Sur la sécurité cyber et physique des humains dans les futurs réseaux

Gérard Le Lann

Sur la sécurité cyber et physique des humains dans les futurs réseaux

Gérard Le Lann

Article invité, Revue des Télécommunications, n° 204, Avril 2022

https://www.telecom-paris-alumni.fr/fr/revue/article/sur-la-securite-cyber-et-physique-des-humains-dans-les-futurs-reseaux/3694

Networks with Humans Inside

"Pour ce qui est de l'avenir, il ne s'agit pas de le prévoir mais de le rendre possible" ***Antoine de Saint-Exupéry***

That's precisely what scientists and engineers do. They change the world!

Prolégomènes (*en anglais*)

There will be humans INSIDE future networks (future Internet, multiverse, networks of fully automated terrestrial and aerial vehicles, etc.). What about safety and security?

Vulnerabilities in physical space (injuries, fatalities) may/will result from vulnerabilities in cyberspace (intentional cyberthreats, unexpected faults/failures). Health, ethics, privacy, and social acceptability issues shall be fundamental design drivers for future networks with humans inside, on a par with correctness and performance.

Will that be the case? Not sure … Players which master technologies at the core of existing networks with HUMANS AT THE EDGE are ideally positioned for determining the fate of networks with HUMANS INSIDE. Will Europe be able to play influential roles?
Those topics are surveyed in this article.

Introduction

La cybersécurité et la sécurité physique des humains seront-elles garanties dans « l'Internet du futur » ? Et qu'entendons-nous exactement par « Internet du futur » ?

Consacrer la ressource *temps humain* aux activités les plus nobles. C'est ce but que nous poursuivons avec la mécanisation et la digitalisation des tâches. Depuis l'avènement d'Internet, les gains en *temps humain* se paient en *atteintes à la sécurité cyber et physique*. La sécurité physique est en dehors des considérations propres à Internet. Elle est requise et non négociable avec les futurs réseaux qui contiennent des humains.

L'Internet du futur

Avec Internet, les humains ont commencé leur « migration » vers un cyber-univers en cours de construction. Ses éléments, son architecture et les équipements qui en fournissent l'accès sont fondés sur des innovations algorithmiques et technologiques qui en font, sans doute, la « machine » numérique la plus puissante jamais construite. Après les annonces de Multivers[1],

[1] https://fr.wikipedia.org/wiki/Multivers

il est tentant de concevoir l'Internet du futur comme une extension de l'Internet actuel constituée d'univers numériques permettant aux humains *qui le souhaitent* de vivre plusieurs vies en réalité virtuelle ou/et augmentée, en plus de leurs vies réelles. D'ores et déjà, et *indépendamment de leurs souhaits*, un ou plusieurs univers numériques existent pour les utilisateurs/utilisatrices d'Internet ou du Web, bâti(s) sur les données personnelles confiées aux réseaux sociaux et sur celles collectées—le plus souvent sans consentement—par les géants du Numérique (GAFAM[2] et leurs partenaires, ainsi que leurs concurrents asiatiques).

La porosité entre univers numériques est l'affaire de ces géants. La porosité entre univers réel et univers numériques existe depuis l'apparition des premiers assistants digitaux. Pour le prix d'un repas dans un bon restaurant, on peut « faire rentrer » l'un des géants chez soi, en installant un assistant vocal. Les géants du Numérique concurrencent les Pouvoirs Publics : Big Browser côtoie ou remplace Big Brother !

Dans l'Internet du futur, les risques encourus par les humains sont blessures et morts *numériques* : violations de la vie privée, usurpation d'identité, cybersurveillance illégitime, données et avatars falsifiés, ou définitivement effacés, etc. Ces cyberattaques peuvent entrainer des blessures et des morts *physiques*. Par exemple, altération des facultés mentales (harcèlements, rançongiciels) et décès (hack de stimulateurs cardiaques, salles d'urgence des hôpitaux privées d'électricité).

« Internet » étant également utilisé pour signifier « réseau », il importe de distinguer :

-- Le réseau des réseaux qui libère les humains de la contrainte de synchronicité espace-temps pour la plupart de leurs activités et qui leur permet d'exploiter des réseaux d'artefacts (IoT par exemple),

-- Les réseaux cyberphysiques qui contiennent des humains—ici appelés réseaux cyberphysiques habités (RCH)—où les risques encourus sont blessures et morts *physiques*.

Les réseaux cyberphysiques habités du futur

Bases habitées sous-marines ou spatiales (ISS, etc.), systèmes de transport automatisé terrestre (véhicules individuels, Hyperloop, etc.) ou aérien, missions spatiales, flottes hybrides de robots et d'humains (interventions rapides post catastrophes), sont des exemples de RCH.

Un précurseur est le système/réseau embarqué sur la Navette Spatiale[3] chargé de contrôler son inclinaison lors des phases de rentrée atmosphérique (plus de 7 km/s). Pour garantir la survie des astronautes, la température de la structure interne doit être maintenue en-dessous de 180°C. Cela est possible si, grâce à des calculs d'inclinaison extrêmement précis, les températures que doit supporter le bouclier thermique n'excèdent pas 1.650°C. Un système-bord quadruplé (capteurs, ordinateurs, actionneurs) assure cette tâche, hors de portée des humains. Les ingénieurs du projet SIFT (1976-1982) démontrèrent que la redondance minimale pour tolérer f défaillances de type arbitraire (ordinateur arbitrairement « menteur ») est $3f+1$ ($f = 1$ pour la Navette)[4]. Les commandes des actionneurs sont calculées grâce à un algorithme de consensus distribué, devenu célèbre sous le nom d'algorithme des Généraux Byzantins, précurseur des algorithmes BFT (*Byzantine Fault Tolerance*), désormais au cœur des blockchains et hyper-ledgers.

---

[2] Ou AMMAM, si l'on utilise les noms des holdings (Alphabet, Meta).

[3] https://fr.wikipedia.org/wiki/Navette_spatiale_am%C3%A9ricaine

[4] M. Pease, R. Shostak, and L. Lamport, "Reaching Agreement in the Presence of Faults", Journal of the ACM, vol. 27(2), April 1980, pp. 228–234.
https://www.microsoft.com/en-us/research/publication/reaching-agreement-presence-faults/

À la même époque commencèrent les travaux sur les véhicules autonomes (VA), l'objectif *S* visé étant la sécurité physique (*safety*) des passagers : réduction d'un facteur important (10 par exemple) des accidents mortels. Les débuts ne sont pas très prometteurs. On dénombre à ce jour plus d'une centaine d'accidents impliquant des VA (en mode autonome) ayant causé de graves blessures irréversibles et/ou des décès. Il se confirme que la robotique embarquée ne suffit pas. Les solutions fondées sur l'IA (*deep learning*, réseaux neuronaux, etc.) n'apportent pas grand-chose pour les scénarios critiques, les seuls qui importent vis-à-vis de *S*.
D'où le bien-fondé de l'adjonction des communications. Depuis une douzaine d'années, des protocoles de communications radio wifi ou cellulaire de portée ~ 300m (sans relayage) et des normes V2X (*Vehicle-to-X*)[5] pour les véhicules autonomes communicants (VAC) font l'objet d'études par le C2C Communication Consortium, la 5G Automotive Alliance, et la Society of Automotive Engineers. Malheureusement, les solutions V2X souffrent de graves défauts. Par exemple :
-- Les VAC à la V2X sont conçus comme des smartphones-sur-roues. Ils feront donc l'objet des cyberattaques pratiquées quotidiennement dans Internet et le Web. La différence est que les smartphones-sur-roues peuvent tuer.
-- Le balisage périodique (BP)—diffusion de messages contenant les coordonnées GPS des émetteurs. En trafic dense, un VAC est à portée radio d'au moins une centaine de voisins. Il n'existe aucune étude d'impact sur la santé des passagers des VAC bombardés pendant 1 heure toutes les *x* secondes (*x* de 0,1 à 1) par des émetteurs très proches (éventuellement chaque jour).
-- BP ne sert à rien pour la sécurité (BP « viole » un fameux résultat d'impossibilité)[6]. Par contre, BP facilite les cyberattaques (espionnage des trajets, prise de contrôle à distance des VAC[7], d'où collisions massives, qui peuvent aussi être crées par simple brouillage radio, etc.).

Est-ce pour ces raisons que (jusqu'à présent), ni Waymo (Alphabet) ni Tesla n'ont prévu de recourir à V2X ? Oui à l'adjonction des communications, mais pas n'importe lesquelles…

Les capteurs intérieurs (micros, caméras, avec ou sans reconnaissance faciale) permettent l'enregistrement illimité des données personnelles des passagers. Le RGPD est inapplicable. Consentement préalable à la collecte des données ? Droit à l'effacement des données ? Cela n'a guère de sens avec les VA ou les VAC. Ici aussi, les atteintes à la sécurité cyber peuvent avoir de graves conséquences en matière de sécurité physique.

Des solutions (autres que V2X) garantissent sécurité cyber et physique ainsi que respect de la vie privée des passagers. Le lecteur intéressé pourra consulter un rapport récent[8].

Dans un avenir proche, les questions de sécurité cyber et physique se poseront en 3D, les véhicules aériens habités automatisés (*unmanned aerial vehicles*) se trouvant « mélangés » avec drones, constellations de dizaines ou centaines de milliers de minisatellites en orbites basses, et débris de toute sorte. Bien que circulant dans des couloirs bien définis, par catégories, ces « objets » volants doivent se coordonner quasiment en permanence pour éviter les collisions (« croisements » dans les couloirs, traversées des couloirs lors des phases d'ascension et de descente).

---

[5] X = V (vehicle), I (infrastructure), P (pedestrian).

[6] M. Fischer, N. Lynch, and M. Paterson, "Impossibility of Distributed Consensus with One Faulty Process", Journal of the ACM, Vol. 32 (2), April 1985, pp. 374-382. http://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf

[7] Janvier 2022, un hacker White Hat a pu prendre le contrôle à distance de plus de 20 Tesla dans 10 pays. https://www.linformaticien.com/

[8] G. Le Lann, "Cyberphysical Constructs and Concepts for Fully Automated Networked Vehicles", INRIA RR 9297, Oct. 2019, 64 p. https://www.researchgate.net/publication/337023484

D'où la nécessité de doter les RCH 2D et 3D d'algorithmes de coordination distribuée temps réel, capables de résister aux défaillances involontaires et aux cyberattaques. Il importe de noter la différence importante entre RCH *spontanés* (véhicules individuels par exemple) et RCH *à horaires et trajets planifiés* (trains/avions/métros automatisés, etc.).

Les problèmes posés sont assez proches de ceux examinés pour l'Internet interplanétaire[9] (qui relève à la fois de l'Internet du futur et des RCH), même si les référentiels d'espace-temps considérés sont différents (Physique Newtonienne, Physique Relativiste).

Qui détermine le futur ?

Le futur appartient :

-- À l'industrie des composants électroniques et photoniques [nano/micro *chips*, processeurs classiques ou quantiques, multicœurs 2D ou 3D, etc. pour le calcul et les communications],

-- Aux géants du Numérique et de l'industrie des Télécommunications, propriétaires des câbles optiques sous-marins,

-- À l'industrie spatiale et aux géants (cf. supra) [constellations de minisatellites, nouveaux *backbones* d'Internet],

-- Aux géants du Numérique et leurs partenaires, propriétaires des logiciels fondamentaux dont dépendent désormais toutes les activités numériques humaines [*firmware*, *handlers* d'entrées/sorties, noyaux, systèmes d'exploitation, applicatifs génériques (*cloud/edge computing*, moteurs d'IA, cryptologie post-quantique, etc.)].

Les « clés » pour la sécurité cyber, les « pièges » éventuels (backdoors, etc.), sont au cœur de ces logiciels fondamentaux. Quelle que soit l'ingéniosité des autres acteurs du Numérique, la sécurité cyber (et donc physique) des humains leur échappe donc, en très grande partie.

Les allégeances sont difficilement évitables. Les glissements de terminologie (par exemple, « cloud « souverain » remplacé par cloud « de confiance ») sont des aveux d'impuissance. Les constructeurs automobiles traditionnels se voient obligés de passer des alliances avec les géants du Numérique (Stellantis avec Amazon / Cruise (GM), BMW et Renault avec Qualcomm, etc.).

L'Europe est à la traine. La maitrise d'un futur en Numérique centré sur les aspects éthique et sécuritaire des humains est de nature *matière grise* technoscientifique, et non pas de nature législative ou politique. En effet, aucune loi dans aucun pays ne peut obliger un géant à publier les codes de ses logiciels fondamentaux (secrets industriels). De toute façon, qui disposerait des compétences permettant de vérifier l'exactitude d'une éventuelle publication ? Sachant en outre que les codes en question peuvent changer au gré des stratégies des propriétaires, des nouvelles versions et des corrections d'erreurs ou de failles. Ils auront donc toujours plusieurs « coups d'avance ». Ces géants craignent les sanctions des marchés financiers, pas les amendes prononcées par les juridictions européennes. Soit parce qu'elles sont de montants négligeables en regard de leurs performances[10], soit parce qu'elles peuvent être annulées. Treize ans après, le tribunal de l'Union Européenne annule l'amende (1 milliard d'euros) prononcée en 2009 contre Intel par la Commission Européenne[11].

Annoncer des investissements pour le futur ne sert pas à grand-chose si l'on ne dispose pas *d'abord* des cerveaux capables de les exploiter intelligemment. Il existe en Europe des équipes de scientifiques et d'ingénieurs d'excellence indiscutable. Pour maitriser les futures

---

[9] IPNSIG https://ipnsig.org/ Voir le numéro 201, août 2021, de cette Revue https://bit.ly/revuetelecomlelannfr

[10] CA 2021 (milliards US$) / Google : 257 / Amazon : 241 / Apple : 365.

[11] https://www.lemonde.fr/economie/article/2022/01/26/intel-voit-son-amende-de-1-milliard-d-euros-annulee-par-la-justice-europeenne_6111070_3234.html

technologies, il faut les enseigner (ainsi que les Mathématiques), ce qui n'est pas suffisamment le cas en France. L'Europe n'a toujours pas réussi à développer les écosystèmes équivalents à ceux créés aux États-Unis. La marche est trop haute. Une stratégie possible est de sceller des alliances avec les plus forts, le temps de regagner le terrain perdu, pour faire jeu égal in fine.

Conclusion

Dans quel type de société voulons-nous vivre ? Si rien ne change, la sécurité cyber et physique des humains ne sera pas garantie dans les réseaux du futur (Internet et autres).

L'Europe doit recouvrer sa souveraineté pour ces enjeux stratégiques. La route sera longue. Il est temps d'agir …

Bio express

Ingénieur ENSEEIHT et Docteur d'État en Informatique.

1969 : CERN (Genève) / projet Omega (réseau d'acquisition des données produites au sein de l'accélérateur de particules).

1972 : chercheur IRIA (Rennes) / il découvre le mécanisme de « fenêtre glissante » (contrôle d'erreur et de flux) désormais au cœur des protocoles réseaux.

1973 : Stanford University, invité par Vint Cerf / il participe à la spécification du protocole TCP.

1977 : publication du premier algorithme distribué tolérant les défaillances.

De 1978 à 2011 : directeur de recherche INRIA (Rocquencourt) / travaux à l'origine de plus d'une centaine de publications, contrats, audits, brevets et transferts industriels.

Depuis 2011, directeur de recherche émérite / travaux sur les réseaux de véhicules autonomes communicants terrestres et aériens.

https://www.researchgate.net/profile/Gerard_Le_Lann

Il fait partie des pionniers Internet cités sur la plaque « Birth of the Internet » inaugurée à Stanford University en 2005.

En 2012, il a reçu le prix Willis Lamb de l'Académie des Sciences, pour ses travaux algorithmiques et ceux intéressant la Défense.