PROGRAMME ASIE

LA CYBERGUERRE ET LA STRUCTURATION DES RELATIONS INTERNATIONALES : LE CAS NORD-CORÉEN

PAR EMMANUEL MENEUT

SPÉCIALISTE DES QUESTIONS ÉCONOMIQUES ET TECHNOLOGIQUES
EN ASIE ORIENTALE ET EN CYBERDEFENSE

DÉCEMBRE 2017

ASIA FOCUS #54

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

En résumé, nous explicitons la séquence des récents événements entre la Corée du Nord et les Etats-Unis dans le cadre de la diplomatie coercitive. Nous constatons que le recours quasi systématique aux cyber-armes renforce dans un premier temps la probabilité de succès de cette stratégie. Cependant, l'utilisation généralisée à des cyber-armes déstabilise le rôle des systèmes conventionnels tel que les missiles/anti-missiles dans l'élaboration de l'équilibre des forces et elles fragilisent le rôle de la dissuasion nucléaire. Cette nouvelle configuration accroit finalement le risque de conflit. Ainsi, la généralisation des cyber-armes devient un élément structurant pour les relations internationales dans le cadre de la diplomatie coercitive. Leur utilisation conduit à déplacer la réponse de l'Etat ciblé dans le champ des activités économiques afin de décrédibiliser cette forme nouvelle de menace. Ce couplage des enjeux de sécurité et économiques est porteur de modifications profondes des interdépendances de la globalisation des marchés.

Nous explicitons la séquence des récents événements entre la Corée du Nord et les Etats-Unis dans un cadre de diplomatie coercitive. Nous constatons que le recours quasi systématique aux cyber-armes renforce dans un premier temps la probabilité de succès de cette stratégie. Cependant, la généralisation recours à ces cyber-armes déstabilise le rôle des systèmes conventionnels tel que les missiles/anti missiles dans l'élaboration de l'équilibre des forces et elles fragilisent le rôle de la dissuasion nucléaire. Cette nouvelle configuration accroit finalement le risque de conflit. Ces conséquences conditionnent un comportement des Etats plus agressifs dans d'autres secteurs de la sécurité. Ainsi, la conflictualité est étendue aux activités économiques de l'acteur à l'origine de la stratégie coercitive.

LES ENJEUX DU CYBER ESPACE DANS LES RELATIONS INTERNATIONALES SELON L'APPROCHE RÉALISTE

Depuis 2010, après l'attaque des centrifugeuses iraniennes avec la cyber arme « Stuxnet », le potentiel de destruction d'une cyber-arme est avéré et croissant. Les derniers développements technologiques ont permis aux grandes puissances numériques d'intégrer dans leur arsenal des cyber-armes « tueuses » de centrales électriques. Ainsi, l'extension du cyber espace à l'ensemble des activités humaines rend possible en permanence et de façon imprévisible pour un adversaire de « détruire une infrastructure vitale, en bénéficiant d'un anonymat presque total. Des réseaux électriques pourraient être mis en surtension et des centrales électriques hors d'usage par des actions entreprises exclusivement à l'extérieur du territoire physique d'une nation. » (KISSINGER, 2014) p325 C'est une problématique classique des affaires stratégiques. L'enjeu du cyber espace est de même nature que celui induit par la rupture technologique des armes nucléaires à l'aube de la Guerre Froide: « Comme lors de toutes les innovations technologiques, il sera difficile de résister à la tentation de profiter de ce nouveau domaine pour prendre un avantage stratégique. » (KISSINGER, 2014) p323.

Selon H. Kissinger, le moteur de cette dynamique est la nature des cyber-armes. Elles permettent des cyber-attaques en permanence, autant en temps de paix que de guerre car elles sont difficiles à attribuer. Le cyber espace devient donc un environnement très similaire à l'état de nature théorisé par Hobbes. (KISSINGER, 2014) p324 L'anonymat des cyber-armes est un outil efficient des rivalités dans l'environnement anarchique de la société internationale, l'affrontement permanent des grandes puissances numériques.

LA DIPLOMATIE COERCITIVE : LE CAS DE LA CORÉE DU NORD

Notre propos est d'évaluer le rôle des futures cyber-attaques dans la continuité de « Stuxnet » ou de « Wannacry » et notamment le conditionnement des stratégies entre les Etats telle que la diplomatie coercitive. Nous rappelons les caractéristiques de cette approche puis nous illustrons sa mise en œuvre par les Etats Unis sur la Corée du Nord.

La diplomatie coercitive est une stratégie qui conduit l'adversaire à changer son comportement grâce à la menace d'utiliser la force. Elle permet d'obtenir un résultat très important (+$10) avec un coût très faible. Cependant, sa probabilité de succès est faible (p = 0.1) et en cas d'échec le recours à la force est une nécessité dont le coût est élevé (-$10). La guerre à grande échelle est alors un échec de la diplomatie coercitive. Il faut toujours garder le contrôle des conséquences de la menace. La stratégie de pression économique a le même objectif, avec une probabilité de succès plus importante (p' = 0.5) et en cas d'échec la perte concerne simplement les échanges commerciaux (-$5).

Plus précisément, si nous modélisons la situation entre les Etats-Unis et la Corée du Nord sous la forme d'un dilemme de sécurité concernant le choix de la stratégie nous avons :

		Corée du Nord	
		Maintien du pg nucléaire	Changement comportement
US	Diplomatie coercitive	(-$10,$10)	($10,-$10)
	Pression économique	(-$5,$10)	($10,-$10)

Ainsi, l'utilité espérée de cette situation décisionnelle est :
EU(diplomatie coercitive) = - 0.9 x $10 + 0.1 x $10 = -$8
EU(pression économique) = - 0.5 x $5 + 0.5 x $10 = +$2.5
Et sous un voile d'ignorance complet concernant le point de vue Coréen, nous avons :
EU(Maintien du pg nucléaire) = 0.5 x $10 + 0.5 x $10 = +$10
EU(Changement comportement) = - 0.5 x $10 - 0.5 x $10 = -$10

Ce qui conduit les dirigeants américains a rationnellement choisir la stratégie des pressions économiques et les dirigeants Coréens à maintenir leur programme nucléaire militaire.

Afin d'accroitre la probabilité de succès de la diplomatie coercitive une utilisation limitée de la force peut être envisagée. (ART, mai 2003). D'où la problématique que nous examinons dans la suite de cette note, quel usage des cyber-armes pour élaborer la menace de la diplomatie coercitive ? Une cyber-attaque est-elle un moyen efficace d'un usage limité de la force ? Pour cela, elle doit rester sous le contrôle de son auteur et elle ne doit pas entraîner de victimes ou de dégâts similaires à une attaque conventionnelle. Sans contrôle des conséquences des effets de la cyber-arme, elle n'est pas un moyen de la diplomatie coercitive mais d'escalade et de conflit.

Les conditions de succès d'une cyber-attaque sont :

- dans la sphère publique, le doute sur l'origine doit être toujours possible afin de ne pas mettre l'attaquant en position d'accusé public, de perdre la face
- Maitriser la communication dans la sphère publique et disposer de capacité de conditionnement de l'opinion publique pour ne pas être « entrainé » vers une escalade
- Les conséquences doivent être sous contrôle de l'attaquant et il doit avoir la capacité d'y mettre fin à tout moment
- L'impact de la cyber-attaque doit être convaincant en termes de nombre de cibles mais sans effet réel, afin de démontrer simplement la capacité d'attaque à travers des nuisances

Numériquement, si la probabilité de succès de la diplomatie coercitive augmente, par exemple p=0.7, alors nous avons :
EU(diplomatie coercitive) = - 0.3 x $10 + 0.7 x $10 = +$4
EU(pression économique) = - 0.5 x $5 + 0.5 x $10 = +$2.5
Et la diplomatie coercitive devient une stratégie préférée aux simples pressions économiques.

LA STRATÉGIE AMÉRICAINE INITIALE : LES PRESSIONS ÉCONOMIQUES ET LA SÉCURITÉ RÉGIONALE

La pression économique américaine sur la Corée du Nord vise des entreprises coréennes mais aussi chinoises. Par exemple, l'entreprise chinoise Limac et la nord-coréenne Ryonbong General avait établi une joint-venture en 2008 pour l'extraction de tantale, de niobium et de zirconium qui sont des matières premières critiques pour les smartphones, les ordinateurs, les réacteurs nucléaires et les missiles. L'entreprise Limac

avait un partenaire à Houston et importait du matériel canadien de construction dans le domaine nucléaire. La joint-venture a été identifié par le cabinet d'intelligence économique Sayari Analytics qui travaille pour le gouvernement américain et le secteur financier. Les Etats-Unis ont sanctionné ces entreprises en 2005, suivi par l'ONU en 2009. Les actions américaines ciblent directement les dirigeants d'entreprises tant chinois que coréen à partir des liens entre les entreprises sino-coréennes. (PAGE & SOLOMON, 9/5/2017)

Au mois de juillet 2017, le tir d'essai de missile HAWSONG 12 a volé 47 minutes, il a atteint une altitude de 3 724 km et il a parcouru une distance de 998 km, ce qui démontre sa capacité à atteindre l'Alaska. Après ce tir, les Etats-Unis ont choisi de renforcer les pressions économiques à travers des sanctions internationales pour convaincre la Chine et la Corée du Nord de modifier leur comportement déstabilisant pour la sécurité régionale. (RESTUCCIA & DAWSEY, 31/7/2017).

Plus précisément, la pression américaine s'exerce en priorité sur la Chine avec le lancement d'une enquête sur les pratiques commerciales de Pékin dont les conclusions autoriseraient le président Trump, selon la section 201 du Trade Act de 1974 à prendre des mesures unilatérales de rétorsion. C'est un moyen de pression économique plus fort que par le passé, il est associé directement à l'inaction de Pékin face à Pyongyang et son programme nucléaire. (BRADSHER, 1/8/2017).

Ainsi, l'administration Trump continue de cibler des entreprises chinoises, hormis de grandes banques chinoises concernées par la dette américaine. Celles qui aident Pyongyang à développer son programme nucléaire. La Chine est le principal partenaire commercial de la Corée du Nord, les échanges sino-coréens ont augmenté de 37% au 1er trimestre 2017. (ALLEN-EBRA HIMIAN, 13/7/2017) L'administration Trump a aussi autorisé des ventes d'armes à Taïwan ainsi que des manœuvres en Mer de Chine. De plus, elle a finalisé le déploiement du système anti missile Terminal High Altitude Area Defense (THAAD) en Corée du Sud dans le district de Cheongju, ce qui est perçu par les russes et les chinois comme une déstabilisation de l'équilibre stratégique de la région. La Chine craint l'effondrement du régime nord-coréen, ce qui signifierait des millions de réfugiés sur son territoire et des soldats américains sur la rivière Yalu en cas de réunification.

LA STRATÉGIE AMÉRICAINE : LA DIPLOMATIE COERCITIVE

Cependant, cette stratégie de pressions économiques est renforcée par une approche plus coercitive. En effet, à partir de 2014, le président Obama faisait évoluer significativement la stratégie américaine anti missile vers une utilisation de cyber-armes

au lieu de systèmes antimissiles conventionnels. (RYALL J. , 64/2017) C'est le début des actions dans le cyber-espace avec des campagnes cybernétiques de sabotage des essais de missiles dans la continuité du programme « Olympics game ». (CORNET, 2017) Ce programme lancé sous l'administration W. Bush et poursuivis sous l'administration Obama produisit la cyber-arme « Stuxnet » pour saboter les centrifugeuses du programme d'enrichissement nucléaire iranien. Ainsi, selon le New York Times, les Etats-Unis ont lancé la stratégie « left of launch » dont l'objectif est de saboter et « d'abattre le missile avant son lancement ». (ELLISON, 2015).

A l'aide de systèmes de guerre électronique (propagation d'ondes électromagnétiques qui interfèrent avec les communications entre le missile et son centre de commande et de guidage) activés dès le lancement du missile ou de cyber-armes introduites dans les composants électroniques utilisés par les ingénieurs nord-coréens qui interfèrent avec le système de contrôle et de commande du missile, celui-ci est détourné ou détruit. (LINDSAY & GARTZKE, 15/3/2017). En effet, l'ensemble des composants électroniques complexes doivent être importé par la Corée du Nord. Les sanctions sont un outil de contrôle de ces importations. Elles sont utilisables par les américains pour laisser passer uniquement des composants infectés par des cyber-armes. (RYALL J. , 64/2017)
Le secrétaire aux Affaires étrangères britannique Sir Malcolm Rifkind déclarait à l'issue d'un échec de tir de missile nord-coréen, « les Etats-Unis à l'aide de méthodes cybernétiques ont réussi à plusieurs occasions à interrompre ces tests et provoquer leur échec » (RYALL, SMITH, & MILLWARD, 16/4/2017) Entre 2014 et 2017 près de 90 missiles sont lancés avec un taux d'échec de 88% pour le missile de type BM-25 MUSADAN dont la portée permet d'atteindre Guam[1]. (SANGER & BROAD, 18/4/2017) Le programme nucléaire nord-coréen semble souffrir d'un taux élevé d'échecs. (RYALL J. , 64/2017) Toutefois, la difficulté reste d'évaluer réellement l'impact de cette nouvelle capacité.

Cette composante cybernétique vient s'ajouter aux autres capacités développées comme le THAAD. Ce système anti missile de batteries terrestres cible les missiles balistiques à proximité de leur cible. Cependant, la grande vitesse des missiles dans leur phase finale, 4 miles par seconde, réduit l'efficacité de ces systèmes conventionnels. THAAD est couplé avec le système PATRIOTS afin de renforcer son taux de succès. (SANGER & BROAD, 4/3/2017) La défense est complétée avec le système AEGIS BMD et surtout GMD qui interceptent les missiles balistiques durant leur phase endo ou exo atmosphérique (après le lancement et avant d'approcher la cible). AEGIS BMD est embarqué sur des navires de guerre. Les systèmes PATRIOT, THAAD et AEGIS ont une

[1] L'île de Guam se situe dans le Pacifique, il y a 160 000 résidents, c'est le territoire américain le plus éloigné du continent à 3370 km de la péninsule coréenne. Elle a une étendue de 550 km^2. Elle fut conquise en 1898 lors de la guerre hispano-américaine. Depuis sa reconquête en 1944, elle est une des plus importantes bases aérienne et navale américaine qui occupe 30% du territoire où son stationné 6 000 soldats et des bombardiers B52 et des avions de chasses.

portée de destruction respective de 12, 125 et 1350 miles (resp. 19, 200, 2172 km) mais un taux de succès qui n'est pas de 100%.

Les deux derniers tests du missile HAWSONG 12 (en juillet et aout 2017) ont survolé le territoire japonais, le dernier survol date de 2009, pendant plusieurs minutes. La décision de ne pas les abattre fut justifiée par l'absence de charge nucléaire sur ces missiles. Mais la décision de destruction d'un missile balistique n'est pas aussi triviale. Il y a le risque de chute de débris sur les zones urbaines et les populations ainsi que l'explication à fournir si la destruction a échoué ou si la destruction du missile pendant sa phase de vol à haute altitude s'avère impossible. La difficulté avec la défense anti missile concernant un missile nucléaire balistique, c'est qu'il suffit que le taux de succès ne soit pas de 100%, qu'un seul missile puisse franchir le bouclier, pour que le pays ciblé se considère sans défense. (MAULDIN ECONOMICS, 2017).

Ainsi, l'utilisation de systèmes de guerre électronique et de cyber-armes trouve une justification stratégique structurelle qui conduit nécessairement à leur utilisation pour neutraliser les missiles dès leur lancement. En 2017 le Pentagone a officiellement lancé un programme, « Nimble fired », pour généraliser l'utilisation de ces nouvelles techniques cybernétiques et électroniques de destruction de missiles. (SANGER & BROAD, 4/3/2017).

L'élément le plus significatif de cette composante anti missile c'est la publicité que les américains donnent à l'utilisation de cette nouvelle capacité au contraire de l'utilisation de la cyber-arme « Stuxnet » contre le programme nucléaire iranien, notamment à travers le document officiel « The Joint Integrated Air and Missile Defense : Vision 2020 » de 2013 et la déclaration du président Trump en avril 2017. (CORNET, 2017).

L'approche plus coercitive des Etats-Unis à l'égard de Pyongyang et Pékin semble porter ses premiers résultats. Selon l'agence de presse sud-coréenne, les sanctions communes votées par les Etats-Unis et la Chine au Conseil de Sécurité ont conduit à l'expiration progressive des visas octroyés par la Chine à plus de 100 000 travailleurs nord-coréens expatriés sur son territoire qui assurent un transfert de $500 millions en devise en direction de la Corée du Nord. (YONHAP, 3/10/2017).

Supposons que cette nouvelle capacité cybernétique traduise l'intention de l'administration américaine d'obtenir un changement de comportement Nord-Coréen similaire à l'Iran, autrement dit l'utilisation des cyber-armes à des fins de diplomatie coercitive, nous allons examiner les conséquences potentielles sur les relations internationales.

LA RÉPONSE CORÉENNE : « WANNACRY » ET LA COURSE AUX CYBER-ARMES

Il semble que la réponse Nord-Coréenne a commencé à prendre forme avec la cyber-attaque de Sony Picture Entertainment en juin 2014, mais surtout avec la cyber-attaque « Wannacry » en mai 2017 dont l'ampleur et la rapidité sont beaucoup plus importantes.

Selon Europol, l'attaque « Wannacry » a touché des milliers d'ordinateurs dans plus d'une centaine de pays depuis le 12 mai dernier, notamment des acteurs comme Vodafone, Fedex, Renault, National Health Service britannique, Deutsche Bahn, Ministère de la Défense français, Mégaphone, MTS, VimpelCom, ministère de l'Intérieur russe, Sberbank, etc.

Cette cyber arme crypte les fichiers informatiques de l'utilisateur qui doit verser une somme d'argent (ici $300) afin d'y accéder de nouveau. Cette cyberattaque se caractérise plus par son ampleur que par le montant demandé. Les auteurs ont récupéré un butin de $140 000 alors qu'ils ont pénétré plus de 300 000 ordinateurs dans 150 pays. (TRUJILLO, 4/8/2017) Ainsi, cette cyber-attaque a plus un objectif politique, démontrer une capacité de destruction potentielle, que criminel, obtenir un gain financier important. Le fait marquant de cette cyber-attaque est la rapidité et l'ampleur de sa diffusion qui semble toucher principalement l'ensemble des entreprises des pays de la communauté internationale fortement connectés, concernés par le programme nucléaire nord-coréen.

L'origine de cette cyber-arme et le commanditaire de cette cyber-attaque sont associés à la Corée du Nord. Le principe de l'identification du producteur de la cyber-arme est le reverse engineering du logiciel de la cyber-arme. Il s'agit d'examiner le code et de chercher la ressemblance avec les cyber-armes précédentes et leurs auteurs pour identifier le concepteur présumé, notamment à travers les liens sociaux de l'auteur potentiel. Selon les entreprises FireEye, Symantec et Kaspersky, spécialistes de la sécurité informatique, il y a des similarités entre « Wannacry » et des composants utilisés par des hackers nord-coréens. Le virus « Wannacry » contient même des composants logiciels développés et déjà utilisés par la Corée du Nord (GROLL, Security firms tie Wannacry ransomware to North Korea, 23/5/2017). Plus précisément, « Wannacry » utilise un composant (Cheval de Troie) du groupe Lazarus associé à la Corée du Nord. (CAMPBELL, 16/5/2017). En effet, Symantec a établi un lien entre des caractéristiques de « Wannacry » et le groupe Lazarus qui est à l'origine de l'attaque en 2014 contre Sony Picture Entertainment. (GROLL, Security firms tie Wannacry ransomware to North Korea, 23/5/2017) Selon le Director of National Intelligence Dan Coats, la Corée du Nord a bien les capacités de réaliser ce type d'opération. (GROLL, Security firms tie Wannacry ransomware to North Korea, 23/5/2017) Malgré ces

éléments techniques à charge, il est très difficile d'incriminer Pyongyang comme le commanditaire et le bénéficiaire de cette opération. C'est la nature politique de l'attaque qui nous conduit finalement à établir ce lien et à désigner la Corée du Nord comme l'auteur de cette cyber-attaque.

En effet, cette cyber-arme pour une attaque massive dont les conséquences financières sont très limitées est équipée d'un bouton interrupteur, un « kill switch » pour désactiver la propagation du virus et limiter sa diffusion (GROLL, Security firms tie Wannacry ransomware to North Korea, 23/5/2017). Il s'agit donc d'une cyber-attaque avec un objectif plus politique que criminel pour signifier à l'adversaire « je peux frapper massivement vos systèmes informatiques à travers le monde. » Cette cyber-arme a ainsi visé des acteurs étatiques mais surtout non étatiques, principalement des entreprises.

L'IMPACT SUR LES RELATIONS INTERNATIONALES

Par conséquent, le président de Microsoft, Brad Smith, a réagi vivement en accusant la communauté du renseignement et sa propension à identifier des failles dans les logiciels commerciaux et à développer les cyber-armes pour exploiter ces vulnérabilités à des fins de renseignement, de sabotage et de destruction. La NSA accumule la connaissance des failles de sécurité des produits Microsoft pour ses propres besoins. Mais elle ne peut pas garantir l'étanchéité de cet armement. (GROLL, Who is really to blame for the Wannacry ransomware ?, 15/5/2017).

Ainsi, les adversaires de la NSA et de la CIA peuvent dérober ces éléments pour construire eux-mêmes leurs propres cyber-armes qui deviennent très efficaces. (AFP, 15/5/2017) La production de cyber-armes par la NSA conduit nécessairement à des fuites qui sont des sources d'avantages stratégiques pour ses adversaires. Par exemple, la cyber arme « Wannacry » exploite une faille du système d'exploitation Windows XP déjà utilisée par la NSA pour le déplacement de ses cyber-armes dans le cyber espace et nommée « Eternal Blue » dont l'existence avait été révélée en avril 2017 par les groupes de pirates TheShadowBroker et EquationGroup. (CAMPBELL, 16/5/2017)
Selon la logique transcendante suivi par Microsoft, la prise de conscience de ce risque devrait conduire les acteurs concernés à rendre publique toutes les découvertes de failles par les agences de renseignement afin de mobiliser les entreprises informatiques pour mettre au point des parades au plus tôt et renforcer la sécurité de tous les acteurs économiques et sociaux… y compris les adversaires de la communauté du renseignement américain !

Le concept de cyber-sécurité collective a le même défaut que son prédécesseur la sécurité collective. Selon H. Kissinger : « la communauté de force [la SdN] dont parlait

Wilson remplaça la rigidité des alliances [qui avaient conduit à la WWI] par l'imprévisibilité [qui conduit à la WWII] » (KISSINGER, 2014) p.249 En effet, un régime de sécurité collective nécessite d'établir des normes : « la sécurité collective cherche à régler le problème de la violation de normes. Dans la mesure où leur définition est sujette à des interprétations divergentes, le fonctionnement de la sécurité collective est imprévisible » (KISSINGER, 2014) p.250 Au contraire d'une alliance qui repose sur la perception commune d'une menace et qui conduit à des comportements explicites, la sécurité collective doit répondre à la violation d'une règle internationale au cas par cas. (KISSINGER, 2014) L'anonymat des cyber-armes et l'impossibilité de les dénombrer et de surveiller leur production ne permet pas d'établir une norme qui préserve contre l'émergence rapide d'une cyber-arme dont les conséquences ne sont pas couvertes par la norme. Le programme « left of launch » et le recours aux cyber-armes pour améliorer la défense anti-missile illustre cette impossibilité d'une norme face à des ruptures technologiques permanentes. Si les normes ne sont pas une solution pour établir la sécurité dans le cyber espace, elle sera donc le résultat « d'un mélange de dissuasion et de retenue mutuelles, associés à des mesures destinées à éviter une crise due à une mauvais interprétation ou à une erreur de communication. » (KISSINGER, 2014) p326, c'est un retour à la Guerre Froide entre les grandes puissances numériques de la scène internationale. Plus précisément, les cyber-armes sont un outil de la diplomatie coercitive où la guerre est latente et dont l'espionnage et la guerre de l'information sont les caractéristiques saillantes du quotidien des relations internationales.

De plus, la production de logiciels commerciaux s'accompagne d'une diffusion systématique de failles dans la sécurité. Les experts considèrent qu'il y a 15 à 50 failles pour chaque KLOC (kilo de lignes de codes) d'un logiciel produit quels que soient les efforts de tests et de qualité. (GROLL, Who is really to blame for the Wannacry ransomware ?, 15/5/2017).

Le principal levier d'action proposé par Microsoft face à cette réalité, c'est la nécessité pour les clients d'acheter et de mettre à jour régulièrement la version de leurs produits Windows ce qui est parfois plus proche de la vente forcée que de l'échange économique « gagnant – gagnant » étant donné la place du numérique dans les sociétés contemporaines. La production de nouvelles versions s'accompagne de nouvelles failles en permanence. (BIDDLE) C'est une réalité sociale structurelle. Ainsi, l'argument du président de Microsoft ne convainc pas tant que la société internationale sera caractérisée par l'anarchie et la possibilité permanente d'utiliser la force et la ruse. La logique fataliste du réalisme et du dilemme de sécurité à l'origine de la course aux armements s'impose aux grandes puissances numériques.

Aujourd'hui, les cyber-armes telles que « Industroyer » permettent de saboter des réseaux électriques comme ce fut le cas en Ukraine en 2015 et 2016, mais aussi des

réseaux de distribution de gaz, d'eau et les infrastructures du trafic routier. Elles permettent de démontrer sa capacité à toucher l'ensemble des infrastructures vitales d'un pays et de faire pression sur lui pour obtenir un changement de son comportement sur la scène internationale. Cette cyber-arme fut mis au point par le groupe de hackers russes Sandworm à partir de composants dérobés aux américains et aux israéliens. (DESAUNAY, 17/6/2017).

La cyber-attaque « Wannacry » illustre la vulnérabilité de l'ensemble des activités économiques à ce type d'attaque : université, services publics, magasins, hôpitaux, administration, cinéma, notamment aux Etats-Unis mais aussi en Chine, Russie, Japon, Corée du Sud et Singapour, etc. Le coût financier est de l'ordre de $100 millions sans victimes. (CIRENZA, 16/5/2017) Mais une attaque de même ampleur sur des avions, trains, voitures, raffineries, centrales nucléaires, stations de traitement de l'eau, aurait entrainé des conséquences beaucoup plus graves. Comme l'origine de cette cyber-arme est la fuite de certains composants des agences de renseignement ; au niveau de la société internationale et pour rompre la spirale de la logique fataliste, l'ensemble des grandes puissances numériques pourraient envisager la mise en place d'une convention de renoncement aux cyber-armes comme la Convention sur les armes biologiques de 1972 car les cyber-armes sont incontrôlables, non discriminantes et disproportionnées dans leur utilisation. (CIRENZA, 16/5/2017).

Toutefois, la cyber-attaque « Wannacry » montre la capacité de l'auteur à contrôler l'impact à travers un « kill switch », à limiter les conséquences financières de la frappe, et à discriminer entre les systèmes d'informations des acteurs de la société civile et ceux des forces militaires. L'objectif politique de cette attaque du régime nord-coréen c'est d'envoyer un message, « nous pouvons frapper massivement des objectifs économiques en cas d'attaque conventionnelle de votre part » pour « répondre » aux « ingérences » sur son programme nucléaire. La supériorité militaire américaine est « dissuadée » par une capacité de nuisance massive, donc significative, sur son économie.

Ce type d'attaque par ransomware semble traduire l'évolution de la situation des tensions actuelles. La société CheckPoint recense les cibles de cyber-attaque du même type que « Wannacry », 23.5% des organisations internationales ont été visées par la cyber-arme « RonghTed » et 19.7% des entreprises ont été touché par « FireBall », tous deux des cyber-armes de type ransomware. Le pourcentage de ce type d'attaque a doublé par rapport à 2016 à hauteur de 48%. C'est un moyen dual de s'enrichir un peu, donc de financer le développement de cyber- armes et de démontrer ses capacités d'attaque de façon à dissuader un adversaire en ciblant ses acteurs économiques.

Au niveau étatique, selon James Stavridis il est nécessaire de lancer une forte coopération public/privée, une législation pour réduire la responsabilité des entreprises dans le partage contraignant d'informations avec l'Etat, un organisme public de cyber sécurité de l'ordre de 10 000 personnes dans la Silicon Valley pour concrétiser la résilience des services et produits des entreprises du secteur numérique, cette organisme pourra suivre la même trajectoire de l'ICANN qui est désormais une première institution de la gouvernance globale d'Internet, enfin une dissuasion qui repose sur des capacités offensives de cyber-attaques sous la responsabilité du cyber command. (STAVRIDIS, 15/5/2017) Ces recommandations saisissent la particularité de la production des cyber-armes par des Etats. L'enjeu ce sont les entreprises, les groupes non étatiques et leur articulation avec les capacités numériques étatiques. Ainsi, l'administration américaine a récemment supprimé la société russe Kaspersky Lab des listes de fournisseurs dont les produits de cyber sécurité sont approuvés pour les agences gouvernementales car ces logiciels n'assurent pas l'intégrité et la confidentialité des systèmes d'information qu'ils sont censés protéger. (KOLZ & FINKLE, 11/5/2017) Il semble impossible aux acteurs étatiques et aux entreprises d'agir collectivement dans le domaine de la cyber-sécurité.

De plus, l'un des fournisseurs de l'auteur de la cyber arme « Wannacry », le britannique Marcus Hutchins qui avait identifié le bouton interrupteur (kill switch) dont l'activation avait permis de stopper la diffusion massive de cette cyber-arme, a été arrêté pour avoir contribué à la production et la diffusion d'une cyber-arme il y a quelques années (la cyber-arme Kronos du même type que « Wannacry »). Le kill switch se présentait sous la forme d'une adresse Internet dont il avait acheté le nom de domaine (DNS) pour $10 ce qui avait permis de piéger tous les virus « Wannacry » du cyber espace. (TRUJILLO, 4/8/2017) Les acteurs de la société civile ont un comportement classique de « black ops », de double jeu, de la communauté du renseignement.

Les Etats font le constat que la probabilité de succès d'une stratégie coercitive avec une cyber- attaque augmente, comme le succès du programme « Olympics Games » l'avait démontré dans le cas du programme nucléaire iranien. Cela conduit à un dilemme de sécurité tel que nous l'avons formulé au début de cette note. L'accroissement de l'utilisation des cyber-armes pour accroitre le taux de succès de la diplomatie coercitive est une tendance qui se généralise à l'ensemble des grandes puissances numériques. Elle s'observe aussi dans les cas de l'Ukraine et du Qatar.

En juin 2017, la veille de la célébration nationale de l'anniversaire de sa constitution, l'Ukraine a été touché par une cyber-attaque, elle a ciblé les institutions du gouvernement, l'aéroport, le réseau électrique, les transports, les médias et les banques. (TAMKIN, 27/6/2017)] Le ciblage d'acteurs non étatiques fait donc partie des stratégies

d'utilisation des cyber-armes à des fins de diplomatie coercitive. L'Ukraine accuse la Russie qui nie son implication.

Selon le Washington Post, c'est la cyber-attaque contre l'agence de presse gouvernementale du Qatar qui a servi de justification à l'embargo actuellement en cours. Cette cyber-attaque mise en place par les Emirats Arabes unis après la publication par cette agence du discours de l'émir qui soutenait l'idée de reprendre le dialogue avec l'Iran. (DEYOUNG & NAKASHIMA, 16/7/2017) L'Arabie saoudite, Bahreïn, l'Egypte et les Emirats arabes unis ont rompu le 5 juin 2017 leurs relations diplomatiques avec le Qatar et mis en place un embargo, l'accusant de se rapprocher de l'Iran, grand rival régional du royaume saoudien. Il bénéficie de l'appui de la Turquie, la Chine et la Russie. Les 4 pays arabes demandent au Qatar de rompre ses relations avec l'Iran, de fermer la base militaire turque sur son territoire et de mettre fin à sa chaine de télévision Al Jazeera.

Ces deux exemples de diplomatie coercitive illustre le recours aux cyber-armes du type « Wannacry » et le ciblage des acteurs non étatiques. Les limites de l'action collective de la société internationale permettent la généralisation de l'utilisation de cyber-armes pour la diplomatie coercitive à l'ensemble des grandes puissances numériques. Ce dilemme de sécurité devient structurant pour les relations internationales. Cependant, les cyber-armes modifient le rôle des moyens conventionnels et nucléaires comme l'illustre le cas nord-coréen.

LES ENJEUX POUR LA RELATION SINO-AMÉRICAINE : SÉCURITÉ ET ÉCONOMIE

La fragilisation de l'équilibre conventionnel du glaive et du bouclier, de la dissuasion nucléaire et un risque de conflit plus élevé.

Ainsi, au cours du test de missile moyenne portée Nord-Coréen du mois de mai 2017, les américains ont mis en état opérationnel le système anti missile THAAD qui s'ajoute à la présence de 28 000 soldats américains dans le cadre du traité de sécurité avec la Corée du Sud. La Chine a alors considérée cette activité américaine comme une menace pour ses propres capacités de dissuasion et l'équilibre des forces régionales. Selon le spécialiste des Etats-Unis et de l'Asie Barthélémy Courmont, ce bouclier antimissile contre Pyongyang a pour objectif de maintenir la supériorité des capacités militaires américaines sur celle de la Chine et de la Russie. (FEERTCHAK, 28/9/2017).

La Chine a ainsi rappelé aux Etats-Unis que ce bouclier ne modifiera pas significativement les rapports de force régionaux, notamment en Mer de Chine. 4

vedettes des gardes côtes chinois ont rejoint le 25 septembre 2017 la zone d'accostage des îles Diaoyu/Senkaku selon l'administration océanique de la Chine afin d'effectuer une inspection de routine. Ces îles de la Mer de Chine sont aussi revendiquées par le Japon et une protestation diplomatique fut émise. En 2008, la Chine et le Japon étaient tombés d'accord pour exploiter conjointement les ressources pétrolières et gazières autour de ces îles, mais depuis 2010 une succession d'incidents diplomatico-militaires ont fait disparaitre toute coopération économique.

En effet, nous avons vu que les systèmes antimissiles classiques n'étaient pas capables de détruire 100% des missiles balistiques, c'est même l'un des facteurs à l'origine de l'utilisation de cyber-armes par les Etats-Unis, ce constat renforce l'utilité de la dissuasion nucléaire pour le régime nord-coréen. Il a testé la bombe A en 2006, 2009 et 2013. La bombe H fut testée en janvier 2016 et en septembre 2017. De plus, 18 missiles balistiques de courte et moyenne portée furent lancés ce qui porte le total des essais à une trentaine depuis 3 ans (WILLIAMS, 16/8/2017). L'arme nucléaire fait donc partie de la dissuasion crédible de la Corée du Nord et la Chine ne semble pas renoncer à modifier l'équilibre des forces en faveur des Etats-Unis dans son environnement maritime immédiat.

De plus, la course aux cyber-armes fragilise le pouvoir de dissuasion de l'arme nucléaire et rend la possibilité d'une confrontation plus probable. En effet, la dissuasion nucléaire repose sur la transparence et la croyance partagée entre les acteurs que les systèmes de chacun fonctionneront, ainsi aucun n'a intérêt à prendre le risque d'une première frappe. La possibilité que les missiles nord-coréens soient piégés dès leur production rend moins certaine cette relation de dissuasion. La conscience nord-coréenne de la vulnérabilité de ses missiles peut rendre cet acteur plus imprédictible et paranoïaque. (FARLEY, 8/3/2017) De plus, si la Russie et la Chine perçoivent une nouvelle vulnérabilité de leur système de dissuasion, cela fragilise l'équilibre stratégique de la région. La dissuasion nucléaire repose sur une communication précise et transparente entre les acteurs afin d'être efficace et stable. Au contraire, les cyber-armes donnent l'avantage à l'offensive et elles renforcent la ruse et la tromperie dans les relations stratégiques. Ainsi, l'usage des cyber-armes est peut-être à limiter à l'espionnage et la collecte d'informations plus tôt qu'à des fins de menaces pour la diplomatie coercitive car elle rend caduc la dissuasion nucléaire, clé de voûte de l'équilibre des forces et de la sécurité régionale en Asie. (LINDSAY & GARTZKE, 15/3/2017).

Les cyber-armes sont des armes offensives, elles donnent l'avantage à celui qui les utilise le premier. La difficulté, c'est que ces armes qui rendent le succès d'une attaque plus probable, renforcent aussi la probabilité d'en déclencher une.

Pourtant, lors de leur rencontre le 6 et 7 avril 2017 à Mara Lago en Floride, les présidents Xi et Trump avaient abordé à la fois les questions commerciales et géostratégique nord coréennes, selon le ministre des Affaires étrangères chinois, Wang Yi, ils étaient tombés d'accord pour intensifier leur coopération sur ces dossiers. Les sanctions d'abord brandies par l'administration Trump à l'encontre des entreprises chinoises ont été mises de côté afin de convaincre Pékin de coopérer sur le dossier nord-coréen, notamment lors du vote du Conseil de Sécurité. Mais cette position américaine est dangereuse. A long terme, si la Chine restreint la Corée du Nord de poursuivre ses provocations avec ses tirs d'essais, le président Trump sera obligé de ne pas punir la Chine pour ses pratiques commerciales illicites ce qui continuera de peser à moyen terme sur l'économie américaine. A court terme, tant que dure la confrontation entre le président Trump et Kim Jong Un, les menaces de sanctions pour pratiques déloyales sont suspendues. La Chine n'a donc pas intérêt à presser son allier nord-coréen de céder rapidement, et lorsque ce sera le cas, ces menaces de sanctions ne seront plus utilisables. (KUTTNER, 15/8/2017) Ainsi, le recours à une diplomatie coercitive dont la probabilité de succès est renforcée par l'utilisation de cyber-armes, et afin d'éviter une guerre avec la Corée du Nord qui serait un échec de cette diplomatie coercitive, elle aurait des conséquences catastrophiques et immédiate au niveau économique, l'administration Trump n'a pas d'autre choix que de renforcer la dépendance de l'économie américaine à la Chine ! Pour maintenir son rôle de clé de voûte de la sécurité régionale en Asie, le développement des moyens coercitifs cybernétiques renforce la puissance économique de la Chine. ■

BIBLIOGRAPHIE

AFP. (15/5/2017). Cyber-attaque mondiale : Poutine nie la responsabilité de la Russie. *L'Express*.

ALLEN-EBRA HIMIAN, B. (13/7/2017). With possible new sanctions, White House gets serious on China's north Korea ties. *Foreign Policy*.

ART, R. J. (mai 2003). *Coercive diplomacy from the US and coercive diplomacy.* US Institute for Peace.

BIDDLE, S. (s.d.). The real roots of the worldwide ransomware outbreak : militarism and greed. *The Intercept*.

BRADSHER, K. (1/8/2017). Trump administration is said to open broad inquiry into China's trade practices. *New York Times*.

CAMPBELL, S. (16/5/2017). North Korea hacking group is thought to be behind cyber attack which wreaked havoc accross the globe. *The Daily Mail*.

CIRENZA, P. (16/5/2017). Wannacry ransomware should prompt movement toward a cbyer weapons convention. *The Diplomat*.

CORNET, G. (2017). *L'intégration progressive du cyber dans la stratégie américaine.* Mémoire de recherche - ICP - FASSE.

DESAUNAY, D. (17/6/2017). Industroyer, cyber tueur de centrales électriques. *RFI*.

DEYOUNG, K., & NAKASHIMA, E. (16/7/2017). UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials. *The Washington Post*.

ELLISON, R. (2015, 3 16). *Left of launch.* Récupéré sur Alerts - Missile Defense Advocacy Alliance: http://missiledefenseadvocacy.org/alert/3132/

FARLEY, R. (8/3/2017). Left of launch cyber efforts against North Korea : good idea ? *The Diplomat*.

FEERTCHAK, A. (28/9/2017). Corée du Nord, Iran, doit on craindre une prolifération nucléaire dans le monde. *Le Figaro*.

GROLL, E. (15/5/2017). Who is really to blame for the Wannacry ransomware ? *Foreign Policy*.

GROLL, E. (23/5/2017). Security firms tie Wannacry ransomware to North Korea. *Foreign Policy*.

KISSINGER, H. (2014). *World order.* New York: Penguin Press.

KOLZ, D., & FINKLE, J. (11/5/2017). US intelligence briefs say reviewing use of Kaspersky software. *REUTERS*.

KUTTNER, R. (15/8/2017). US vs NK : the winner ? China, . *The Huffington Post,*.

LINDSAY, J., & GARTZKE, E. (15/3/2017). The US wants to stop North Korean missiles before they launch. That may be not be a great idea. *The Washington Post*.

MAULDIN ECONOMICS. (2017, 9 20). *Here's why US missile defense probably won't protect us from a North Korea attack*. Récupéré sur Business insider:

http://www.businessinsider.com/north-korea-attack-might-not-be-defended-by-us-missile-defense-2017-9?IR=T

PAGE, J., & SOLOMON, J. (9/5/2017). Venture undeterred by North Korea sanctions. *Wall Street Journal*.

RESTUCCIA, A., & DAWSEY, J. (31/7/2017). Trum plan on China may come as soon as this week. *Politico*.

RYALL, J. (64/2017). US Cyberattacks may be bringing North Korean missiles down. *The telegraph*.

RYALL, J., SMITH, N., & MILLWARD, D. (16/4/2017). North Korea's unsuccessful missile launch may hvae been thwarted by US cyber attack. *The Telegraph*.

SANGER, D., & BROAD, W. (18/4/2017). Hand of US leaves North Korrea's missile program shaken. *The New York Times*.

SANGER, D., & BROAD, W. (4/3/2017). Us strategy to hoblle North Korea was hidden in plain sight. *The New York Times*.

STAVRIDIS, J. (15/5/2017). The US is not ready for a cyber Pearl Harbor. *Foreign Policy*.

TAMKIN, E. (27/6/2017). , Ukraine hit by massive cyber attack. *Foreign Policy*.

TRUJILLO, E. (4/8/2017). Les hackers de la cyber-attaque Wannacry récupèrent leur butin. *Le Figaro*.

WILLIAMS, I. (16/8/2017). *North Korea missile lounches : 1984-Present.* Center ofr Strategic and International Studies - Missile Defense Project.

YONHAP. (3/10/2017). N. Korean workers in China return home amid tougher sanctions. *Yonhap*.

ASIA FOCUS #54

LA CYBERGUERRE ET LA STRUCTURATION DES RELATIONS INTERNATIONALES : LE CAS NORD-CORÉEN

Par Emmanuel MENEUT/ Spécialiste des questions économiques et technologiques en Asie orientale et en cyberdéfense.

DÉCEMBRE 2017

ASIA FOCUS
Collection sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférence à l'Université catholique de Lille, et Emmanuel LINCOT, Professeur à l'Institut Catholique de Paris – UR « Religion, culture et société » (EA 7403) et sinologue.
courmont@iris-france.org – emmanuel.lincot@gmail.com

PROGRAMME ASIE
Sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférence à l'Université catholique de Lille
courmont@iris-france.org

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES
2 bis rue Mercoeur
75011 PARIS / France

T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org