Conférence du 18 Octobre 2021 – IHEDN **« De la guerre aux cyberguerres »**

L'hyperconnectivité engendre des conséquences qu'elles soient positives ou négatives. Elle va déterminer la manière dont nous allons confisquer le levier multiplicateur d'information.

Une dépendance aux données peut-être crée, seulement il peut y avoir des risques d'intrusion. Le **cyber** est une forme de défense offensive, nous pouvons donc d'une certaine manière pouvoir dominer nos adversaires.

Les Etats-Unis et la Chine, une rivalité depuis toujours :

Dans les débuts de conflit entre la Chine et les Etats-Unis, « La guerre sans limites » un ouvrage expliquant la situation d'il y a 20 ans, nous conte que les Chinois pensaient avoir aucunes chances de contrer les Américains. La deuxième flotte américaine se situant le long des côtes chinoises, est une puissance colossale qui a des moyens d'écraser la Chine. Ils ont donc imaginé un système qui coupe les réseaux de communication entre les bateaux, les sous-marins et les tours de contrôles extérieures, les torpilles et sous-marins. Il n'y aura donc plus de deuxième flotte.

La marine et l'armée chinoise développe alors une stratégie, il privilégie un certain nombre d'armes devant lesquelles on ne peut réagir. Les Occidentaux ne savent pas gagner les guerres, ils vont ainsi procéder à une recherche d'informations et de menaces. Face à cela, depuis les années 2000, nous nous sommes rendu compte qu'il y a une nouvelle forme de guerre par ses capacités, c'est la **cyberguerre.**

L'informatique, un nouvel outil pour contrer les ennemis :

Nous avions déjà eu des prémices de cette forme de guerre, il s'agit de la première guerre en Irak. Saddam Hussein avait comme projet d'envoyer des scuds (missiles développés par l'Union soviétique), le problème est qu'il fallait empêcher les missiles d'arriver sur la ville de Tel Aviv. La question qui se posait était comment empêcher les Israéliens d'attaquer la ville, les Américains ont donc chercher une solution. Ils ont introduit dans le GPS une variation de 1,5 km. C'est de cette façon que les Américains ont empêché les attaques des Israéliens, par la **cyberattaque**.

Il y a eu depuis quelques années un autre problème à soulever : Empêcher les Iraniens d'avoir les armes atomiques, ils ont détruit les centrifugeuses d'usines. Un sabotage à grande échelle qui fut effectué par deux grands pays spécialistes du cyber, ils ont donc inventé un virus attaquant les systèmes industriels automatisés dans les usines. Ce virus déclenchait une accélération et une décélération de l'ensemble des centrifugeuses, il a été installé via une clé USB introduite sur un des ordinateurs. Deux heures après, 60% des centrifugeuses ont été détruites.

Autre exemple : L'ennemi numéro 1 des Américains sont les Chinois, comment calmer le jeu avec les Russes pour pouvoir attaquer les Chinois ? Ils accusent les Russes de faire de multiples attaques sur des cibles américaines par un groupe d'hacker nommé « REvil », qui a attaqué des points importants américains sur le point de l'administration. « Darksite » et « REvil » ont été supprimé de tous les écrans, afin d'éviter de s'approcher de trop près des présidents et par conséquent assurer leurs arrières.

Les renseignements, la protection des intérêts fondamentaux des Etats :

Nous sommes actuellement dans un monde complexe, avec les frontières de plus en plus difficiles à comprendre. Les militaires sont les seuls qui savent travailler avec des outils dans n'importe quelles situations. Certains groupes criminels, les militaires mais aussi le renseignement utilisent l'open source comme outils pour des logiciels par exemple. Le renseignement est essentiel dans le monde d'aujourd'hui. En moyenne, lorsque les cybercriminels entrent dans une société, ils restent 220 jours pour connaître une entreprise dans son intégralité sans que les directeurs n'aient eu le temps de les identifier. En fonction de ce qu'ils vont trouver, ils effectuent un travail d'observation sur la manière dont les directeurs travaillent et leur objectif va être de trouver une forme d'attaque par la cyberattaque.

Le groupe « High », un groupe cybercriminel très important, ont réussi à bloquer tous les hôpitaux de deux états américains. La cyberguerre ne concerne pas uniquement les militaires et les états mais aussi les entreprises et chacun d'entre nous. Les renseignements ont pu suivre ceux qui ont hacké une fois l'ensemble des clients de Dominos Pizza, ils ont vendu les fichiers à un autre groupe de cybercriminel et demanda une rançon aux clients.

Ce qui est important dans ce type de guerre est de la comprendre, transmettre ce message en comprenant et en se sensibilisant, en ayant une formation nécessaire pour éviter ces erreurs. C'est souvent une erreur personnelle d'un des salariés dans une entreprise ayant commis une erreur comme le fait de cliquer sur le mauvais lien.

Au-delà de cette nécessité d'information sur cette guerre, une multitude de documents sortent sur ce sujet par exemple : « comment se défendre dans une toute petite entreprise ? ». Il faut avoir un esprit de défense, dans ce combat terrible contre les attaquants tout le monde est concerné, la faille se trouve dans chacun d'entre nous. Les cyberguerres se font, pour notre part c'est-à-dire la France, en défensive, apprendre à se défendre au niveau individuel mais aussi collectif est d'une haute nécessité dorénavant.

Les problématiques des entreprises et des services de renseignement des états :

Les services de renseignement sont redoutablement efficaces (russes, chinois). 50% des attaques viennent des autres entreprises, 20% des pays ennemis et 30% des entreprises étrangères. Pegasus est un logiciel espion visant à surveiller des personnes potentiellement terroristes, cependant il ne pouvait pas espionner les téléphones ayant un suffixe anglais et américain. Le DNB allemand ont été pris en flagrant délit à écouter les Français, pareillement pour les Anglais. En cyber, il faut savoir que l'on ne peut pas tout empêcher. Pour ne pas être attaqués, ces services vont sous-traités aux autres les attaques qu'ils veulent mener à l'extérieur.

L'évolution d'outils plus performants :

Les Américains utilisent 60 000 hackers, les Russes utilisent des mercenaires ou des groupes criminels. L'intelligence artificielle et le big data, deux nouveaux outils qui ont eu un résultat fantastique pour nous tous. Plus on a d'informations, plus on réduit la marge d'incertitude (10%) de nos formations.

Dans les cyberguerres, nous faisons de moins en moins d'erreurs en utilisant les outils et techniques qui s'améliorent, nous en sommes qu'au début. Lors de l'utilisation des outils dans plusieurs sites de localisation, chaque flux dans d'un outil à un autre peut-être une cible, cela devient donc de plus en plus compliqué.

Réponses aux questions posées :

La limitation étatique sur Internet : la Chine interdit certains logiciels et systèmes, les Etats-Unis font de même comme la suppression de Tik tok car ils soupçonnent les Chinois d'espionner via cette application. Cependant lorsque certains programmes sont réellement pernicieux, il faut savoir les interdire. Il faut être prudent, dans certains cas être plus autoritaires, pour ne pas tomber dans un système totalitaire pour le cas de la France, le cyber est totalitaire en tant que tel. Lorsque l'on partage des données que ce soit de bonne foi ou non, il faut se demander ce qu'ils vont en faire, c'est-à-dire prendre du recul avant d'agir.

Les problématiques des réseaux sociaux : ils sont en train de devenir des moyens indispensables de communication, ils jouent un rôle d'échanges d'informations très importants, nous sommes dans un monde dans lequel nous ne voyons plus les autres. Cependant avec nos méthodes de travail, on a besoin de communiquer (travail à distance), le réseau social est le moyen de s'exprimer pour une personne qui n'a pas d'interlocuteurs. La contrepartie est le risque, lorsque des personnes malveillantes peuvent manipuler les gens en ayant les discussions des autres. Il faut donc les contrôler, ce qui est d'une haute nécessité. L'information fait partie des réseaux, les personnes vont les privilégier pour se renseigner car il y a une désinfection de l'information sur les télés, les journaux. Ils veulent de l'information brute, des articles courts. Le deuxième risque est que si dans les informations il y a des fakes news, les personnes vont donc les mémoriser et continuer à y croire. Les réseaux doivent respecter un certain nombre de règles, sinon cela peut entrainer des conséquences tragiques sur les populations.

Il existe plusieurs offensives qui touchent de manière directe et indirecte les services de renseignement : seuls les renseignements français n'ont pas eu de problèmes jusque-là contrairement aux Américains, Chinois et Russes par exemple.

Des projets d'avenir : Blockchain, cryptomonnaie : Blockchain est un système très sécurisé, l'ensemble des banques ont choisi ce système en sécurisant les échanges. Cela va nous simplifier la vie, c'est un projet d'avenir.

Le problème de la justice est que nos lois sont inadaptées par rapport au monde actuel du cyber. La fraude au président, c'est le vendredi soir en tant qu'un patron d'entreprise, arrive un message sur internet au responsable comptable, lui disant de virer une certaine somme sur un compte. L'hacker se fait passer pour le patron et donc la responsable vire cette somme en croyant que c'est une mission venant de lui-même. Les rois du cyber sont les gendarmes, ils sont en avance sur tout le monde et détiennent de nombreux outils pour trouver les informations dans le but d'arrêter les criminels.

Influence et dissuasion : Il y a-t-il un moyen de gagner la guerre ? Il faut que l'influence soit crédible en partant d'un fait réel et ajouter dessus des choses crédibles cependant qui vont en changer les indications. Grâce aux réseaux sociaux les Russes, ont pu envoyer un message a de nombreux Américains d'une retranscription d'un mail entre Hillary Clinton et son directeur de campagne, elle parlait d'une manière péjorative de ses concurrents voulant se présenter aux élections.

La souveraineté dans le cyber est détenue par les Américains à 90%, ils détiennent un cloud permettant aux services américains de regarder à n'importe quel moment les données de sa population. Les cloud français sont plus sécurisés et respecte la confidentialité des datacenter.

WURTZ Inès