Atelier ATU/UIT sur la stratégie de cybersécurité dans les pays africains, Khartoum, 24 et 26 juillet 2016

Stratégie nationale de cybersécurité : impacts et défis régionaux et internationaux

par Emmanuel ADJOVI, OIF

ORGANISATION INTERNATIONALE DE la francophonie

ORGANISATION INTERNATIONALE DE la francophonie

PLAN

I- IMPACTS MULTIDIMENTIONNELS.

A/ Interactions juridico-politiques.

B/ Impacts économiques.

II- NECESSITE D'UNE STRATEGIE INTERNATIONALE.

A/ Besoins de collaboration internationale pour une efficacité globale et domestique.

B/ Protection des intérêts économiques et stratégiques majeurs des grandes nations et des pays industrialisés.

ORGANISATION INTERNATIONALE DE la francophonie

INTRODUCTION

- Commentant le guide de gouvernance et d'aide à la formulation de stratégie de sécurité du CTO (Commonwealth Telecommunications Organisation), Daniel Ventre, titulaire de chaire de cyberdéfense de l'Ecole militaire de Saint-Cyr en France, a écrit «La cybersécurité n'est pas neutre, ses politiques et stratégies provoquent des effets. Chaque stratégie s'inscrit donc dans un contexte spécifique où de multiples facteurs vont entrer en ligne de compte».

- Ces propos d'un grand spécialiste de cybersécurité illustrent bien les implications des stratégies de cybersécurité sur les contextes régional et international.

ORGANISATION INTERNATIONALE DE la francophonie

- S'il est vrai que les choix opérés dans la stratégie nationale peuvent emporter des conséquences aussi bien sur plan national que régional et international, les impacts ne sont pas provoqués par la seule adoption d'une stratégie nationale. Encore faudrait la mettre en œuvre à travers une politique et la prise de mesures concrètes.

- Conscientes de ces enjeux d'impacts systémiques et de particularités des pays, les organisations internationales comme l'UIT, l'OIF et la CTO recommandent dans leurs guides de cybersécurité ou de stratégies nationales que les orientations proposées doivent être adoptées en fonction des contextes nationaux. Elles devraient même ajouter «contextes régionaux et internationaux», car le déploiement d'une stratégie de cybersécurité impacte ces différents niveaux.

ORGANISATION INTERNATIONALE DE la francophonie

- Quelle est la nature et les caractéristiques de ces impacts et quels défis ils impliquent en termes de stratégies et/ou de politiques publiques à l'international ?

- Il ressort de l'analyse des corrélations entre stratégie nationale et les contextes régionaux et internationaux que les impacts sont multidimensionnels (I). Leur nature et leur ampleur affirment la nécessité d'une stratégie internationale, en raison du caractère transfrontalier du cyberespace (II).

ORGANISATION INTERNATIONALE DE la francophonie

I- IMPACTS MULTIDIMENSIONNELS

A/ Interactions politico-juridiques.

1- Difficulté de coopération due à des différences d'approches : pas de traité global.

- La convergence formelle des stratégies et politiques de cybersécurité de nombreux pays masque difficilement les différences d'approches, liées au fait que ces Etats n'ont pas toujours les mêmes objectifs, ni les mêmes intérêts (cultures différ.) .

- L'extérieur étant considéré comme la source principale des menaces, la stratégie est conçue et mise en œuvre sur la base des besoins de protection nationale.

- Une des conséquences : parfois difficulté de coopération, car les différences de structures, institutions, mesures et mécanismes qui résultent de ces approches nationales se reflètent dans les enceintes régionales et internationales

ORGANISATION INTERNATIONALE DE la francophonie

2- Impact géopolitique : luttes d'influences entre Etats.

- Le cyberespace est à la fois l'enjeu et le théâtre de conflits d'intérêts et de rivalités de pouvoir, mais aussi l'outil d'expression de ces rivalités. Avec leur stratégie nationale, certains Etats cherchent à affirmer leur hégémonie sur le Net : cyberconflits (cyber-terrorisme, cyber-espionnage, etc.)

3- Facilitation des convergences juridiques versus différence régionale.

- Certaines normes juridiques et techniques adoptées par les pays industrialisés ne prennent pas en compte diverses caractéristiques importantes des pays en développement : intégrer les facteurs régionaux.

4- Diminution des paradis de cybercriminalité.

- L'adoption d'une stratégie nationale de cybersécurité affirme une volonté de l'Etat en question d'exclure son cyberespace de la liste des paradis des crimes en ligne. Cela peut amener les attaquants qui opèrent sur son territoire à se déplacer ailleurs. Cas des adeptes du SCAM 419 du Nigéria qui se sont déplacés dans les années 2010 vers les pays d'Afrique de l'Ouest.

ORGANISATION INTERNATIONALE DE la francophonie

B/ Impacts économiques.

- La stratégie nationale de cybersécurité vise principalement à sécuriser les acteurs publics et privés contre les cybermenaces tout en favorisant le développement économique et social du pays concerné.
- Confiance accrue dans le cyberespace facilite la création et l'innovation. Elle signifie :

- développement du commerce électronique ;
- développement de e-banking et e-monnaie ;
- développement des e-services ;
- expansion des équipements électroniques et cybernétiques.

- La protection des infrastructures essentielles de l'Internet et du numérique ainsi des réseaux critiques (énergie, eau, gaz, banque, transport, santé, etc.) constitue un enjeu crucial de l'écosystème économique du numérique.
- L'OCDE (2015) recommande aux Etats, la gestion du risque de sécurité numérique, c'est-à-dire sa réduction à un niveau acceptable, déterminé selon le contexte et les objectives économiques et sociaux en jeu. D'après cette organisation internationale *«A la différence d'une approche purement technique ou centrée sur un objectif isolé de sécurité absolue, la gestion du risque de sécurité numérique permet la sélection de mesures de sécurité appropriées et proportionnées qui ne nuisent ni aux activités économiques qu'elles visent à protéger, ni aux intérêts légitimes d'autrui»*. Ce qui s'entend aussi les acteurs régionaux et internationaux

.

ORGANISATION INTERNATIONALE DE la francophonie

- La stratégie et la politique nationale de cybersécurité sont en passe de devenir des variables de politique internationale permettant de faire de la politique (avec quel pays va-t-on coopérer, échanger des données, faire de la politique de sécurité…). Mais elles permettent aussi de faire du business : existence d'indices permettant d'apprécier le risque cyber pesant sur les entreprises et la société ; indices boursiers/financiers appréciant la valeur du secteur industriel de la cybersécurité (cf. D. Ventre).
- De même, la cybersécurité est considérée désormais comme un secteur industriel à part entière, un secteur d'exportation et donc d'expansion économique avec des répercussions sur les plans régional et international.

ORGANISATION INTERNATIONALE DE la francophonie

II/ Nécessité de stratégie internationale.

A/ Besoins de collaboration internationale pour une efficacité domestique.

- Vu les enjeux et les impacts de la stratégie nationale de cybersécurité et du caractère transfrontalier du cyberespace, il apparait indispensable pour chaque pays de se doter d'une stratégie internationale. En effet, des éléments internationaux importants ont un impact sur les efforts de protection et de réponse nationales issues des stratégies : les groupes de cybercriminels opèrent à travers les frontières nationales; le cyberespionnage se développe; et les États-nations étrangères ont la capacité de lancer des attaques destructrices contre les infrastructures essentielles. Ces risques ne peuvent pas être correctement gérés sans coopération internationale. Celle-ci doit constituer un volet essentiel de la stratégie nationale. Les axes peuvent être scindées en deux parties :

- Cristin Flynn Goodwin et J. Paul Nicholas de Microsoft («Developing a National Strategy for Cybersecurity. Foundations for security, growth and innovation"), recommandent aux Etats la structuration de leur engagement international dans la stratégie nationale de cybersécurité. Pour ce faire, ils doivent y insérer des dispositions qui vise à :

- favoriser une meilleure coopération internationale entre les CERT/CSIRT ;
- promouvoir la coopération policière et judiciaire : l'entraide et l'extradition (agences d'application de la loi) ;
- favoriser les normes internationales et l'harmonisation des certifications internationales ;
- développer des normes de cybersécurité (désigner un organe, chargé de coordonner, de développer et de faire respecter ces normes)

ORGANISATION INTERNATIONALE DE la francophonie

- On peur ajouter à cette liste,

- l'harmonisation des législations régionales et internationales afin de surmonter les difficultés d'établissement d'un traité international : par exemple, les conventions du Conseil de l'Europe, de l'Union africaine et de la Ligue arabe présentent de nombreuses similitudes si bien qu'elles contribuent à harmoniser le droit de la cybercriminalité entre les pays. Sur le plan sous-régional, on peut aussi citer les actes additionnels de la CEDEAO, les lois-types de la CEEAC, les modèles de loi de la COMESA, le cadre juridique harmonisé de EAC, etc.
- la participation et la contribution à des plates-formes et des forums internationaux sur la cybersécurité : groupes d'études des Nations Unies, UIT, Interpol/Europol, OCDE, UNODC, UNICRI, ICANN, ISO, CEI, IETF, FIRST, etc…

ORGANISATION INTERNATIONALE DE la francophonie

B/ Protection des intérêts économiques et stratégiques majeurs des grandes nations et des pays industrialisés.

- Le besoin de coopération internationale s'explique également par la défense des intérêts géopolitiques et économiques des Etats développés

1- Maintenir leur influence dans le monde

- Les modèles de stratégie de la Chine et de la Russie sont différents de celui des Etats-Unis. A l'intérieur du camp occidental, le modèle américain n'est pas réductible au modèle français ou européen.
- La volonté de coopération avec le reste du monde vise à défendre et à partager ses valeurs, ses modèles et sa vision du monde.
- Elle a également pour but de prolonger dans le cyberespace son hégémonie ou son influence dans le monde analogique ou physique.

ORGANISATION INTERNATIONALE DE la francophonie

2- Développer des intérêts économiques.

- Un volet de politique industrielle de cybersécurité : la cybersécurité étant devenue une filière économique à part entière, les nations développées en font un axe de coopération internationale pour favoriser le développement de leur industrie nationale et régionale de cybersécurité. Dans ce contexte, des préoccupations de cyberespionnage officiellement évoquées pour écarter des équipements ou produits d'entreprise étrangères peuvent parfois cacher de puissants intérêts économiques nationaux.
- La normalisation ou standardisation participe de cette volonté de protection de l'industrie nationale ou régionale.

- Le volet de coopération internationale de la stratégie nationale vise aussi à favoriser l'exportation des équipements, matériels et logiciels des pays industrialisés.

ORGANISATION INTERNATIONALE DE la francophonie

MERCI POUR VOTRE ATTENTION

Emmanuel V. ADJOVI

Responsable programme «Société de l'information »/ Information Society Project Manager

Direction de la Francophonie économique et numérique

Organisation internationale de la Francophonie

adjovie@francophonie.org