Conférence – 28 avril 2015

# GÉOPOLITIQUE GLOBALE À L'ÈRE DE LA CYBER-GUERRE
## Réponses globales et nationales face aux incidents de hacking internationaux (Ukraine-Russie)
## Analyse de la cyberattaque contre TV5 monde
## Lecture cartographique de la cybersécurité dans la géopolitique globale

Compte-rendu

Anaïs Dufrasnes

Bruxelles, 15 juin 2015

Le 28 avril dernier, l'institut européen des relations internationales a organisé la 8ième session de l'Academia Diplomatica Europaea intitulée "**Géopolitique globale à l'ère de la cyber-guerre**". Le chairman de cette conférence était **Irnerio Seminatore**, **Directeur de l'Institut Européen des Relations Internationales**, qui après une brève introduction des trois intervenants, a présenté quelques réflexions sur l'ère dans laquelle nous vivons aujourd'hui.

Selon Professeur Seminatore, la logique du déséquilibre des forces est renversée par le retour de l'asymétrie. La cyberguerre se présente comme une rupture stratégique en raison de ses caractéristiques suivantes: universalité du champs d'action et multiplicité des opportunités consenties à l'attaquant. Pour beaucoup d'analystes, l'espace cybernétique sera le nouveau champs de guerre, d'attaque. On peut dés lors se demander si les attaques et virus informatiques remplaceront la balistique, l'atome, les armes à feu. Les combats seront non létales, non codifiés, et donc opaques, obéissant à des signes politiques à visée stratégiques. Si le cyber-espace devient le champs de la nouvelle guerre, une attaque planifiée et massive sur ce champs, peut-il déborder sur une guerre classique? D'après Monsieur Seminatore, nous assistons au retour de l'offensive, l'allongement du temps stratégique, de la préparation et de l'offensive. La question sous-jacente à cette problématique peut selon lui être résumée comme suit: la révolution induite dans la stratégie par l'informatique est-elle de même nature que la révolution induite par la stratégie de l'atome? Si l'atome a valorisé, et porté à l'extrême, la défensive, et donc la dissuasion, le concept de non-guerre, et a fait naître une forme particulière de la menace et de la diplomatie, la stratégie informatique laisse-t-elle un espace à la diplomatie, à la modération et à la politique étrangère.

**Olivier Kempf, Directeur de la Vigie, Professeur Associé à Sciences Po Paris**

retient trois notions de la présentation de Monsieur Seminatore: inattribution ou opacité, non létalité et enfin offensive. L'un des points sur lequel Monsieur Kempf a dans un premier temps insisté est celui de la notion même de cyber-guerre, impliquant une guerre dans le cyber. En raison de la non létalité, les experts préfèrent parler de cyberconflictualité, qui s'articule autour de cas stratégique. En vue d'une meilleure compréhension du sujet, une description succinte des fondamentaux de la cyberstratégie sera donnée dans un premier temps  avant d'appliquer cette méthode d'analyse à l'attaque contre TV5monde.

Comme l'illustre Monsieur Kempf, en régime de cyberconflictualité, il existe trois types différents: le militaire, le cyber dans la guerre (dans la chaîne de commandement et dans l'offensive), le géopolitique (entre états, et pas seulement), et l'économique.

De plus, le rubik's cube stratégique à trois dimensions qu'il fait elles-mêmes percevoir sous forme d'une succession d'angles d'analyse qui sont eux-mêmes à trois dimensions. Le cyber espace est constituée de trois couches successives, la première est une couche physique (matérielle), le cyber espace étant avant tout réel, et non virtuel comme certains peuvent le dire. La seconde couche est celle du codage, de la programmation. Enfin, il y a la couche sémantique, la couche d'information. La donnée a du sens, et il faut s'intéresser au sens de l'information. L'attaque subie par TV5monde a touché principalement la couche sémantique.

Le deuxième angle que Monsieur Kempf a ensuite abordé est celui des acteurs. Après la guerre froide est apparue une distinction entre l'acteur étatique et non étatique. Avec le cyber espace, il y a une nouveauté stratégique, dans le sens où l'acteur individuel émerge, ou une coalescence d'acteurs individuels, en vue d'exécuter notamment une opération spécifique.

Le troisième angle illustré par Monsieur Kempf n'est autre que le type d'agression, dont les caractéristiques techniques sont combinables (espionnage, sabotage (usage de maliciel, chevaux de Troie...) pour entraver, voire détruire un système informatique, la subversion (usage du cyber espace pour manipuler les esprits, une manipulation collective ou ciblée). Monsieur Kempf aborde ensuite la question du type d'alliance derrière les attaques cybernétiques et le résultat obtenu suite à l'attaque.

L'attaque contre TV5monde consiste aux faits suivants. Dans la nuit du 8 avril, la chaîne de télévision francophone est piratée par un groupe qui se nomme cyber-califat, les serveurs d'encodage sont piratés et cessent de fonctionner, le cyber-califat publie sur internet des documents qu'il dit être confidentiel. L'affaire fait la une des médias, des experts interviennent et utilisent le terme cyber-guerre, les déclarations politiques se succèdent. Les experts par contre gardent leur calme puisque l'analyse

forensique vient seulement de débuter. Sur ce point, Monsieur Kempf souligne le succès de l'opération d'un point de vue tactique.

En reprenant les dimensions mentionnées ultérieurement, Monsieur Kempf arrive à l'analyse suivante. L'opération a été menée principalement dans les couches logiques et sémantiques, d'abord avec des piratages des serveurs internes et comptes sociaux. Comme il le rappelle, ce n'est pas la première fois qu'une telle attaque arrive (Saoudi Ramco, Sony picture, Reynders...) Le niveau logicielle de l'agression est sérieux mais ce n'est pas du niveau technique de ce qui a été fait par les américains et les israéliens dans succnet contre les américains.
Au travers de ce sabotage, le groupe a voulu frappé les esprits, et donc touché la couche sémantique. Il y a une revendication de la part du cyber-califat d'impliquer la France dans le conflit contre ISIL, une dimension qui est très géopolitique, et une volonté de lier l'agression au conflit militaire qui se déroulait en Irak de par les informations militaires qui ont été divulguées. Néanmoins, militairement parlant, ce n"est pas probant. Pour ce qui est de la dimension économique, dans le cas de TV5monde, il y a eu une interruption pendant une nuit des émissions mais cela n' a pas entravé le bilan économique de la chaîne.

Au contraire, le point fort de cette attaque, comme le démontre Monsieur Kempf, repose sur l'organisation, la professionnalisation des structures. Jusqu'à présent, c'était surtout de la propagande. Le cyber-califat aurait en effet passer contrat avec un groupe de hacker, plus performant qui aurait construit l'opération et livré l'opération dans les mains du cyber-califat. Cela n'est qu'une hypothèse, possible. Si elle s'avérait, elle montrerait une alliance hybride entre des acteurs individuels. On voit qu'il y a trois modes successifs stratégiques, une étape d'espionnage (passée par de l'ingénierie social sur les réseaux sociaux) pour permettre ensuite le sabotage, phase ensuite de sabotage, qui se veut être visible, ensuite la phase de la subversion, faire parler du cyber-califat et ainsi promouvoir l'état islamique, action dans la couche sémantique, endroit du véritable succès. Comme expliqué, il y a eu une bonne étude de la cible stratégique, deux mois après Charlie Hebdo, frapper un média lui permet d'acquérir à coup sure une audience maximale. Cela a été un levier parfait. Les médias se sont sentis eux-mêmes une cible. On a eu ce transfert psychologique. L'affaire public était pour eux une affaire personnel, ils sont tombés dans le jeu des agresseurs.

**Pierre-Emmanuel Thomann, Géopoliticien,** a ensuite pris la parole. Le thème de sa présentation était le suivant: « L'émergence de la cybergéopolitique, les États-Unis, une puissance digitale occupante en Europe ».

La définition de la cybergéopolitique consiste en l'étude des rivalités de pouvoir sur un territoire. Elle est, aux yeux de Monsieur Thomann, une grille de lecture centrale pour comprendre les conflits actuels. La mondialisation est une lutte de répartition

des espaces géopolitiques sur terre (guerre en Crimée), mer, air, et dans le cyberespace également, objet de rivalité entre groupes, états, rivaux qui luttent entre eux pour le contrôle de cet espace. Les rivalités géopolitiques prennent une autre dimension avec les nouvelles technologie de l'information et de la communication.

Quand on essaie de comprendre l'évolution du monde au travers de la géopolitique, on remarque que se reproduisent les rivalités antagonistes passées dans l'espace cybernétique. Il y a ainsi un bipolarisme existant entre ceux qui tentent de préserver un monde unipolaire (États-Unis et Europe) et ceux qui désirent développer la multipolarité dans cet espace particulier.

La question de la cyberconflictualité c'est aussi un quadrillage sur le terrain, notamment au travers des bases de l'OTAN pour les États-Unis. Dans cette bataille géopolitique mondiale, les anglo-saxons adoptent une perspective unipolaire, alliés aux États-Unis, en avance sur ses voisins. En se plaçant au centre de cette problématique, les États-Unis deviennent un centre de rassemblement d'information. Une hiérarchie se met en place, au centre de laquelle les États-Unis se trouvent, puis nous avons les five highs qui bénéficient d'accords privilégiés. L' Union européenne en générale est dans une zone grise, de coopération et de rivalité. Les accords sont cependant asymétriques, et rendent l'Union européenne et ses états membres dépendants des États-Unis. Quant à la Chine et la Russie, ils font office d'adversaire. La chine menace ainsi régulièrement de dédoubler les réseaux si il n'y a pas une meilleure distribution du pouvoir mondial en la matière.

Pour cette raison, Monsieur Thomann a conclu sa présentation en avançant l'argument selon lequel les citoyens en dehors des États-Unis sont devenus des citoyens de seconde zone, sans recours possible pour lutter contre cette politique.

Notre dernier intervenant n'est autre que Monsieur Gertjan Boulet, **Chercheur au Département Law, Science, Technology & Society à l'Université libre de Bruxelles (VUB).** L'emphase de sa présentation s'est porté sur "la nécessité de développer une plus grande collaboration internationale en ce qui concerne la responsabilité d'acteurs privés ou publics". Il a ainsi débuté par un parallélisme entre les cyberattaques à l'encontre de TV5 monde et celles qu'a pu connaître en 2013 Belgacom, le plus grand réseau de télécommunications en Belgique.

L'un des cas de cyberattaques particulièrement intéressant pour Monsieur Boulet concerne le groupe de hackers pro-russe, qui a joué un rôle dans le conflit russo-ukrainien. Le groupe aurait en effet hacké le système ukrainien durant ses élections, ainsi que le système de l'OTAN et le téléphone d'un membre de la délégation américaine, Joe Biden. Bien que le groupe d'activiste n'ait jamais mentionné de support venant de la Russie, certaines compagnies de sécurité ont trouvé des liens avec la Russie dans ces attaques. Par exemple, BAE systems, après analyse,

considère que le ver informatique utilisé pour une attaque contre les systèmes informatiques ukrainiens aurait été codé en russe. Cependant, les médias et les compagnies de sécurité n'ont jamais explicitement attribué les attaques à la Russie.

Le manuel de Tallin aborde ainsi la question de la cybersécurité sur le plan du droit international. Différents thèmes entrent en ligne de compte: la juridiction, la souveraineté, la responsabilité étatique, ou encore l'état de droit. Le point le plus important à l'égard de la question abordée aujourd'hui tient à l'interprétation de la règle 6, traitant de la responsabilité étatique en matière de cyberattaque, même si celles-ci sont réalisées par des acteurs non étatiques.

Par rapport au conflit ukrainien, le manuel de Tallin considère que les actions des acteurs agissant indépendamment ne peuvent être imputées à l'État. Ainsi, après avoir analysé les différents éléments liés aux cyberattaques connus dans le conflit russo-ukrainien, M. Boulet avance l'idée que d'après les articles 8 et 11 liés à la responsabilité des états, nous ne pouvons imputer la responsabilité de ses attaques à la Russie. Il n'existe, à ses yeux, aucun lien apparent entre les actions des activistes et l'État russe, que ce soit en matière de soutien financier ou d'une accusation de chaîne de commandement venant directement de la Russie.

Les experts du Manuel de Tallin travaillent à nouveau sur une  nouvelle version du manuel pour développer le point concernant la souveraineté des États en cas de cyberattaque, ou encore traiter du respect des droits de l'Homme.

La prochaine conférence de l'Institut Européen des Relations Internationales se tiendra à l'INFOPOINT EUROPA le 12 mai prochain et aura pour thème la multipolarité et le multilatéralisme.