26/08/2019

Initiative pour des normes dans le cyberespace

Synthèse des enseignements tirés et des bonnes pratiques

Le 6 avril 2019, les ministres des Affaires étrangères du G7 se sont réunis à Dinard (France) pour lancer une Initiative portant sur les normes applicables au cyberespace et consacrée au partage des bonnes pratiques tirées de leur expérience en matière de mise en œuvre des normes volontaires et non contraignantes de comportement responsable des États. Les normes exposées dans ce document émanent principalement des travaux du groupe d'experts gouvernementaux des Nations Unies (GGE) et constituent un sous-ensemble du cadre international pour la stabilité dans le cyberespace. Les pays du G7 sont déterminés à poursuivre ces travaux et à coordonner leurs positions sur toute une série de recommandations importantes mises en évidence dans les rapports de ce groupe d'experts.

Norme 1 - Conformément aux objectifs des Nations Unies, notamment la préservation de la paix et de la sécurité internationales, les États doivent coopérer pour élaborer et appliquer des mesures visant à renforcer la stabilité et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) et à prévenir les pratiques reconnues comme dangereuses dans ce domaine ou pouvant présenter une menace pour la paix et la sécurité internationales.

Les pays du G7 ont pris plusieurs mesures pour renforcer la stabilité et la sécurité dans l'utilisation des TIC et prévenir les pratiques les plus dangereuses en la matière. Ces mesures comprennent :

- la promotion au niveau international d'un cadre de stabilité fondé notamment sur l'application du droit international existant et les normes volontaires de comportement responsable des États, que la présente initiative vise à renforcer ;
- la mise en place de mesures de confiance (notamment à l'OSCE, l'OEA et l'ARF) et de dialogues stratégiques sur les enjeux dans le cyberespace avec plusieurs partenaires aux niveaux bilatéral, trilatéral ou multilatéral, afin de renforcer la confiance, les capacités et les mécanismes de coopération, ce qui consolidera également le cadre de stabilité susmentionné ;

Usage officiel uniquement

- le développement de capacités cyber aux niveaux national et international, pour renforcer le niveau général de résilience, de protection et de sécurité des systèmes et réseaux d'information. Les pays du G7 ont notamment tous publié des stratégies interministérielles globales en matière de cybersécurité, dont l'élaboration et la mise en œuvre effective sont considérées comme une étape essentielle et utile pour permettre la coordination des efforts et le renforcement de la sécurité ;
- l'élaboration constante de normes sectorielles sur la sécurité des technologies pour renforcer la cyber-résilience au niveau mondial et parvenir à une harmonisation au niveau international.

Norme 2 - En cas d'incident informatique, les États doivent prendre en considération toutes les informations pertinentes, notamment le contexte général de l'événement, les difficultés d'attribution dans l'environnement des TIC, ainsi que la nature et l'ampleur des conséquences de l'incident en question.

Les États du G7 ont élaboré des procédures de gestion de crise pour réagir aux incidents informatiques au niveau national.

- Ces procédures comprennent en général un partage régulier d'informations et une coopération renforcée entre administrations et organismes compétents, ce qui peut prendre différentes formes ;
- après la détection d'une attaque, il incombe aux agences techniques de présenter une évaluation de la nature de l'incident, qui ouvre ensuite la voie à une réponse interministérielle, si nécessaire ;
- les pays du G7 considèrent que l'attribution d'une attaque est une décision politique souveraine, prise au cas par cas en tenant dûment compte de toutes les informations pertinentes ;
- certains pays du G7 ont jugé utile de mettre en place un cadre de classification des incidents, pour aider les responsables et les décideurs dans leur analyse et leur action.

Norme 3 - Les États ne doivent pas permettre sciemment que leur territoire soit utilisé pour des activités internationales illicites perpétrées à l'aide de TIC.

Pour ce faire, les pays du G7 :

- ont augmenté les ressources et les capacités de leurs organismes nationaux chargés de la cybersécurité ;
- ont renforcé la coopération avec le secteur privé, afin de promouvoir des normes, des cadres et des procédures efficaces en matière de cybersécurité, en ce qui concerne

notamment la notification des incidents et la sécurité des appareils utilisant l'internet des objets, mais aussi en vue d'améliorer le partage d'informations sur les menaces et d'organiser des campagnes de sensibilisation à la cybersécurité ;

- ont pris des mesures concrètes pour empêcher et dissuader les cybercriminels d'agir sur leur territoire ou en utilisant leurs infrastructures numériques, notamment en qualifiant d'infractions pénales les actes illicites perpétrés à l'aide de TIC, comme les intrusions non autorisées dans les systèmes de sécurité de l'information de tierces parties.

Certains pays du G7 ont pris des mesures pour encourager une notification responsable des vulnérabilités et la mise en place de centres de compétences nationaux. Certains pays ont également choisi d'autres approches pour réduire les dommages causés par les attaques courantes.

Norme 4 - Les États doivent étudier les meilleures modalités de coopération pour échanger des informations, se prêter mutuellement assistance, sanctionner les utilisations terroristes et criminelles des TIC et mettre en œuvre d'autres mesures de coopération pour lutter contre ces menaces. À cet effet, il pourra être nécessaire pour les États d'envisager la possibilité d'élaborer de nouvelles mesures.

Les pays du G7 ont élaboré une série de mesures pour renforcer la coopération avec leurs partenaires afin de prévenir et sanctionner les utilisations terroristes et criminelles des TIC, notamment :

- la ratification de la Convention sur la cybercriminalité du Conseil de l'Europe de 2001 (Convention de Budapest) qui prévoit des moyens efficaces, souples et modernes de coopération internationale en matière de lutte contre la cybercriminalité ;
- la mise en place de partenariats forts avec des partenaires publics et privés, y compris au niveau technique et opérationnel, grâce à des échanges entre équipes d'intervention (CERT) et autres agents des forces de l'ordre ;
- un soutien apporté aux autres pays pour qu'ils développent leurs propres capacités de lutte contre la cybercriminalité de manière bilatérale ou en agissant dans le cadre ou aux côtés d'organisations européennes et internationales.

Certains pays du G7 ont également alloué d'importantes ressources à la coopération avec le secteur privé et la société civile pour prévenir l'utilisation d'internet à des fins terroristes et en retirer les contenus terroristes.

Norme 5 - Les États, tout en assurant la sécurité dans l'utilisation des TIC, doivent respecter les résolutions A/HRC/RES/20/8 et A/HRC/RES/26/13 du Conseil des droits de l'homme (promotion, protection et exercice des droits de l'homme sur l'Internet), ainsi que les résolutions A/RES/68/167 et A/RES 69/166 de l'Assemblée générale des Nations Unies (droit à la vie privée à l'ère du numérique) afin de garantir le plein respect des droits de l'Homme, notamment de la liberté d'expression.

Tous les pays du G7 partagent un même attachement à un internet libre, ouvert et sûr, dans lequel les droits de chacun sont protégés en ligne comme ils le sont hors ligne. Ils jouent un rôle actif pour défendre et promouvoir cette approche, notamment :

- en veillant à ce que la législation nationale en vigueur protège en particulier le droit à la vie privée, la liberté d'expression et les données personnelles et prévienne les nuisances en ligne ;
- en soutenant les initiatives internationales et, le cas échéant, européennes sur la protection des droits de l'Homme sur l'internet (comme le Guide des droits de l'homme pour les utilisateurs d'internet du Conseil de l'Europe, les résolutions pertinentes du Conseil des droits de l'homme, le règlement général sur la protection des données de l'Union européenne, etc.).

Norme 6 - Un État ne doit pas mener ni soutenir sciemment des actions informatiques contraires à ses obligations découlant du droit international et portant atteinte intentionnellement à des infrastructures essentielles ou affectant d'une autre façon l'utilisation ou le fonctionnement d'une infrastructure essentielle assurant des services au profit du public.

Les pays du G7, en tant qu'États responsables, ont réaffirmé leur soutien à cette norme et l'ont défendue au niveau international. Plusieurs d'entre eux ont indiqué clairement que l'utilisation de capacités cyber offensives nationales devait être régie par le respect du droit international, notamment du droit humanitaire.

Norme 7 - Les États doivent prendre des mesures appropriées pour protéger leurs infrastructures essentielles des menaces informatiques, en tenant compte notamment de la résolution 58/199 (2003) de l'Assemblée générale des Nations Unies sur la « Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information » et des autres résolutions pertinentes.

Pour protéger leurs infrastructures essentielles des menaces informatiques, les pays du G7 ont :

- mis en place des cadres réglementaires efficaces, exigeant que les entreprises augmentent leur niveau de protection, soient suffisamment résistantes aux menaces informatiques et notifient les incidents informatiques, ce qui a renforcé de manière significative la coopération entre les secteurs public et privé, en particulier avec les acteurs et les systèmes jugés essentiels ou critiques ;
- encouragé la coopération régionale et internationale sur cette question, notamment par le partage de bonnes pratiques et d'informations sur des menaces et incidents spécifiques, ainsi que par l'élaboration de mesures de confiance entre États ;
- élaboré des programmes et des activités d'éducation, de formation et de coopération pour renforcer leurs capacités et leurs ressources dans ce domaine.

Norme 8 - Les États doivent répondre aux demandes d'assistance appropriées d'autres États dont les infrastructures essentielles subissent des activités informatiques malveillantes. Ils doivent également répondre aux demandes appropriées visant à réduire les activités informatiques malveillantes émanant de leur territoire et prenant pour cibles les infrastructures essentielles d'un autre État, en tenant dûment compte de la souveraineté.

Pour faciliter la réponse aux demandes d'assistance appropriées, les pays du G7 ont mis en place des points de contact permanents précis et opérationnels, qui sont généralement situés au sein des équipes d'intervention en cas d'urgence informatique (CERT) ou des centres de réponse aux incidents de sécurité informatique (CSIRT) et joignables en permanence. Ces points de contact sont généralement partagés avec les autres membres des organisations régionales et internationales compétentes, comme l'OSCE, le réseau des CSIRT de l'UE ou les parties à la Convention de Budapest.

Norme 9 - Les États doivent prendre des mesures raisonnables pour garantir l'intégrité de la chaîne d'approvisionnement, afin que les utilisateurs finaux aient confiance dans la sécurité des produits informatiques. Ils doivent s'efforcer de prévenir la prolifération d'outils et de techniques informatiques malveillants et l'utilisation de fonctionnalités cachées dangereuses.

Les pays du G7 ont pris une série de mesures pour garantir l'intégrité de la chaîne d'approvisionnement et prévenir la prolifération d'outils et de techniques informatiques malveillants ainsi que l'utilisation de fonctionnalités cachées dangereuses, comme :

- l'élaboration et la promotion de cadres, de recommandations, de codes de conduite, de normes et de règles pour les entreprises afin d'améliorer la sensibilisation à la sécurité de la chaîne d'approvisionnement et d'aider les entreprises à mettre en place un contrôle et une surveillance effectifs de leur chaîne d'approvisionnement ; il peut s'agir également de dispositifs de labellisation, d'évaluation et de certification ;
- la mise en place de procédures pour faire en sorte que les passations de marchés publics dans le domaine des TIC contribuent à l'amélioration de la sécurité et de la résilience ;
- la promotion du recours à des régimes de contrôle des exportations adaptés et efficaces pour prévenir la prolifération des outils et des techniques informatiques malveillants.

Norme 10 - Les États doivent encourager une remontée d'informations responsable concernant les vulnérabilités en matière de TIC et partager les connaissances associées concernant les solutions existantes pour pallier ces vulnérabilités, afin de limiter voire d'éliminer les menaces potentielles pesant sur les TIC et les infrastructures reposant sur ces dernières.

Les pays du G7 ont mis en place des procédures, des mécanismes et parfois des cadres juridiques qui facilitent et encouragent la communication responsable des vulnérabilités par et à leurs organismes nationaux chargés de la cybersécurité. Ils ont renforcé leur coopération avec les partenaires publics et privés pour améliorer le partage d'informations sur les vulnérabilités, les mesures d'atténuation et de rétablissement ainsi que les programmes conçus pour aider les partenaires à mettre en place des procédures de divulgation des vulnérabilités.

Norme 11 - Les États ne doivent pas mener ni soutenir sciemment des activités visant à porter atteinte aux systèmes d'informations des équipes agréées d'intervention en cas d'urgence informatique (CERT ou CSIRT) d'un autre État. Un État ne doit pas utiliser ses équipes agréées d'intervention en cas d'urgence informatique pour se livrer à des activités internationales malveillantes.

En tant qu'États responsables, tous les pays du G7 ont réaffirmé fermement le principe selon lequel ils ne mèneraient ni ne soutiendraient sciemment des activités visant à porter atteinte aux CERT d'un autre État et n'auraient pas recours à leurs propres CERT pour se livrer à des activités internationales malveillantes./.