

JE SUIS  
INTERNET

# DOSSIER DE PRESSE

---

CONFÉRENCE INTERNATIONALE  
CONSTRUIRE LA PAIX ET LA SÉCURITÉ INTERNATIONALES  
DE LA SOCIÉTÉ NUMÉRIQUE

*#SecNumConf*  
*<https://jesuisinternet.today>*

6 - 7 AVRIL 2017



# SOMMAIRE

---

## **ÉDITORIAL - LOUIS GAUTIER**

**SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE**

*Page 3*

## **ÉDITORIAL - GUILLAUME POUPARD**

**DIRECTEUR GÉNÉRAL DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

*Page 4*

## **COMMUNIQUÉ DE PRESSE**

**« CONSTRUIRE LA PAIX ET LA SÉCURITÉ INTERNATIONALES DE LA SOCIÉTÉ NUMÉRIQUE »**

*Page 7*

## **ENJEUX & ÉTUDE**

*Page 9*

## **PROGRAMME PRESSE**

*Page 13*

## **LA PLATEFORME COLLABORATIVE « JE SUIS INTERNET.TODAY »**

**PARTICIPEZ À LA CONSTRUCTION DE LA PAIX ET DE LA SÉCURITÉ INTERNATIONALES DE LA SOCIÉTÉ NUMÉRIQUE**

*Page 15*



# CONSTRUIRE LA PAIX ET LA SÉCURITÉ INTERNATIONALES DE LA SOCIÉTÉ NUMÉRIQUE

---



“ Le numérique est au cœur du développement de nos sociétés. Si nous savons en préserver la stabilité, il peut être source de développement humain, de croissance économique et d'amélioration du fonctionnement de nos démocraties. Dans un contexte marqué par la montée de l'insécurité dans le numérique, la conférence internationale à laquelle vous participez aujourd'hui est l'un des volets de l'initiative que j'ai voulu pour favoriser les échanges entre des acteurs du numérique de natures, d'origines et de sensibilités différentes. Etats, entreprises, organisations gouvernementales ou non et citoyens ont chacun une part de responsabilité dans la construction de la paix et de la sécurité internationales. Cette responsabilité commune est au cœur des deux jours d'échange. ”

*Louis GAUTIER, Secrétaire général de la défense et de la sécurité nationale*

# BUILDING INTERNATIONAL PEACE AND SECURITY IN THE DIGITAL SOCIETY

---

“ Digital is at the heart of the development of our societies. If we know how to preserve stability, it can be a source of human development, economic growth and improved functioning of our democracies. In a context marked by the rise of insecurity in the digital world, the international conference in which you are participating today is one of the components of the initiative I wanted to encourage exchanges between digital actors of nature, Origins and sensibilities. States, enterprises, governmental and nongovernmental organizations and citizens have each a share of responsibility in the construction of international peace and security. This common responsibility is at the heart of the two-day exchange.”

*Louis GAUTIER, General secretary of defense and national security*

# DE QUELLE SOCIÉTÉ NUMÉRIQUE VOULONS-NOUS ?

---



“ Pourquoi réunir des experts de multiples disciplines, des cadres d’entreprises multinationales, des hauts fonctionnaires de plusieurs pays ou d’organisations internationales et des représentants d’organisations non gouvernementales ?

Le travail effectué dans les organisations internationales a déjà permis l’édiction de bonnes pratiques, de règles de comportement ou à la mise en place des mécanismes de coopération qui devraient permettre aux Etats de lutter contre la cybercriminalité, d’assurer une certaine résilience des infrastructures critiques et d’éviter l’escalade dans un affrontement numérique nécessairement destructeur pour l’ensemble des belligérants. Un accord a été arraché sur l’applicabilité du droit international et de ses principes au cyberspace. Pourtant, dans un contexte de croissance du nombre d’attaques informatiques de plus en plus sophistiquées ou massives selon la cible visée, la perspective que des Etats prennent unilatéralement des initiatives susceptibles d’entraîner un accroissement significatif du nombre d’attaques informatiques est un risque que nous ne pouvons pas collectivement prendre. Ces deux jours de débats et d’échanges vont permettre d’évoquer ce risque et d’approcher les diverses options envisageables pour l’éviter tout en favorisant des pratiques conformes au droit international, au respect de la souveraineté des Etats et à la précision de leurs devoirs. Dans cet objectif, l’étude conduite par Karine Bannelier et Théodore Christakis introduit au bon niveau des réflexions qui devront être menées sans a priori. ”

*Guillaume Poupard, Directeur général de l’Agence nationale de la sécurité des systèmes d’information (ANSSI)*

# WHAT DIGITAL SOCIETY DO WE WANT ?

---

“ Why gathering experts from various academic fields, CEOs of multinational companies and representatives of governmental and non-governmental organizations from various States and international organizations ? The work done by international organizations had allowed the adoption of best practices, rules of conduct or the establishment of cooperation mechanisms, which should enable States to combat cybercrime, ensure a certain resilience for critical infrastructures and avoid escalation during a cyber-confrontation that could be destructive for all Parties involved. An agreement on the applicability of international law, and its principles, to cyberspace was found with difficulty. However, as the number of increasingly sophisticated cyber-attacks with precise targets is increasing, the possibility that States could be tempted to take unilateral measures that may seriously provoke a notable increase of computer attacks, is a risk that we cannot collectively take. These two-day debates and discussions will allow us to apprehend this risk and to consider available options so as to avoid it while favoring recognized and lawful practices in due respect of the States sovereignty and duties. To reach this objective, the study led by Karine Bannelier and Théodore Christakis introduces ideas and points of view that ought to be shared at the right level and in good spirits. ”

*Guillaume Poupard, Director general of the Agence nationale de la sécurité des systèmes d'information (ANSSI)*



*Communiqué de presse*

*Paris, le 6 avril 2017*

**CONFÉRENCE INTERNATIONALE  
PARIS, 6 ET 7 AVRIL 2017**

# **CONSTRUIRE LA PAIX ET LA SÉCURITÉ INTERNATIONALES DE LA SOCIÉTÉ NUMÉRIQUE**

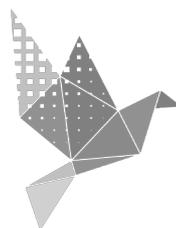
---

**P**oint d'orgue de l'initiative prise en début d'année par la France sur la scène internationale, la première conférence « Construire la paix et la sécurité internationales de la société numérique » se déroulera les 6 et 7 avril prochain au siège de l'UNESCO à Paris. Cet événement innove tant par le sujet abordé très complémentaire des questions liées à la militarisation de l'espace numérique, que par la diversité des auditeurs conviés et le mode de discussion envisagé.

Pendant deux jours, des représentants des Etats, de la société civile et de l'économie numérique, venus des cinq continents, vont ainsi dialoguer ensemble pour faire émerger des pistes de réflexion novatrices et adaptées. Ils envisageront ainsi des pratiques et des équilibres susceptibles de favoriser une utilisation pacifique et sûre de l'espace numérique.

Ces orateurs de haut niveau viendront partager et confronter leur vision du sujet, selon leur culture, leur sensibilité mais aussi leur rôle dans le numérique. Ils constitueront un véritable socle à même d'évoquer des règles de comportement partagées par l'ensemble de la communauté internationale et des différents acteurs. Ceci dans l'objectif de faire du numérique un espace sécurisé, pour les organisations et les personnes, qui réponde aux aspirations de développement économique et de liberté qui y sont associées.

Cette conférence, ouverte au public, est également l'occasion pour les auditeurs de participer à la création de la paix et de la sécurité internationales du numérique, dans un même esprit d'échanges et d'ouverture qui a accompagné la mise en ligne en février de la **plateforme collaborative** « **jesuisinternet.today** ».



**JE SUIS  
INTERNET**



# LES ENJEUX

---

Il y a quelques années, l'Homme inventa Internet, un incroyable moyen de communication reliant les humains, les Nations et les gouvernements du monde entier. Aujourd'hui, cette précieuse invention est également utilisée comme un espace d'affrontement avec des armes informatiques et des pratiques qui menacent son existence. C'est ici que peut naître le citoyen numérique, somme de toutes les voix humaines, qui aspire à la paix, à l'égalité et à la fraternité.

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 » relative aux questions liées à la stabilité du numérique. C'est dans cette dynamique que s'inscrit la conférence pour la paix et la sécurité à l'UNESCO « Construire la paix et la sécurité internationales de la société numérique ».

# AT STAKE

---

The Internet, invented by Man some time ago now, is an incredible means of communication for connecting human beings, Nations and governments across our entire world. Nowadays, the very existence of this valued invention is under threat of being used as much as a space for confrontation and electronic weaponisation as a means for good. This has inspired the creation of the digital citizen, a voice for all humanity, with aspirations for peace, equality and fraternity.

In the French national digital security strategy, the French Prime Minister confided in the general secretary of defense and national security, Louis GAUTIER, the task to «develop an autonomous way of thinking that is in line with our values» when it comes to ensuring stability in the digital world. The UNESCO conference «Building international peace and security in the digital security» is the first step toward this goal.

# CYBERATTAQUES

## PRÉVENTION-RÉACTIONS : RÔLES DES ÉTATS ET DES ACTEURS PRIVÉS

---

**L'étude menée par Karine Bannelier et Théodore Christakis s'inscrit dans une réflexion plus globale lancée par le Secrétaire général de la défense et de la sécurité nationale et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2017. Elle posera les bases des échanges qui se tiendront lors de la conférence internationale.**

Cette étude se propose de conceptualiser et de présenter de façon concise les principales questions que posent, du point de vue du droit international, le rôle des Etats et des acteurs privés dans la prévention et la réaction aux cyberattaques. Elle représente le résultat de recherches conduites par ses auteurs sur les questions relatives à la sécurité de l'espace numérique, la protection des données et de la vie privée.

La sécurité de l'espace numérique, la lutte contre la cyber-criminalité, la gouvernance et la protection des données, sont des enjeux majeurs pour la sécurité internationale et nationale. Alors que les organisations internationales, les Etats et le secteur privé se mobilisent pour adopter de nouvelles normes et codes de conduite dans ce domaine, le droit international existant apporte déjà un grand nombre de réponses pour assurer la coexistence pacifique et la coopération des Nations à l'heure du numérique.

### > Les enjeux de la prévention

L'étude examine, entre autres, la question de la protection des infrastructures critiques numériques et le devoir de diligence due que les Etats doivent exercer à l'égard des acteurs non-étatiques qui opèrent depuis leur territoire (qu'il s'agisse de groupes terroristes, de cybercriminels, d'entreprises ou d'autres acteurs privés).

### > Les réponses aux cyberattaques développées dans le respect du droit international

L'étude procède à une classification des réactions possibles aux cyberattaques et propose une sorte de « mode d'emploi » pour des Etats victimes d'attaques qui souhaitent réagir dans le cadre de la légalité internationale.

### > Les enjeux du « hack-back » et de la « cyber-défense active »

Après avoir montré les avantages, les inconvénients et les risques du hack-back, les auteurs examinent dans quelle mesure les acteurs privés peuvent déclencher unilatéralement des mesures cyber-offensives en conformité avec le droit et dans quelle mesure les Etats peuvent autoriser le hack-back et/ou s'appuyer sur des acteurs privés pour conduire des contre-attaques.

### **Cyberattaques / Prévention-réactions : rôles des Etats et des acteurs privés**

**Karine Bannelier, Maître de Conférences-HDR, Université Grenoble Alpes**

**Théodore Christakis, Professeur, Université Grenoble Alpes/Institut Universitaire de France**

**Les Cahiers de la Revue Défense Nationale, Paris, 2017**

# CYBER-ATTACKS PREVENTION-REACTIONS : THE ROLE OF STATES AND PRIVATE ACTORS

---

**The study led by Karine Bannelier and Théodore Christakis has been prepared within the framework of the French Cybersecurity Initiative launched in 2017 by the General secretary for national defense and security and the french national cybersecurity agency (ANSSI). It will be presented for the International Conference.**

The point of departure for this book is that the dramatic rise of cyber-attacks involving States and non-State actors could constitute a real threat to international peace and security. In 2013, the members of the UN GGE recognized the application of International Law in the cyberspace.

The cyberspace is not a «No Law's Land»; rather, it can be regulated by International Law, as are virtually all international activities. But the task in this field is infinitely more complex, not only because of the very nature of the cyberspace but also because the great diversity of the actors involved. This situation creates an impressive number of combinations, which in their respective turns affect the type and appropriateness of a response.

> Issues of prevention

The book focuses on the issue of prevention and the concept of «cyber-diligence», forged on the basis of existing international law and the obligation of any State not to allow knowingly its territory to be used for acts contrary to the rights of other States.

> The responses to cyber-attacks developed in accordance with international law

The book proceeds to a classification of the possible reactions to cyber-attacks, by proposing a kind of « user's manual » for victim States that wish to react within the limits of international legality.

> Issues of « active cyber defense » and « hack-back »

After analyzing the advantages, disadvantages and risks of hack-back, we answer to the question of whether private actors can unilaterally undertake cyber-offensive measures in accordance with the law, and examine to what extent States can authorize a hack-back operation and/or rely on private actors to conduct counter-attacks.

**Cyber-Attacks – Prevention-Reactions :  
The Role of States and Private Actors**

**Karine Bannelier, Maître de Conférences-HDR, Université Grenoble Alpes**

**Théodore Christakis, Professeur, Université Grenoble Alpes/Institut Universitaire de France**

**Les Cahiers de la Revue Défense Nationale, Paris, 2017**



# PROGRAMME PRESSE

---

## Jeudi 6 avril

### 8h30 - 9h30 : Point presse

Introduction : Enjeux de la conférence et nécessité d'harmoniser les pratiques juridiques entre les pays

- > Louis Gautier, Secrétaire général de la défense et de la sécurité nationale,
- > Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information
- > Karine Bannelier, Maître de conférence-HDR à l'Université de Grenoble Alpes et  
Théodore Christakis, Professeur à l'université de Grenoble Alpes, auteurs de l'étude préparatoire à la conférence.

### 12h30 - 13h : Point presse

Prévention des attaques informatiques et protection : qui doit faire quoi ?

- > En présence des intervenants du panel 1 - Organisations Internationales

### 17h30 - 18h : Point presse

Réponse aux attaques informatiques : qui peut faire quoi ?

- > En présence des intervenants du panel 2 - Les entreprises

## Vendredi 7 avril

### 13h : Point presse

Gouvernance et régulation de la sécurité numérique : quel rôle pour chacun ?

- > En présence des intervenants du panel 3 - Gouvernements

JE SUIS  
INTERNET

**SPEAK UP FOR YOUR RIGHT TO PEACE  
AND SECURITY IN THE DIGITAL WORLD**

UNESCO, Paris 6th and 7th April 2017

01

DAYS

14

HOURS

58

MINUTES

22

SECONDS



USER OF DIGITAL TECHNOLOGIES



LEGAL EXPERTS



**LA PLATEFORME COLLABORATIVE « JESUISINTERNET.TODAY »**

# **PARTICIPEZ À LA CONSTRUCTION DE LA PAIX ET LA SÉCURITÉ INTERNATIONALES DE LA SOCIÉTÉ NUMÉRIQUE**

---

## **Une réflexion inédite et novatrice**

### > Une expérience inédite

La plateforme collaborative « [jesuisinternet.today](http://jesuisinternet.today) » vise à recueillir les contributions d'utilisateurs et d'acteurs du numérique de tout pays autour d'un thème jusqu'ici inédit et novateur : la construction de la paix et de la sécurité internationales de la société numérique. Deux parcours sont proposés : pour les juristes d'une part et pour les autres acteurs du numérique d'autre part. Cette plateforme, comme les contributions qu'elle accueille, est accessible en 10 langues : allemand, anglais, arabe, chinois, coréen, espagnol, français, italien, portugais, russe.

### > Le déroulement

La consultation s'étalera sur toute l'année 2017. Elle offre à tous la possibilité de contribuer à cette réflexion en l'enrichissant et en la faisant évoluer. Les internautes peuvent publier des contributions sur différents thèmes illustrés sous forme de questions.

### > La conférence internationale

La première conférence « Construire la paix et la sécurité internationales de la société numérique » se déroule les 6 et 7 avril prochain au siège de l'UNESCO à Paris.

Pendant deux jours, des représentants des Etats, de la société civile et de l'économie numérique, venus des cinq continents, vont dialoguer ensemble pour faire émerger des pistes de réflexion novatrices et adaptées. Ils envisageront ainsi des pratiques et des équilibres susceptibles de favoriser une utilisation pacifique et sûre de l'espace numérique.

Cette conférence a donné lieu à une étude préparatoire intitulée « Construire la paix et la sécurité internationales de la société numérique » et réalisée par deux chercheurs de l'Université de Grenoble Alpes, Karine Bannelier, Maître de conférence-HDR, et Théodore Christakis, Professeur.

A l'automne 2017, les actes de la conférence seront publiés sur la plateforme et alimenteront la réflexion.

### > Le livrable

Les contributions recueillies permettront de nourrir la réflexion des séminaires d'experts tenus régulièrement autour des questions liées à la cybersécurité et à la construction de la paix dans la société numérique.

## Le principe de cette consultation

### > Pourquoi cette consultation ?

Pour affiner et enrichir la réflexion sur la paix et la sécurité internationales du numérique. De nombreuses conférences ont lieu régulièrement sur les moyens d'éviter l'escalade dans les conflits numériques. L'idée est ici de faire en sorte que le numérique soit le lieu du moins de conflits possibles, les éventuels effets dominos des attaques informatiques étant imprévisible.

### > Comment ça marche ?

Il suffit de :

- se connecter à la plateforme participative [jesuisinternet.today](http://jesuisinternet.today)
- d'identifier une question à laquelle vous souhaitez répondre
- de cliquer sur « M'exprimer sur ce sujet »
- d'inscrire son pseudo et d'écrire puis partager sa contribution

### > Qui peut contribuer à la réflexion ?

La plateforme est ouverte aux spécialistes du droit international mais également aux acteurs ou utilisateurs du numérique. La page d'accueil propose ainsi deux parcours de contribution : un destiné aux experts en droit, l'autre à un public plus large — particuliers, entreprises, ONG, acteurs institutionnels, etc. Les internautes peuvent s'exprimer librement.

Vous pouvez contribuer tout au long de l'année 2017. Ensuite, la plateforme restera accessible, mais il ne sera plus possible aux internautes de faire des propositions.

### > À quoi va servir ma participation ?

L'ANSSI et les experts du réseau AMNECYS liront l'ensemble des contributions qui alimenteront la réflexion sur la paix et la sécurité internationales du numérique. Une synthèse des contributions sera publiée en vue de l'élaboration des séminaires d'experts tenus régulièrement autour des questions liées à la cybersécurité et à la construction de la paix dans la société numérique.

## Des thèmes avant-gardistes pour les experts et les citoyens

### Les experts

> Quel rôle respectif des Etats et des acteurs privés dans le domaine de la régulation de la sécurité du numérique ?

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

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

*Comment universaliser les normes agréées dans le cadre du GGE ?*

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

> 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 ?

*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 ?*

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

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

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

## Les citoyens

> 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 numérisés et souvent connectés 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 manipulateurs, 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.*

**Contacts presse**  
**Agence Verba et Res**

Bénédicte Pilliet - 06 63 57 32 33 - [b.pilliet@cybercercle.com](mailto:b.pilliet@cybercercle.com)  
Isabelle Grozelier - 06 07 06 54 59 - [igrozelier@verbaetres.fr](mailto:igrozelier@verbaetres.fr)

