont conduit à un très fort renforcement des structures cyber du ministère des Armées en Bretagne. L'écosystème breton historiquement fortement marqué par les Télécom y offrait un terreau favorable, avec en sus une concentration à DGA/MI (Bruz) des compétences les plus pointues du ministère dans le domaine numérique. Assez naturellement, le ministère des armées a poursuivi et fortement renforcé la concentration de ses compétences les plus pointues et de sa R&D, rejoint ensuite par des unités opérationnelles. Tout cela est décrit dans le Pacte Défense Cyber promulgué en 2014 par Jean Yves Le Drian : « 50 mesures pour changer d'échelle », et placer l'excellence du ministère des Armées au service de la nation, élément indispensable pour recouvrer
une part de souveraineté dans ce domaine. La rapidité des transports entre Paris et Rennes est aussi un élément

important pour cet écosystème régalien qui ne peut être que global avec un pied à Paris et un pied en Bretagne.

La seconde est la conséquence de la crise des « Bonnets rouges » qui s'est traduite par le Pacte d'avenir pour la Bretagne signé du premier ministre ; la région a fait du cyber l'une de ses grandes priorités pour son développement, mobilisant ainsi les grands acteurs régionaux et ses opérateurs comme BDI ou BCI par exemple.

Le Pôle d'Excellence Cyber fondé par le ministère et la région en 2014 en est l'une des réalisations concrètes. Six années plus tard, c'est plus de 8000 emplois Cyber qui sont comptabilisés en 2020 par l'étude « AUDIAR », du aussi au fort renforcement sur Rennes des grands de la Cyber (Orange,Thalès, Airbus, Sopra, Capgemini…) à proximité de la DGA, permettant l'essor de tout un ensemble de PME/TPE innovantes, et de startups. 10% des startups sont en Bretagne la mettant très largement en tête des régions. Mais leur marché n'est pas en Bretagne, il est national, européen puis mondial.

Un exemple en est SecureIC ou encore Diateam dont une part importante de leurs CA se fait hors d'Europe ; Glimps fondé par des anciens de la DGA et incubé à la « Defense Factory » à Rennes ouvre aujourd'hui une entité à Toronto au Canada ; Sekoia déjà fortement présente à Rennes va y installer prochainement son siège, ou encore DEFANTS entreprise rennaise citée par le Gartner en 2023. Thales y a un Lab d'expérimentation baptisé La Ruche, Capgemini y a inauguré lors de l'ECW 2022 l'un de ses lab d'Innovation « Défense et Cybersécurité », Orange est très implanté sur Rennes et Lannion.

La French Tech Rennes/St Malo « Le POOOL » tient une place importante dans ce dispositif, les territoires de Vannes/Lorient, Brest ou encore de Lannion ont aussi une forte dynamique. St Malo concentre aussi plusieurs sociétés innovantes comme Alcyconie et verra le 29 septembre un

séminaire national « Cap sur la souveraineté numérique et technologique ».

Beaucoup d'organisations s'engagent aussi : le Clusir Bretagne, le Medef 35…La région Bretagne et le PEC ont su mobiliser un ensemble de partenaires pour gagner un EDIH Cyber européen, idem avec un appel à projets sur les compétences et métiers Cyber d'avenir dans le cadre de France 2030, sans parler du Campus et du CSIRT régionaux.

3/ Considérez-vous l'arsenal pénal adapté à la gravité des faits dont les cybercriminels se rendent coupables ?

Je dirais que l'arsenal pénal français me parait adapté mais qu'il devra continuer à s'adapter et surtout disposer de plus de moyens car la cybercriminalité s'envole. A la suite de la DGSI, la Gendarmerie tout comme la Police Judiciaire DCPJ ont pris depuis quelques années le tournant, Europol aussi avec de beaux succès récents. La Justice a développé un réseau de magistrats spécialisés mais c'est plus la coopération internationale qui pèche avec un certain nombre de pays qui ne coopèrent pas offrant des sanctuaires à certains groupes de cybercriminels. La convention de Budapest n'a que peu évolué depuis des années.

4/ La probabilité d'une multiplication des conflits par artefacts interposés joue-t-elle selon vous sur la perception que les jeunes candidats pourraient avoir de la carrière militaire ?

Je ne le pense pas, les gros flux de recrutement concernent les armées traditionnelles et les motivations sont de devenir marin, aviateur ou soldat. Ensuite presque cent ans après l'apparition de l'aviation militaire, une nouvelle composante se développe à partir des ressources des armées et des civils de la défense. Y recruter est un vrai défi car dans le numérique la concurrence est dure et la ressource rare. Je pense que les unités y seront davantage mixtes car pas

forcément besoin d'être en zone de combat pour agir. C'est un défi pour le commandement, offrir des perspectives opérationnelles en poste de responsabilité et d'encadrement au-delà de cinq ans à de jeunes Master2 ou ingénieurs civils et militaires demande à adapter les structures, d'autant que les armées et nos services de renseignement recrutent sous tous les statuts civils et militaires. Certaines structures comme la DGSE y arrivent parfaitement.

En outre, le ministère des armées dans toutes ses composantes offre des métiers que le civil ne peut offrir : le combat numérique avec son volet « action », c'est passionnant et exaltant, et comme dans les autres composantes les carrières peuvent y être courtes. Les arguments ne manquent pas. Ne pas oublier qu'une grande partie des militaires font des carrières courtes de 5 à 10 ans, et que l'on devient de carrière donc en CDI qu'à l'issue de cette période pour ceux qui restent.

J'ai eu la chance d'être à la fondation de la cyberdéfense militaire et de ses premiers engagements ; la motivation des personnels sous statut civil était la même que celle de leur camarade sous statut militaire. Servir son pays mais dans un domaine nouveau en pleine mutation, où il faut innover. Le problème du recrutement initial n'est pas le plus compliqué, je suis en contact avec de nombreuses écoles, tant pour les sciences sociales que pour les sciences technologiques, l'attirance est là avec des motivations assez identiques aux autres domaines, mais celui de la fidélisation et des plans de carrières est plus compliquée, la capacité cyber en est à ses débuts, le cyber militaire a fêté ses dix ans en 2021, je reste optimiste, le COMCYBER saura trouver les solutions.

5/ Sur l'innovation technologique, trouvez-vous les milieux militaire, économique et académique suffisamment proches ?

Ils ne sont jamais assez proches bien sûr mais de nombreuses structures ou initiatives existent, le rôle du Pôle

d’Excellence Cyber en est un exemple, décloisonner, favoriser un écosystème transverse sont dans nos gènes.

On voit aussi beaucoup de TPE fondées par des anciens du ministère ou de l’ANSSI, ou encore du CEA, sans parler de « spin off issues » de l’INRIA ou du CNRS et de différents centres de recherche, voire d’écoles comme EPITA, à travers la France, les IRT aussi et j’en oublie. La région rennaise en comporte un certain nombre.

En France l’innovation se porte plutôt bien, chaque année de nombreuses, voire trop de startups voient le jour, sont accompagnées, certaines disparaissent aussi. France 2030 mobilise beaucoup de moyens et d’acteurs, on peut penser au rôle de l’INRIA, au Campus Cyber national, au Pôle Systematic avec ses 900 membres, à Cyberbooster ou encore Auriga Capital, à la French tech qui a des antennes très dynamiques, notamment à New York ou à Singapour, à Paris Station F où Thalès est très présent.

La DGA n’est pas en reste avec sa CyberFactory basée à Rennes, ou encore les processus RAPID, et ses Programmes d’Etude Amont (PEA) qui alimentent le domaine Cyber et préparent l’avenir. DGA/MI ce sont aussi des centaines d’ingénieurs dédiés à ces sujets. Il en sort des sociétés comme GLIMPS par exemple. On peut aussi penser à ANOZRWAY. Mais la vraie difficulté est le passage à l’échelle pour transformer ces jeunes pousses souvent fragiles en scale-ups, puis PME aptes à conquérir des marchés européens, puis aller sur le marché américain ou asiatique…

Le marché national est trop étroit et fragmenté, comment doit-il se consolider, comment nouer des partenariats et avec qui ? Ce sont de vraies questions, tout comme les besoins en investissements pour pouvoir se développer rapidement et rester à la pointe de l’innovation. L’apparition de fonds à vocation souveraine bien comprise, il ne suffit pas d’être français, il faut avant tout gagner des marchés face à la

concurrence souvent bien installée et très bien financée. Là encore de nombreuses initiatives ont vu le jour : Tikeau avec les fonds Brienne 3 puis 4, pour ne parler que du plus gros, sans oublier le rôle de la BPI et de la DGE, ou encore DefInnov et DefInvest en lien étroit avec le ministère des armées.

Des PME peuvent aujourd'hui lever des dizaines de millions d'euro en France, voire une centaine pour les dernières opérations : CHAPSVISION, TEHTRIS, PRELIGENS en sont des exemples. Mais cela pose aussi la question des dirigeants, être patron charismatique d'une TPE de quelques centaines d'employés ne garantit pas de pouvoir devenir patron d'une société de plusieurs milliers de personnes…

***6/ On sait combien le défilé du 14 juillet dope chaque année le sentiment patriotique des Français.* Que faudrait-il imaginer pour qu'ils tirent leurs trois couleurs de leurs poches les 364 autres jours de l'année ?**

Le 14 juillet est effectivement un moment fort de cohésion nationale, mais on peut aussi penser aux finales des différentes coupes du monde. Ce sont des moments où la fierté d'être français se manifeste. Ils sont rares… et précieux dans un monde incertain, de plus en plus dangereux où la cohésion nationale est tous les jours attaquée par différentes idéologies, différentes formes de complotismes et de communautarismes ou ingérences extérieures. Le numérique amplifie tous les discours de haine, la désinformation a pris une très forte ampleur notamment grâce à toutes sortes d'outils, à base d'IA génératives notamment, qui faussent les perceptions. Il sera de plus en plus difficile de discerner la réalité et le vrai dans la masse d'informations accessibles et de source plus ou moins fiables, des TPE comme Storizy ou encore Pluralisme s'attaquent au sujet.

« Fier d'être français » est pour moi l'une des clefs, cela

passe par l'éducation, la culture, la mise en avant d'évènements et d'initiatives positives. C'est une opération de reconstruction où les valeurs de la République doivent être fortement affirmées. Les armées sont intéressantes à regarder ; elles intègrent toutes les origines et composantes de la nation, autour de valeurs fortes et d'un cadre bien défini, permettent à des soldats de devenir officier, voire général. La force morale insufflée et la fierté des anciens et des traditions y tiennent une place importante pour fonder la cohésion. L'action d'association comme « Espérance banlieue » ou encore de l'Association des Membres de la Légion d'Honneur (SMLH) sont aussi des exemples qui montrent que cela est possible.

De nombreux militaires en retraite se sont investis dans ce type de projet depuis des années. On peut aussi penser au général de Villiers dont les ouvrages rencontrent un vrai succès. Quand on commande à tous niveaux, des unités militaires engagées dans l'action, que ce soit du groupe de combat confié à un sergent, ou au niveau d'un dispositif comme Barkhane, on est au contact de la jeunesse de toutes origines, la moyenne d'âge est plus proche des 25 ans que des 40 ans, pareil sur un navire de combat… Je suis certain que de nombreux militaires qui quittent l'institution relativement jeunes ont encore envie de servir dans un cadre civil ou associatif, de transmettre, de poursuivre leur engagement, idem en ce qui concerne les gendarmes ou les policiers, ils sont formés pour encadrer. Ils forment une ressource humaine qui pourrait être davantage mise à contribution dans des projets concrets, au contact sur le terrain.

7/ Quel avenir prédisez-vous à un monde dans lequel les belligérants seraient tenus d'employer les moyens de leurs adversaires pour maintenir leurs positions ? Nous pensons particulièrement au recours aux deepfakes dans le cadre des campagnes de déstabilisation et autres

PsyOps ? (Le US Special Operations Command se prépare à mener de vastes campagnes de déstabilisation en ligne en recourant à l'usage de #deepfakes, selon des documents contractuels fédéraux)

En ce qui concerne les unités militaires, même si elles comprennent des civils, placées sous le commandement du CEMA (Chef d'état-major des Armées), je ne peux qu'être en désaccord, une démocratie ne peut se comporter comme une autocratie ou une bande de voyous, c'est une question d'éthique et de valeurs. Comme en ce qui concerne la torture, le viol ou toutes sortes d'exactions que l'on voit en période de guerre, ce sont des choses répréhensibles y compris pénalement en droit national et international. L'action des forces militaires françaises est clairement encadrée par le Droit des Conflits armés (DCA) et le Droit International Humanitaire (DIH), et le droit pénal national. Cela fixe un cadre qui dans les ordres d'opérations se traduit par des règles d'engagement et de comportement, certaines cibles comme les hôpitaux sont interdites par exemple. Le cyber n'y déroge pas même si l'application en est plus complexe et nouvelle que dans les domaines traditionnels.

Le DCA autorise cependant la ruse, mais pas la perfidie. Se faire passer pour un adversaire et le tromper, fausser ses perceptions : OUI à condition de s'attaquer aux belligérants à ceux qui participent à la confrontation ; forces militaires et étatiques bien sûr mais aussi aux « groupes armés » partie prenante. Se faire passer pour la Croix Rouge, commettre des appels à la haine : NON. Le ministère des Armées a d'ailleurs produit un document public donnant sa vision juridique du combat numérique ; se démarquant d'ailleurs du Manuel dit de Tallinn qui est très influencé par le droit anglo-saxon qui est plus permissif en termes d'emploi de la force. Dans ce cadre le recours aux technologies, s'attaquer à la force morale adverse, y compris en utilisant des deep fake, des avatars ou autres moyens d'action informatique n'est pas interdit à condition de respecter le cadre fixé. La guerre informationnelle n'est pas nouvelle… il suffit de relire Sun Tzu… Briser la force morale de l'adversaire, fausser ses

perceptions et donc sa capacité de décision et d'action, gagner la confrontation sans devoir combattre… D'autres exemples très concrets peuvent être cités quand on regarde la préparation des grands débarquements de la guerre 39/45 afin in fine de surprendre l'adversaire. En ce qui concerne nos amis américains, on peut être plus circonspect et vigilant. L'IA au sein d'une coalition peut aussi servir à fausser la prise de décision des partenaires. Il y a tout juste 20 ans Dominique de Villepin a pu prononcer son discours devant l'ONU car la France bénéficiait d'un renseignement satellitaire autonome et souverain. Il ne faut pas non plus oublier les révélations Snowden qui lèvent en 2013 le voile sur les agissements des services de renseignement US et leur espionnage de masse.

L'introduction en masse de l'IA générative, des réseaux sociaux, de la désinformation va rendre l'appréciation de situation beaucoup plus complexe. Aujourd'hui face à toutes les technologies d'IA notamment générative la question de l'appréciation souveraine se pose. C'est bien pour cela qu'une cyberdéfense autonome couvrant tous les volets d'action est un élément fort de notre souveraineté stratégique, et pas seulement une question économique. L'Etat en a pris conscience, la création récente de VIGINUM, et le renforcement depuis 2011 du cyber dans les armées et les services de renseignement en est un autre. Mais, je le concède la voie est étroite car ces technologies sont totalement duales et tirées par la dynamique du numérique civil, cela ne peut se concevoir que dans une politique globale reposant sur une forme de souveraineté technologique, ou plutôt d'autonomie stratégique, car face à un domaine difficilement maitrisable marqué par une suprématie américaine et chinoise, et où les autocraties ne respectent pas les mêmes règles, il faut trouver une voie qui préserve notre autonomie d'appréciation et d'action, notre éthique. La confrontation est tant économique, culturelle que stratégique, avec un volet militaire qui n'est pas forcément premier.

8/ Nous vous savons attachés à la question : qu'apportent les profils atypiques en matière de cyberdéfense ?

L'une des clefs essentielles du cyber ce sont les compétences, les talents. Nous avons besoin de tous les talents et les neuro-atypiques, notamment les asperger, en recèlent beaucoup. En général, ils sont très concentrés sur le problème à résoudre, sur le respect des consignes, ils vont au fond des choses et raisonnent différemment « out of the box », font preuve d'une très grande loyauté, certains développent des facultés étonnantes, ont un rapport aux chiffres ou au codage différents. Ce sont des qualités précieuses. Pourquoi s'en priver ? Pourquoi les laisser au bord de la route ? C'est pour cela que nous avons lancé un manifeste pour l'inclusion que nous proposons aux membres du PEC et aux exposants à l'European Cyber Week (ECW) de signer. Nos amis israéliens et américains ne s'y sont pas trompés et développent des programmes d'accueil spécifiques notamment en matière de codage, de renseignement, de crypto, de « retro engineering » ou encore de cyber.

Nous avons lancé en 2018 un programme d'accueil au sein du ministère des armées, certaines grandes entreprises comme Airbus ou Capgemini ont aussi des programmes, l'Etat a lancé l'initiative « Aspi Friendly » avec un ensemble d'universités et d'écoles pour des formations allant jusqu'au master. Mais ce sont des personnes qui ont besoin d'un environnement adapté et bienveillant, de beaucoup d'attentions ; ils doivent être accompagnés par des organismes spécialisés. C'est important et cet accompagnement est la clef de leur bonne intégration. Au sein du PEC, nous avons un groupe de travail sur le sujet avec des membres mais aussi des entités spécialisées comme Auticonsul, Avencod ou encore AFG autisme. Mais ce qui est important c'est de faire du concret… Lors de l'ECW 2023 nous lançons un challenge spécialisé à leur profit. Ensuite je tiens à signaler l'excellente coopération que nous avons avec l'institut Solacroup (IMTS) de Dinard, ou encore Rennes

Métropole et le rectorat. Nous devrions présenter et diffuser lors de l'ECW 2023 un guide pratique d'accueil. Pour ceux que cela intéresse, vous pouvez consulter sur le site du PEC – en cours de refonte – le nouveau sera présenté lors de l'ECW 2023 -, les podcasts qui reprennent les tables rondes de l'ECW 2022, les témoignages y sont décoiffants….

9/ Internet a souvent été comparé au domaine maritime. Trouvez-vous qu'il est encore possible de filer utilement la métaphore en 2023 ?

Bien sur toute proportion gardée, on peut aussi le comparer à un gigantesque combat urbain. Ce sont des métaphores pour faire référence à des choses connues et rendre plus compréhensibles les défis posés et les solutions trouvées par nos ainés, mais il est clair que cela s'arrête assez vite car le numérique a un tempo bien plus rapide, ses innovations et nouveaux services irriguent toutes les activités humaines, les technologies sont duales, les frontières classiques sont gommées. On peut perdre la guerre en mer si on perd sa maîtrise, Napoléon et Hitler en sont des exemples, la mer apporte un recul stratégique et les flux logistiques permettent de peser sur les confrontations à terre, là où les hommes vivent, mais on ne la gagne pas la guerre en mer, cela se finit toujours à terre. Le numérique est un peu comparable… On peut être défait avant de combattre, être désorganisé par des attaques informatiques et informationnelles, d'autant que la guerre est de plus en plus globale et ne se limite pas à la seule action militaire, il permet de mener des actions de tout genre au cœur de la nation attaquée. Le rêve de Sun Tzu était de gagner une confrontation sans combattre par des actions de renseignement et de sabotage, en faussant les perceptions, par des actions indirectes qui brisent les forces morales et la confiance dans ses capacités et structures de commandement et de gouvernance. Préserver ou perdre la supériorité numérique est un facteur important, voire essentiel dans la confrontation. C'est bien pour cela que depuis les années 2000 la guerre informatique, offensive et défensive, est devenue

structurante dans les moyens d'action des nations. En France le tournant a été pris en 2008 par le Livre blanc sur la sécurité et la défense qui en a fait une priorité. L'histoire tout d'abord nous apporte des exemples : l'époque d'extension du commerce maritime avec son lot de pirates, de corsaires, de libertaires qui côtoient l'activité militaire, de pêche et commerciale des nations avec encore l'expansion des grandes compagnies maritimes qui vont défier les rois, un peu aujourd'hui comme les GAFA et autres grands acteurs civils du numériques, qui sont des attributs de puissance et d'influence, voire de mise sous dépendance pour ceux qui n'arrivent pas à suivre le rythme effréné des évolutions technologiques, on peut penser au traitements et circulations des données, à l'intelligence artificielle, ou encore à la 5G, aux câbles sous-marins, aux data center et à leur puissance de calcul, au quantique…. La mer est source de richesses et d'échange, mais voit aussi son lot de prédateurs aux statuts divers, d'actions à distance contre la terre, de blocus…. Cet espace est non régulé autrement que par la force, les cargaisons diverses or, drogue, thé, esclaves, biens manufacturés crée de la richesse et permettent la domination et l'expansion des nations maritimes. La cargaison d'un côté, les données de l'autre. Les Etats ont réagi et su trouver des formes de souverainetés maritimes à géométrie variable, su s'accorder et coopérer face à la piraterie. Le droit maritime a mis 300 ans à éclore et à se structurer, pour le numérique on ne peut pas être dans le même calendrier…… Force est de constater que si les droits nationaux savent rapidement évoluer, il n'en est absolument pas de même pour le droit international où peu de progrès ont été faits depuis 2009. Beaucoup de choses restent à inventer…. Ensuite la mer est un espace toujours en mouvement, un monde fluide, d'une force qui vous dépasse… avec ses zones plus ou moins bien connues comme les grands fonds… On peut les comparer au « dark web » très mal cartographié et en mouvement….

10/ Quel personnage historique s'étant illustré jusqu'au XVIIIème siècle feriez-vous volontiers intervenir à notre époque ? Et pour quelle raison ?

Etant marin je ne peux que penser à Surcouf chef de guerre plein d'audace qui pensait hors des sentiers battus pour surprendre et défaire ses adversaires pourtant plus puissants, être mobile, les surprendre pour acquérir localement la supériorité et les défaire en leur imposant l'heure, le lieu et le contexte de l'attaque. Un chef de guerre. Dans le numérique c'est un peu comparable, il faut combiner innovation tactique, et innovation technologique, un petit groupe audacieux peut mettre à mal une organisation bien plus puissante en exploitant ses faiblesses et ses failles, pas en allant l'attaquer de front, là où il est puissant. L'initiative revient souvent à l'attaquant et une organisation complexe est très difficile à défendre, trouver et exploiter le point faible, le maillon faible souvent humain par ruse, gagner la guerre du temps par la surprise. Cela ne s'improvise pas… il faut beaucoup d'agilité intellectuelle, d'entrainement, de connaissance du terrain, et savoir prendre des risques calculés. Le combat comporte toujours un volet « force morale » et cohésion de ses équipes. Le Cyber n'y déroge pas.

□□ Mezze de tweets

> *□□ ENTRETIEN – @SouveraineTech tiendra son premier colloque (consacré à la souveraineté) le 29 septembre prochain à Saint-Malo.@SouveraineTech a répondu à nos questions ⬇□https://t.co/w3hPm6umXR*
>
> *– Front Populaire (@FrontPopOff) September 19, 2023*

"#BMW Group a choisi #AWS comme fournisseur privilégié de services cloud pour sa plateforme de conduite automatisée." https://t.co/FdMUBIJcbB

— Souveraine Tech (@SouveraineTech) September 20, 2023

#Oracle □□ les fonds de tiroirs du cloud souverain □□https://t.co/PqbHQTK49J

— Souveraine Tech (@SouveraineTech) September 20, 2023

"@OVHcloud_FR, @outscale_fr ou encore @Scaleway_fr pour ne nommer que ceux-ci font partie des clouds locaux vers lesquels les entreprises peuvent se tourner pour contrôler l'exposition de leurs données.
Et @clever_cloudFR, et @icodia, et @Kloudici …https://t.co/NUZYLs1VQp

— Souveraine Tech (@SouveraineTech) September 20, 2023

□ Le gouvernement allemand envisagerait de limiter l'équipement chinois à un maximum de 25 % dans la RAN (réseau télécom rural), ainsi que de l'interdire totalement dans les zones géographiques sensibles comme la capitale. #Huawei https://t.co/W6uuWx24VR

— Souveraine Tech (@SouveraineTech) September 20, 2023

Produits laitiers : la France pourrait ne plus couvrir ses besoins à partir de 2027. https://t.co/d5NpuFmCzp

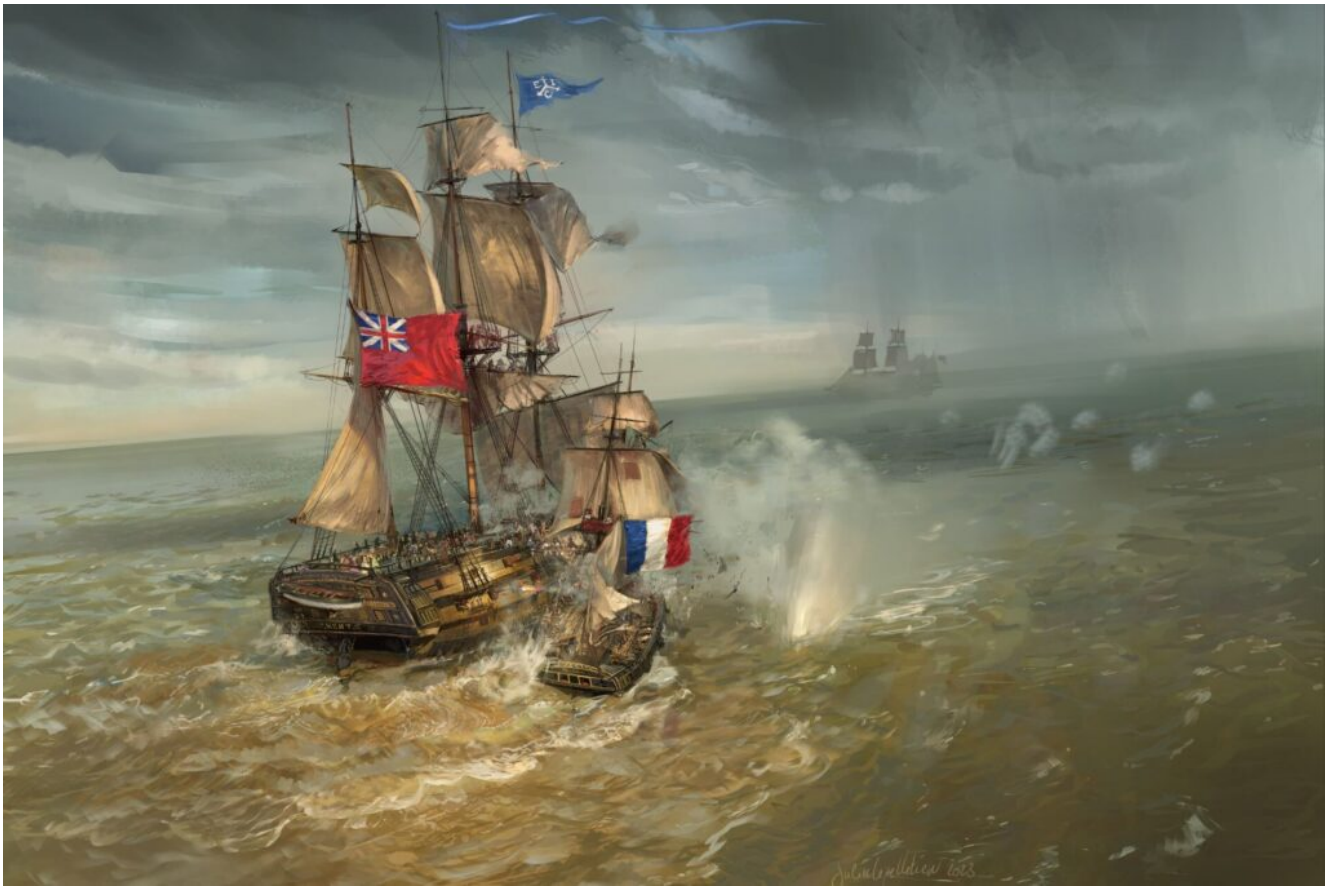
— Souveraine Tech (@SouveraineTech) September 21, 2023

> *#Nearlink, la nouvelle technologie de #Huawei, serait 6 fois plus rapide que le #Bluetooth tout en consommant 60 % d'énergie en moins."https://t.co/xpere6qMNT*
>
> *— Souveraine Tech (@SouveraineTech) September 20, 2023*

> *Les Faïenceries de Cornouaille rapatrient la production de leurs bols bretons dans le Finistère. https://t.co/aCRnrd6vOZ*
>
> *— Souveraine Tech (@SouveraineTech) September 19, 2023*

> *Cartographie des entreprises stratégiques françaises vendues à des concurrents étrangers depuis 15 ans. Beau travail de compilation d'Augustin de Colnet.https://t.co/Lz5KGOBR7F pic.twitter.com/0GibX6pELb*
>
> *— Jerome Bondu (@jeromebondu) September 18, 2023*

□□ Hors spectre



La Prise du Kent par Surcouf par Julien Lepelletier

« Il n’y a pas d’endroit où l’on peut respirer plus librement que sur le pont d’un navire. » **Elsa Triolet**