Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SECRÉTARIAT D'ÉTAT
AU NUMÉRIQUE
ET À L'INNOVATION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES ÉTRANGÈRES
ET DU DÉVELOPPEMENT
INTERNATIONAL

SGDSN

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Initiative française

« Construire la paix et la sécurité internationales de la société numérique »

Acteurs publics, acteurs privés, rôles et responsabilités.

Jeudi 19 janvier 2017

Sommaire

Le contexte

Le numérique a investi la vie politique, sociale et économique du monde au fur et à mesure du développement des infrastructures qui le portent. Il restera source de progrès, de diffusion des cultures et des savoirs si nos sociétés savent l'intégrer, si les équilibres économiques y sont maintenus et la violence contenue.

Or, bien que sa nature ne soit pas clairement identifiée, le monde numérique a d'ores et déjà été présenté comme un nouveau domaine de combat. Des conférences traitent régulièrement de la régulation des conflits armés dans cet espace auquel doivent s'appliquer les principes du droit international comme l'a reconnu le groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GGE) de l'organisation des Nations-Unies (ONU).

Dans la *stratégie nationale pour la sécurité du numérique,* le Premier ministre a confié au secrétaire général de la défense et de la sécurité nationale, M. Louis GAUTIER, la mission de « *développer une pensée autonome et conforme à nos valeurs* » relativement aux questions liées à la stabilité du numérique. C'est dans cette dynamique que l'initiative « Construire la paix et la sécurité internationales de la société numérique » a été élaborée par l'agence nationale de la sécurité des systèmes d'information (ANSSI).

• Partenaires

L'initiative est co-piloté par le ministère des affaires étrangères et du développement international et bénéficie du soutien du secrétariat d'Etat chargé du numérique et de l'innovation. Elle s'appuie sur les travaux conduits par les administrations françaises, notamment au sein des ministères de la Justice, de la défense et de l'intérieur.

L'animation de la plateforme numérique, celle du séminaire multidisciplinaire et la préparation de la conférence internationale bénéficieront également de l'appui du réseau AMNECYS.

AMNECYS (Alpine Multidisciplinary Network on Cyber-security Studies) est le fruit d'une initiative prise au sein de la communauté d'universités et d'établissements Grenoble-Alpes (COMUE Grenoble-Alpes) qui a permis l'émergence d'un réseau interdisciplinaire d'experts travaillant dans le domaine de la cybersécurité. Ce réseau réunit aujourd'hui environ 70 chercheurs issus de 9 différents laboratoires de la COMUE Grenoble-Alpes et d'institutions aussi diverses que l'Université Grenoble Alpes, le CNRS, l'IEP de Grenoble, l'INRIA, Grenoble INP et l'Université Savoie Mont-Blanc.

Au-delà de la qualité scientifique propre de ses chercheurs, une des forces d'AMNECYS réside dans la densité et la qualité scientifique des réseaux internationaux auxquels ses chercheurs sont associés. A titre d'exemple, les

chercheurs d'AMNECYS entretiennent des liens étroits avec l'Interest Group on Peace and Security de la European Society of International Law qui compte plus de 400 membres.

Le caractère pluridisciplinaire du réseau AMNECYS permet, par ailleurs, de contrôler et tester la faisabilité technique et scientifique des propositions normatives[1].

[1] Contact AMNECYS : Karine Bannelier-Christakis, Maître de Conférences (HDR) au Centre d'Etudes sur la Sécurité Internationale et le Coopérations Européennes (CESICE), Université Grenoble Alpes. karine.bannelier-christakis@univ-grenoble-alpes.fr

La plateforme numérique multilingue

Ouverture le 25 janvier 2017

• Principe

A l'image de la consultation proposée par le secrétariat d'Etat chargé du numérique à l'occasion de l'élaboration de la loi pour une République numérique, la plateforme visera à recueillir les contributions d'utilisateurs et d'acteurs du numérique de tous pays.

Accessible via internet à partir du 25 janvier 2017, cette plateforme comme les contributions qu'elle accueillera sera accessible en 10 langues : allemand, anglais, arabe, chinois, coréen, espagnol, français, italien, portugais, russe.

Afin d'attirer les contributions, une communication vers les « experts du droit international » sera initié par le réseau AMNECYS ; une campagne de communication sur les réseaux sociaux de plusieurs pays sera parallèlement lancée pour favoriser les contributions des « acteurs du numérique ».

Coordonnée par l'agence Isobar qui en a assuré la création graphique, la plateforme est développée par les entreprises françaises TalkSpirit et Systran.

• Questions posées

Parti a été pris de favoriser à la fois les contributions à la plateforme de spécialistes du droit international et celles d'autres acteurs ou utilisateurs du numérique. La page d'accueil proposera ainsi deux parcours de contribution : un plutôt destiné aux experts en droit, l'autre à un public plus large – particuliers, entreprises, ONG, acteurs institutionnels, etc.

Les questions posées sur la plateforme aux experts en droit sont les suivantes :

I. Gouvernance-Régulation. Quel rôle respectif des Etats et des acteurs privés dans le domaine de la régulation de la sécurité du numérique ?

i. Quelle place accorder aux acteurs privés dans l'élaboration d'un cadre normatif applicable au cyberespace, à l'échelle nationale et à l'échelle internationale ?

ii. Quel est/devrait être le rôle des organisations internationales existantes dans le domaine de la sécurité du numérique ?

iii. Comment universaliser les normes agréées dans le cadre du GGE ?

iv. Est-il nécessaire de créer une nouvelle structure inter-gouvernementale ou multi-acteurs dans ce domaine ?

II. Prévention-Protection-Réaction. Quels rôles respectifs pour les Etats et les acteurs privés dans la prévention, la protection et la réaction aux cyber-attaques et autres actes malveillants ?

i. Quelles mesures les Etats devraient-ils adopter en matière de sécurité de l'espace numérique afin d'éviter les actes malveillants affectant les droits d'autres Etats ?

ii. Les acteurs privés peuvent-ils unilatéralement déclencher des mesures de « cyber-défense active » ?

iii. Les Etats peuvent-ils s'appuyer sur des acteurs privés pour conduire des mesures de « cyber-défense active » ?

iv. Les Etats peuvent-ils voir leur responsabilité internationale engagée du fait de mesures de « cyber-défense active » adoptées par des entités privées ?

Les questions posées sur la plateforme à l'ensemble des utilisateurs et acteurs du numérique sont les suivantes :

- Peut-on définir des frontières dans l'espace numérique dans lesquelles seraient applicables les droits nationaux ou ceux définis par les organisations intergouvernementales (protection des données, liberté d'expression, sécurité informatique) ?

  Le droit national dans son ensemble, du droit public à celui de la guerre, s'applique en s'appuyant sur la présence de frontières géographiques. Elles instaurent les limites d'application du droit national, parfois différent de celui de pays limitrophes. Les frontières géographiques disent la validité d'un droit national, régional ou spécifique à un espace.

  Or, l'espace numérique ne correspond pas à la vision matérielle d'un territoire, même s'il est porté par des infrastructures physiques. Il est perçu comme un espace n'ayant aucune frontière, échappant donc aux droits nationaux et à l'action publique, d'une part en raison de sa nature en partie immatérielle et d'autre part en raison de sa présence mondiale et de son partage par l'humanité entière, à l'instar des océans. Si en 1982, les Nations Unies ont réussi à faire cohabiter les notions d'eaux territoriales et d'eaux internationales, les frontières de l'espace numérique restent encore à appréhender.

- De quelle manière les entreprises, les ONG et l'ensemble des acteurs peuvent participer à l'élaboration de la paix dans un monde qui se numérise ?

  Le numérique est un apport significatif aux sociétés humaines, en matière de développement, d'économie, de partage des savoirs et des cultures. Il peut nous permettre d'accompagner des défis communs. Les infrastructures critiques civiles, comme la distribution d'électricité ou de l'eau, les hôpitaux, les services bancaires, etc., sont de plus en plus numérisées et souvent connectées à internet.

  L'actualité internationale montre que le développement simultané de la criminalité informatique et l'utilisation de l'espace numérique par certains groupes ou Etats pour y mener des actions hostiles rendent le monde numérique incertain.

  Certaines attaques informatiques interrompent ces services essentiels et mettent ainsi en danger la sécurité des populations. Ces attaques, de plus en plus fréquentes, participent à la prolifération des armes informatiques et à la banalisation de leur utilisation.

  Si aucun mécanisme vertueux n'est mis en place, à long terme, c'est l'existence même du monde numérique qui pourrait être remise en cause.

- Faut-il une « Charte des droits de l'être humain et du citoyen du monde numérique » ? Quels seraient les grands principes de cette charte ?

  Après la seconde guerre mondiale, les Nations Unies adoptent une déclaration universelle des droits de l'Homme requérant des Etats d'agir en faveur et dans la limite de leur territoire, du respect des droits fondamentaux et inaliénables de l'être humain.

  Le monde numérique, de par sa nature non-territorialisée et un certain anonymat, fragilise cette déclaration par des actes numériques malveillants dont les conséquences ont parfois des impacts sur la vie quotidienne des victimes. Ces actes peuvent mettre en péril le droit à la diversité culturelle, les droits sociaux ou économiques.

  Par leurs objectifs manipulatoires, certaines attaques informatiques ou actions d'influence peuvent entraver le droit des peuples à disposer d'eux-mêmes ou déstabiliser des Etats.

- Est-il nécessaire de créer une nouvelle structure internationale et multi-acteurs dans le domaine du numérique ? Si oui, quels en seraient ses missions et moyens ?

  Des sujets complexes ont été régulés par la création d'entités internationales, regroupant des acteurs d'expertises et de responsabilités complémentaires. Le monde numérique, système complexe et multidisciplinaire pourrait être animé ou régulé, équilibré voire organisé par une entité intergouvernementale ou non gouvernementale, éventuellement doté d'outils contraignants.

- Quels seraient, d'après vous, les critères permettant d'attribuer de manière précise une attaque informatique ?

  A la différence d'une attaque physique, qui permet le plus souvent d'identifier l'agresseur, le monde numérique permet de bien des manières d'en masquer l'identité – rebonds, avatars, proxies, etc.

  Certains Etats ou certaines entreprises se fondent sur des faisceaux d'indices non-informatiques pour attribuer la responsabilité d'une attaque dans le monde numérique : l'attitude d'une personne, d'un pays ou d'un acteur, le profit du crime, les compétences nécessaires…

- Doit-on accorder aux entreprises, aux ONG et à l'ensemble des acteurs du monde numérique le droit de répondre à une attaque informatique par une autre attaque informatique ?

  Les attaques informatiques prennent des formes très différentes. A l'heure actuelle, seuls les Etats, peuvent légalement utiliser des armes informatiques ou répondre à une attaque informatique dans des conditions précises, débattus au sein d'instances internationales, à l'exemple du « groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale » des Nations Unies.

  Certains Etats souhaitent autoriser une entreprise victime d'une attaque informatique à riposter par voie numérique, malgré les difficultés d'identification du décideur de l'attaque.

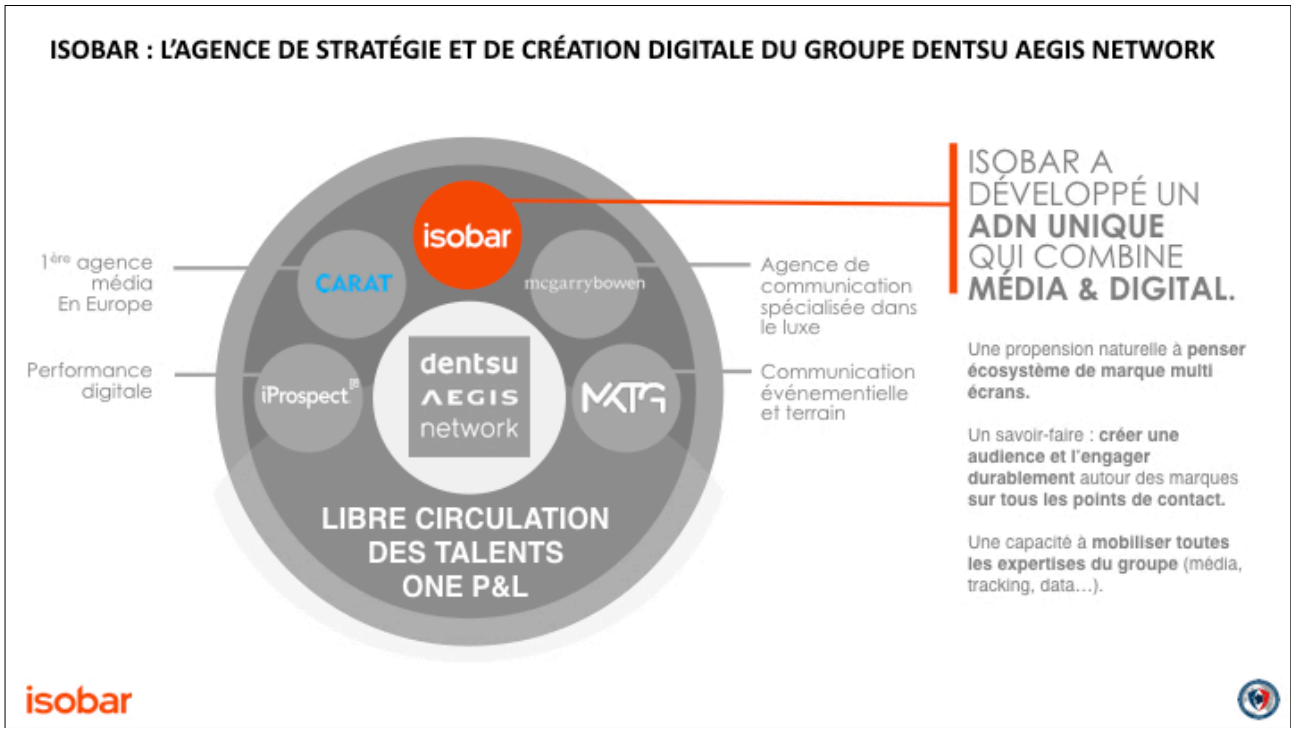
Ces questions seront accompagnées de textes et de vidéos de présentation qui faciliteront leur compréhension.

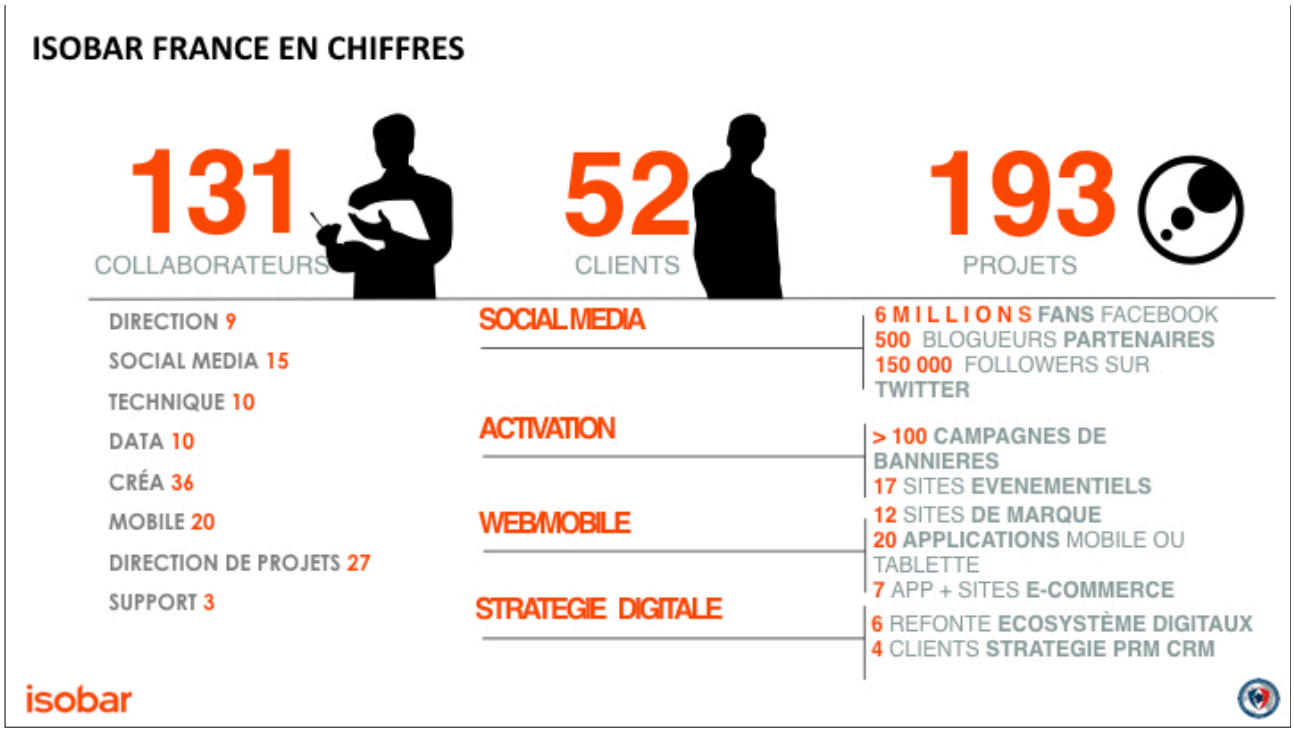
• Conception et développement technique

La création graphique est l'œuvre de l'agence Isobar. Le « moteur de forum » est un développement de Talkspirit et la traduction automatique est assurée par Systran.

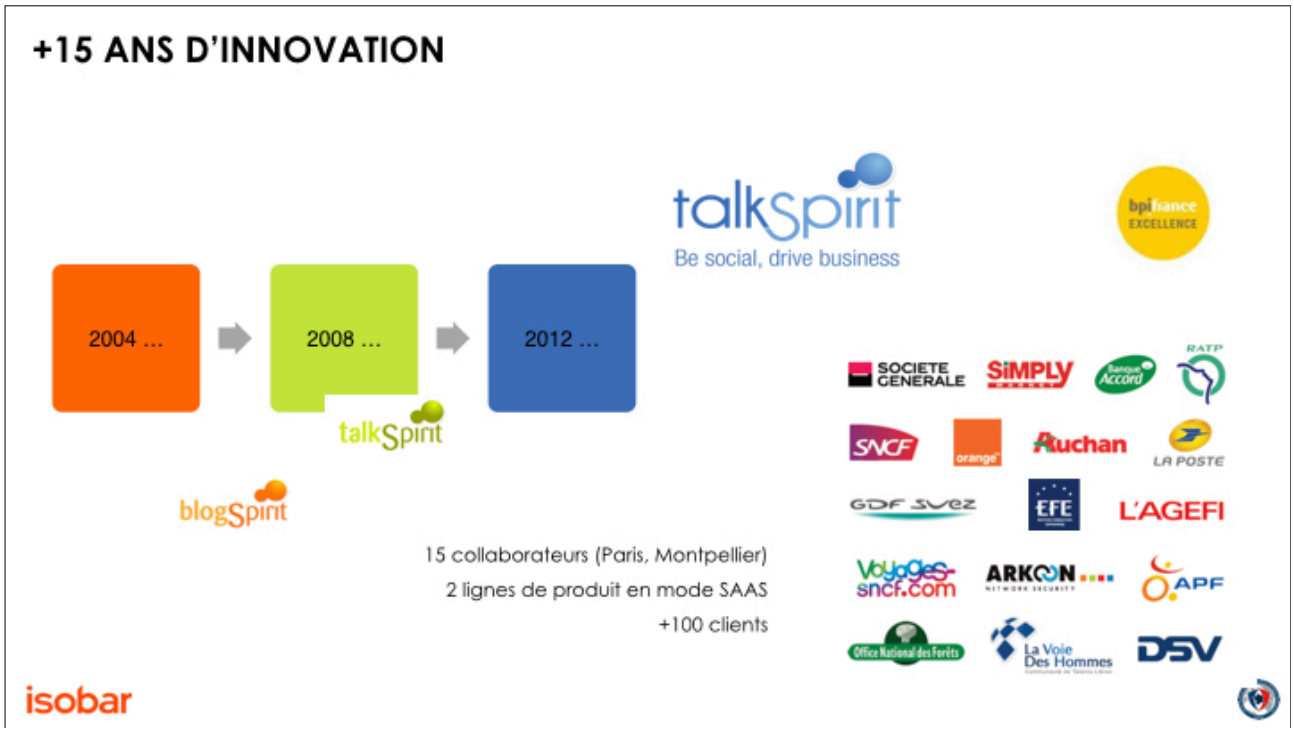
Ces entreprises sont présentées ci-après.

Présentation d'Isobar





Présentation de TalkSpirit



Présentation de Systran

Acteur mondial et pionnier des technologies de traduction.

Avec plus de 40 années de recherche et développement, SYSTRAN est un pionnier des technologies du langage.

SYSTRAN est aujourd'hui la technologie de traduction de référence pour les sociétés multinationales, les acteurs du monde de la Défense et de la Sécurité et les fournisseurs de services linguistiques.

SYSTRAN est également le fournisseur officiel de solutions de traduction pour l'application S-Translator, une application embarquée par défaut sur les smartphones Samsung Galaxy de la série S et Note.

isobar

LA SOLUTION

Facilement intégrable via API REST
Activation immédiate
Appels simples: 3 paramètres

Plateforme haute disponibilité hébergée en France
Redondance matérielle, grappe de moteurs de traduction, monitoring 24/7
Hébergée chez OVH à Roubaix

Coûts au volume traduit

isobar

Le séminaire multidisciplinaire

Les 1er et 2 février - non public

• Principe

Afin d'approfondir certaines notions juridiques complexes et de s'assurer que ces notions sont applicables dans le numérique, un séminaire réunira au secrétariat général de la défense et de la sécurité nationale les 1er et 2 février 2017 des experts en droit international de plusieurs pays et des experts des sciences humaines et du numérique du réseau AMNECYS.

• Questions traitées

Le 1er février : questions centrées sur le droit international

I. Prévention-Protection. Quelles obligations pour les Etats et les acteurs privés dans la prévention et la protection contre les cyber-attaques et autres actes malveillants ?

i. En application du principe de due diligence, quelles mesures les Etats devraient-ils adopter en matière de sécurité de l'espace numérique afin d'éviter les actes malveillants affectant les droits d'autres Etats ?

ii. Quelles mesures les Etats devraient-ils adopter pour protéger leurs infrastructures critiques, leurs données sensibles et les données personnelles ?

iii. Comment les Etats peuvent-ils encadrer la commercialisation des outils et techniques cyber-offensifs ?

iv. Les Etats devraient-ils interdire aux acteurs privés l'usage de techniques cyber-offensives ?

II. Réactions. Quels rôles respectifs des Etats et des acteurs privés en réaction aux cyber-attaques et autres actes malveillants ?

i. Les acteurs privés peuvent-ils unilatéralement déclencher des mesures de « cyber-défense active » (hack-back) ?

ii. Les Etats peuvent-ils s'appuyer sur des acteurs privés pour conduire des mesures de hack-back ?

iii. Les Etats peuvent-ils voir leur responsabilité internationale engagée du fait de mesures de hack- back adoptées par des entités privées ?

iv. Une cyber-attaque conduite par un acteur privé pourrait-elle être considérée comme une agression armée au sens de l'article 51 de la Charte (et sous quelles conditions) ?

Le 2 février :

Gouvernance-Régulation. Quels rôles respectifs des Etats et des acteurs privés dans le domaine de la régulation de la sécurité du numérique ?

i. Quelle place accorder aux acteurs privés dans l'élaboration d'un cadre normatif applicable au cyberespace, à l'échelle nationale et à l'échelle internationale ?
ii. Quel est/devrait être le rôle des organisations internationales existantes dans le domaine de la sécurité du numérique ?
iii. Comment universaliser les normes agréées dans le cadre du GGE ?
iv. Est-il nécessaire de créer une nouvelle structure inter-gouvernementale ou multi-acteurs dans ce domaine ?

Un séminaire de même format sera organisé à l'issue de la conférence internationale d'avril.

La conférence internationale

Les 6 et 7 avril 2017

• Principe

En associant le secteur privé aux efforts entrepris par les pouvoirs publics français pour renforcer la stabilité dans le cyberespace la conférence organisée les 6 et 7 avril 2017 à l'UNESCO vise à quatre objectifs :

- favoriser l'application des principes et du droit international dans un monde qui se numérise par l'approfondissement de certains concepts juridiques ;
- réfléchir à l'impact potentiel de certaines pratiques sur le développement économique durable porté par le numérique sur la stabilité du cyberespace ;
- étudier la manière dont le rôle du secteur privé redéfinit potentiellement les grands équilibres internationaux à l'ère numérique, à la fois en matière de défense, d'offensif et de régulation internationale ;
- offrir un cadre d'échanges à une large variété de sensibilités économiques, géographiques ou culturelles, promouvoir un modèle français émergent (organisationnel, juridique, politique) en matière de sécurité du numérique.

Cette conférence réunira des intervenants élus, des organisations non gouvernementales, des entreprises, des responsables institutionnels et des juristes. Le programme de la conférence et la liste de ses participants est en cours d'élaboration.

Les contributions de la plateforme numérique et les travaux issus du séminaire multidisciplinaire viendront en appui aux débats.