

Compte-rendu du Lundi de la cybersécurité



Intervenant: Olivier KEMPF

Lieu: Télécom ParisTech

Cette conférence du 18 mars nous a été présentée par **Olivier KEMPF** Docteur en science politique, chercheur associé à la FRS, ancien responsable de la politique de **cyberdéfense** de l'armée de Terre, général en deuxième section. Aujourd'hui il est consultant sur les questions de cyber et de transformation digitale. Il est aussi l'auteur de "Alliances et mésalliances dans le cyberspace" (**Economica**), ouvrage de la collection **Cyberstratégie** qu'il dirige.



Pour plus d'informations <http://www.olivierkempf.com/>

Cette présentation visait à nous expliquer la notion d'alliance dans le contexte du cyberspace. Et cela s'est traduit par une description chronologique de la notion d'alliance qui diffère d'une époque à une autre.

Il en ressort des explications que le concept d'alliance est en perpétuelle évolution dans le monde réel et la construction mentale de l'alliance ne marche pas dans le cyber.

C'est pourquoi on parle de **mésalliance** mais cela ne veut pas dire qu'il n'y a pas d'alliance.

Néanmoins, il faut savoir que le cyberspace est un espace bien convoité malgré son opacité et la méfiance qui le caractérise. L'alliance dans le cyberspace est devenue incontournable aujourd'hui, tous les secteurs d'activité sont dans la nécessité de s'allier, y compris les Etat.

Cet exposé nous a permis d'avoir une vision globale sur les alliances, mais aussi sa spécificité dans le cyberspace. C'est ce qui motive les différents acteurs ou parties prenantes à faire des alliances.

Pour traiter notre sujet et mieux comprendre les alliances dans le cyber, nous allons essayer de répondre à quelques interrogations.

- ❖ **La première question qui se pose est de savoir si la notion d'alliance est un sujet actuel et si cela existe dans le cyberspace ? La réponse est OUI**

Avant de montrer les aspects de l'alliance dans le cyberspace, nous allons d'abord donner quelques exemples d'alliances actuelles.

Exemples

Les alliances énumérées ci-dessous illustrent parfaitement l'actualité de la notion d'alliance.

- **L'OTAN et l'UE** coopèrent en matière de cyberdéfense dans le cadre d'un arrangement technique.



- **Le RGPD** : plan de mesure proposé par l'UE adopté par le conseil en décembre 2018, On parle de règlement, une loi d'application directe.



- **L'appel de Paris**: on a des Etats, des ONG et des entreprises privées dans le cadre du forum pour la gouvernance de l'internet (FGI) le 12 novembre 2018.



Le constat que l'on peut faire suite à cette conférence est qu'il existe bel et bien des alliances dans le cyberspace mais ce n'est pas aussi simple car le cyber est un espace conflictuel.

Nous avons aussi relevé que **traditionnellement** un des moyens de gérer un conflit est d'utiliser un rapport de force c'est à dire nouer une alliance soit bilatérale ou multilatérale mais quand elles sont d'ordre mondial ou du système Onusien on parle **d'organisation internationale**. Avec cette vision on a la prééminence de l'**acteur étatique**, mais ce qui est nouveau dans les alliances c'est cette hybridation avec des acteurs non étatiques qui caractérise plutôt le cyberspace.

❖ **La deuxième interrogation qui se pose c'est pourquoi y'a-t-il des alliances ?**

La réponse à cette question fera ressortir les types d'alliances qui peuvent exister d'une manière générale mais aussi ceux du cyberspace.

L'alliance sert à modifier les rapports de force et elle est fondée sur un calcul. C'est pourquoi dans une alliance il est nécessaire de comprendre ce rapport et le calculer.

Des alliances défensives: Pour assurer sa sécurité

Des alliances offensives: Pour renforcer sa position, pour un but stratégique

Nous constatons que traditionnellement les alliances étaient circonstancielle et temporaire. L'OTAN est un prototype de toutes les alliances. C'est un exemple très particulier, un exemple anormal dans le système des alliances. C'est anormal car d'habitude une alliance ne dure pas autant. La théorie classique des alliances montre qu'elle est temporaire et ne dure qu'au maximum 3 ans. Elle peut être bilatérale et multiple.

L'armée napoléonienne mise en place par une alliance, que l'on qualifie d'alliance de revers, nous sert d'exemple.

Dans le cyber, l'alliance peut être formelle ou tacite c'est-à-dire une alliance qui est nouée par rapport à un objectif. Cette alliance peut être aussi précise, générale, passive, fluide ou structurée. Mais on constate que le cyber est difficile à mesurer car il est opaque, on peut maquiller l'action à ce qu'on ne puisse être identifié ou on peut masquer son message dans le cyberspace.

Ainsi l'objet politique qui se pose aujourd'hui est la structuration de l'alliance. C'est ainsi que l'on va essayer de montrer la nouvelle logique d'alliance dans le cyberspace.

❖ Quelle est la logique des alliances et y'a-t-il une logique d'alliances dans le cyber ?

En général, un pays fort peut avoir des stratégies d'alliances plus offensives que les autres. On parle là de notion de régulation internationale, ou de régulation ou alliance générale.

Dans le cyber on ne peut pas mesurer quelque chose d'opaque, donc on ne peut pas évaluer l'effectivité d'un traité. Aussi le vrai problème du cyberspace est qu'on a beaucoup de métriques pour mesurer la force d'un pays par rapport à un autre. En fait il existe des mesures de protection mais seulement au niveau des entreprises et non à l'échelle internationale (les métriques nourrissent les décisions mais ne prennent pas de décision).



La logique des alliances dans le cyberspace est une notion qui **n'est pas encore claire** car dans une alliance entre deux états, le pays le plus fort peut surveiller son allié, mettre à zéro son système, ou bien modifier et y prendre des infos en fin d'alliance.

Ceci ne veut pas dire qu'on ne doit pas avoir d'alliances mais il faut distinguer les alliés des amis.



❖ **Le cyberspace est-il un monde d'inattribution et de partage des faiblesses ?**

Nous constatons que le cyberspace est caractérisé par la loi de l'inattribution qui fait qu'on ne peut pas attribuer une attaque à un acteur.

La difficulté dans le cyber est quand une attaque est lancée on ne peut pas savoir d'où elle vient, ni jusqu'où elle peut aller et ni qui est l'attaquant.

C'est pourquoi on qualifie le cyberspace de monde de cupidité dans lequel la coopération peut être un très bon moyen d'espionnage, car s'allier en cyber suppose le partage d'information. Cette approche peut conduire à un risque d'affaiblissement potentiel.

La conséquence de l'inattribution fait que dans le cyberspace on n'a pas d'amis, pas d'ennemis ou qu'il n'y a que des ennemis. Dans ce sens on revient dans cette notion de l'état violent (préhistorique) où on ne trouve plus de frontières.



Avant l'apparition du cyberspace on avait un critère extérieur: la **MENACE**, mais aujourd'hui la **menace** n'est plus un critère des alliances mais c'est la **confiance** qui suppose le partage des vulnérabilités.

Avec qui je m'allie? Je m'allie avec quelqu'un de **confiance** avec qui je peux partager mes vulnérabilités et pas uniquement pour des raisons liées au cyber. **On en conclut** que nous devons être très sélectifs dans nos alliances et les raisons peuvent être d'ordre politique, économique et pas seulement pour des enjeux cyber.

Toutefois partager ses faiblesses suppose un partage de secrets. L'enjeu du cyber c'est le **secret**: le vrai secret ce sont nos vulnérabilités.

CONCLUSION

En somme, même si le cyberspace est un monde conflictuel, on y trouve des alliances entre Etats et une hybridation des alliances. On distingue deux types d'alliances, défensives et offensives. Mais chaque alliance se fait pour une ou plusieurs raisons qui nécessitent le partage et on ne peut pas tout partager.

Finalement on n'a pas de critère de force dans le cyber. Dans le cyber l'étalon de mesure c'est la faiblesse. Le moyen de protéger un secret est en lui-même un secret, car dans le cyber on ne peut pas avoir d'amis. C'est pourquoi il est recommandé de mener des entraînements et des exercices pour nous permettre de nous développer et de nous mesurer afin de savoir dans quelle ligue nous jouons. Cependant, certains ont eu des surprises en se fiant à ces mesures, mais c'est le meilleur moyen pour se mesurer aux autres. Donc on peut dire qu'il est très difficile de savoir en qui avoir confiance ou avec qui il faut s'allier.

Nous tenons à remercier

- **Olivier KEMPF** pour la qualité de la présentation et des échanges
- L'école TELECOM PARISTECH et Télécom ParisTech Entrepreneurs de nous avoir accueilli dans leurs locaux ;
- Le MEDEF Hauts-de-Seine, Béatrice LAURENT et Gérard PELIKS pour l'organisation des « **Lundi de la cybersécurité** ».



Yélina Taïbou DIALLO et Seddik CHARKI

MBA Management de la sécurité des données numériques, Institut Léonard de Vinci

Contacts : tahiboudiallo90@gmail.com / charkiseddik@gmail.com