DGRIS
Direction générale des relations internationales et de la stratégie
MINISTÈRE DE LA DÉFENSE

ETUDE PROSPECTIVE ET STRATEGIQUE

DESCRIPTION DE LA MANIERE DONT LA CYBERCRIMINALITE ET LA LUTTE INFORMATIQUE SONT ABORDEES PAR LES ACTEURS POUVANT INFLUENCER LE DOMAINE

(SYNTHESE)

Mars 2015

N° 2014 1050029622 – EJ court 1505280001

Compagnie européenne d'intelligence stratégique
CEIS

Le ministère de la Défense fait régulièrement appel à des études externalisées auprès d'instituts de recherche privés, selon une approche géographique ou sectorielle, visant à compléter son expertise interne. Ces relations contractuelles s'inscrivent dans le développement de la démarche prospective de défense qui, comme le souligne le dernier Livre blanc sur la défense et la sécurité nationale, « *doit pouvoir s'appuyer sur une réflexion stratégique indépendante, pluridisciplinaire, originale, intégrant la recherche universitaire comme celle des instituts spécialisés* ».

Une grande partie de ces études sont rendues publiques et mises à disposition sur le site du ministère de la Défense. Dans le cas d'une étude publiée de manière parcellaire, la Direction générale des relations internationales et de la stratégie peut être contactée pour plus d'informations.

AVERTISSEMENT : Les propos énoncés dans les études et observatoires ne sauraient engager la responsabilité de la Direction générale des relations internationales et de la stratégie ou de l'organisme pilote de l'étude, pas plus qu'ils ne reflètent une prise de position officielle du ministère de la Défense.

Description de la manière dont la cybercriminalité et la lutte informatique sont abordées par les acteurs pouvant influencer le domaine

ceis

L'intelligence de l'Information

Introduction

1.1 Contexte

- **Plusieurs acteurs prennent position sur le sujet de la lutte contre la cybercriminalité et la cyberdéfense et essaient d'influencer les politiques des Etats :**
  - Société civile : ONG, associations , hacktivistes et hackers
  - Acteurs du tissu économique

- **On distinguera 3 problématiques**
  - Comment appréhender le flot d'annonces officielles et non officielles issues d'acteurs étatiques ?
  - Quels enseignements tirer de ces annonces ?
  - Ces déclarations sont-elles annonciatrices de risques majeurs ou surfent-elles uniquement sur un effet d'annonce dissuasif ?

ceis

Introduction

1.2 Objectifs et méthodologie

- **Analyser la perception que les acteurs ont du sujet et leur capacité d'influence**

- **Démarche plus globale de guerre de l'information**
  - Pour justifier et faire accepter par les opinions publiques l'éventualité de conflits dans le cyberespace
  - Pour contribuer à la stratégie de dissuasion « floue » des Etats
  - Pour développer une nouvelle forme de citoyenneté

- **Plusieurs étapes sont nécessaires :**
  - Echantillonnage : recueil d'informations auprès d'un panel d'acteurs et de sources d'information représentatifs. Confronter les postures officielles avec celles des acteurs
  - Identification des arguments, leviers et facteurs d'influence : identifier les rôles des acteurs tiers et leur évolution dans le temps
  - Evaluation des risques et des conséquences de la LIO

ceis

PARTIE 1 : Etats des lieux des postures

ceis
L'intelligence de l'Information

Cas d'étude

1.1 Daesch et la guerre de l'information

- **Mouvement général de dépréciation des activités du groupe islamiste**
  - Condamnation des actes via les réseaux sociaux
  - Promotion de la non-diffusion de vidéos ou images publiées par Daesch

- **Point de vue académique et médiatique**
  - Comprendre quelles sont les tendances et stratégies de communication de l'Etat islamique sur internet
    - ✓ Discours destiné aux potentiels combattants : recruter de nouveaux membres
    - ✓ Discours adressé aux « ennemis » : choquer et instaurer un sentiment de terreur

- **Point de vue étatique**
  - Renforcement global du système législatif
  - Blocage des réseaux sociaux (Irak), renforcement des dispositifs de sécurité sur internet (Etats-Unis, Canada, Royaume-Uni, France), plateformes de contre-propagande

- **Point de vue du secteur industriel :** refus de parler de « cyberguerre »

ceis

Cas d'étude

1.2 La LPM et l'échec de la mobilisation de la société civile

- **Loi de programmation militaire (LPM) 2014-2019**
  - Modification des textes pour augmenter les capacités des autorités sur internet
    - ✓ Article 20 : possible collecte de données en temps réel sur les réseaux des FAI sans contrôle judiciaire
- **Réactions :**
  - Acteurs étatiques
    - ✓ Nécessité de renforcement des mesures de sécurité
    - ✓ Partisans pour et contre un « *Patriot Act* à la française »
  - Secteur industriel : remise en cause de l'utilité de la mesure
  - Presse : critique sur la non-consultation de la CNIL et le vote en procédure accélérée
  - Société civile : possible déclenchement de la QPC
- **Impact :**
  - Le vote de la LPM a alimenté l'opposition
    - ✓ Manque de clarté sur de nombreux points
    - ✓ Non consultation de nombreux acteurs concernés
    - ✓ Absence de contrôle judiciaire

ceis

Cas d'étude

1.3 OpFrance, la bataille sémantique

- **Opération Charlie Hebdo lancée par les *Anonymous* après les attentats**
  - Risque de perturbation des enquêtes policières
- **<u>Gouvernement français</u>**
  - L'ANSSI a indiqué les étapes de base à prendre en matière de cybersécurité
  - Version numérique du Plan Vigipirate
    - ✓ Priorité aux opérateurs d'importance vitale, aux ministères et aux forces de l'ordre
  - Posture de relativisation
    - ✓ Attaques sur des cibles faciles de faible niveau perpétrées par n'importe quel « geek »
- **<u>Autres acteurs</u>**
  - Experts en sécurité des SI
    - ✓ Moyens techniques faibles (DDoS, défiguration)
  - Victimes
    - ✓ Perturbation des plateformes des localités pendant quelques jours
    - ✓ Absence de vol de données

ceis

Cas d'étude

1.4 Sony, un cas d'étude structurant et regroupant des réactions de divers acteurs

- Réactions et outils d'influence utilisables lors de cyberconflits
  - Pression humoristique et soft power via création artistique
  - Pression cyber par l'outil de l'arme informatique
  - Pression économique par le ralentissement de l'activité d'une entreprise structurante
  - Pression en termes d'image pour l'entreprise
  - Pression en termes d'image pour le pays dont cette entreprise est l'avatar (Hollywood et USA) : s'attaquent à un symbole du soft power américain
  - Pression humaine sur les salariés de l'entreprise : données personnelles + licenciements et démissions
  - Pressions juridiques et judiciaires de la part des Etats-Unis
  - Présentation de faisceau d'indices pour l'attribution désignée
  - Usage des entreprises tiers pour justifier l'attribution (Taia global, etc.)
  - Riposte informatique : usage de l'attaque DDoS pour sanctionner la Corée du Nord et démonstration de force
  - Riposte diplomatique avec des sanctions à l'échelle internationale par les Etats-Unis

Postures par pays

1.1 L'Allemagne

1 **ABSTRACT**	• Cible privilégiée de la cybercriminalité • Peu d'informations sur ses capacités offensives • Communication sur la protection de la vie privée et des libertés en ligne
2 **STRATÉGIE PARTICULIÈRE**	• Place prépondérante dans la coopération internationale • Convaincre de la gravité de la situation avec peu d'informations sensibles • Nouvel ordre de gouvernance (Task force de l'Union Européenne) • Développement de ses propres capacités d'interception
3 **DEPENDANCE DES ETATS-UNIS**	• Coopération entre l'Allemagne, le Royaume-Uni et les Etats-Unis • Dépendance des renseignements américains et britanniques • Ancien hacktivisme très actif (1989)
4 **PORTEE DES MEDIAS INDEPENDANTS**	• Engagement envers la communauté activiste et hacktiviste • Exposition en raison de ses prises de position (exemple : Ukraine)

ceis

Postures par pays

1.2 Le Brésil

1 ABSTRACT	• Affirmation de ses positions en matière cyber • Montée en puissance des capacités de lutte informatique défensives et offensives • Position ferme à l'égard des Etats-Unis
2 COUPE DU MONDE	• Forces armées au cœur de la cyberdéfense et des infrastructures critiques • Militarisation du cyberespace • Explosion du nombre de revendications hacktivistes • Test d'un simulateur de cyberguerre jugé disproportionné
3 REVELATIONS D'E. SNOWDEN	• Mise en place d'une commission d'enquête • Alliances régionales contre l'espionnage américain • Vote de mesures structurelles juridiques • Abandon de la proposition de loi sur l'hébergement local des données • Volonté de s'isoler et de se protéger de l'espionnage américain

ceis

Postures par pays

1.3 La Chine

1 ABSTRACT

- Annonces et réactions fermes
- Opérations de cyberespionnage industriel étatique
- Indépendance en termes d'infrastructures réseau et d'écosystème de marché

2 ENNEMI PRINCIPAL DES ETATS-UNIS

- Actions de communication de la part des Etats-Unis
- Judiciarisation des conflits de cyberespionnage
- Escalade de réactions contre les produits américains
- Indépendance vis-à-vis des Etats-Unis

3 STRATEGIE DE COMMUNICATION

- Absence d'écosystème cybercriminel ou hacktiviste audible
- Vote de mesures structurelles juridiques
- Logique de réponse diplomatique et économique « *no business* »
- Démarche cyber offensive assumée

ceis

Postures par pays

1.4 La Corée du Nord

1 ABSTRACT	• Faiblesse de ses infrastructures et de ses capacités internes • Position « d'ennemi à craindre » sur le plan cyber à l'échelle internationale • Puissance de ses alliés et soutiens (Chine, Russie)
2 STRATEGIE DE COMMUNICATION	• Très peu d'informations • Allégations quant au piratage de la firme japonaise Sony Entertainment • Sanctions économiques et diplomatiques fortes des Etats-Unis à l'encontre du pays
3 SITUATION	• Capacités internes avec des profils mobilisés et dédiés à la cybersécurité offensive • Soutiens et infrastructures alliées pour pallier à ses lacunes • Absence de surface de vulnérabilités importante : absence d'infrastructures sensibles connectées, absence de dépendance accrue aux systèmes d'information connectés au quotidien et faibles conséquences en cas de riposte informatique

ceis

Postures par pays

1.5 Les Etats-Unis

1 ABSTRACT	• Absence de modifications de leur système d'espionnage massif • Stratégie de communication globale : soft power et hard power • Moyens d'influence conventionnels et judiciaires • Implication des acteurs privés aux cœur de sa stratégie (Facebook, Google, Apple, Microsoft, Crowdstrike)
2 MISE EN OEUVRE	• Volonté de judiciariser l'espionnage • Plusieurs types de riposte : économique, judiciaire, technique et diplomatique
3 STRATEGIE DE COMMUNICATION	• Mise en avant de leurs capacités technologiques et offensives par la DARPA • Focus sur quelques pays considérés comme des ennemis (Chine, Russie, Iran et Corée du Nord) • Hébergement d'une forte communauté hacktiviste • Avantage par la maîtrise des données, des protocoles et des infrastructures physiques • Exposition de la menace légitimant toute action défensive

ceis

Postures par pays

1.6 L'Iran

1 **ABSTRACT**	• Le pays souhaite se positionner sur le terrain de l'affrontement asymétrique, position agressive dans le cyberespace • Riposte commerciale, diplomatique, informelle et cyber • « Si les Etats-Unis arment l'Ukraine, la Russie arme l'Iran »
2 **ESQUISSE D'UNE STRATEGIE**	• Communication sur le développement de ses capacités de riposte informatique • Stratégie de riposte et de montée en puissance • Relations avec la Syrie, la Corée du Nord et la Chine • Ambition de créer un « internet iranien » • Volonté d'affirmer sa maîtrise du réseau en refusant puis acceptant les technologies étrangères et en bloquant certains protocoles
3 **VOLONTÉ DE PESER SUR LE TERRAIN CYBER**	• Volonté de porter devant les tribunaux l'affaire *Stuxnet* qualifiée d'agression armée
4 **DYNAMIQUE DE RIPOSTE**	• Opération Cleaver menée par l'Iran fin décembre 2014 à l'encontre d'acteurs occidentaux militaires de différents secteurs (énergie, transport, hôpitaux) • Piratage d'Adelson Sands Corp.

ceis

Postures par pays

1.7 Autres pays

- **Estonie**

Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	OTAN	Europe			Japon

- **Corée du Sud**

Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	-				
Cibles potentielles/ pays ennemis	Corée du Nord	Chine			

- **Royaume-Uni**

Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Etats-Unis	Europe	OTAN		
Cibles potentielles/ pays ennemis	Iran	Corée du Nord	Chine		

ceis

Postures par pays

1.7 Autres pays

- **Israël**

Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Etats-Unis	Europe			
Cibles potentielles/ pays ennemis	Iran	Corée du Nord	Chine		

- **Russie**

Dynamique	Défensive	Offensive	Neutre	Militariste	Montée en capacités
Axes de coopération	Chine	Corée du Nord	Iran	Irak	
Cibles potentielles/ pays ennemis	Etats-Unis et alliés	Israël	Ukraine	Certains pays d'ex-URSS	

ceis

PARTIE 2 : Analyse des risques, conséquences et réactions

ceis
L'intelligence de l'Information

Tendances identifiées et facteurs clés d'évolution

2.1 Fuites de données et guerre de l'information : rôle croissant des hacktivistes

- **<u>Principales actions</u> :**
  - Perturbation massive et soulèvement de foules en ligne (Exemple : Coupe du Monde de football au Brésil) ;
  - Manifestations numériques ;
  - Défiguration des sites internet

- **<u>But</u> : perturber la perception qu'ont les particuliers, les entreprises et les institutions de l'information**
  - Objectifs des *Anonymous* : détruire ou fermer les plateformes de communication ou de relais des messages terroristes ou islamistes
  - Objectifs de la *Goat team* : décrédibiliser le message des djihadistes sur Twitter par l'humour et la dérision

- **Impact considérable de l'affaire Snowden sur la perception des opérations cyber menées par les Etats-Unis**
  - Perte de marchés, de crédibilité, de confiance
  - Montée en puissance du hacktivisme

ceis

Tendances identifiées et facteurs clés d'évolution

2.2 L'incertitude de la notion de cyberterrorisme

- **Notion complexe de « cyberterrorisme »**

- **Absence par l'Etat islamique des capacités pour menacer les infrastructures critiques d'un Etat**
  - Absence des moyens financiers, des moyens humains et des connaissances des systèmes ciblés
  - Pirater un SCADA exige une connaissance accrue du fonctionnement du système
    - ✓ Nécessité de former ses propres membres
    - ✓ Nécessité d'un recrutement exogène de « djihadistes en herbe »
    - ✓ Nécessité d'une mobilisation de hackers experts sympathisants

- **Risque de perturbation massive et d'attaque physique plus classique**

ceis

Tendances identifiées et facteurs clés d'évolution

2.3 Attribution, proxies et espionnage *as a service*

- **Stratégie de « flou » sur les liens entre les Etats et les groupes hacktivistes**
  - Tolérance des Etats de manière passive
  - Soutien des Etats
  - Financement actif par les Etats

- **Logique d'espionnage *as a service* (EAAS)**
  - Faire appel à des acteurs totalement indépendants pour dérober des informations ou procéder à du piratage informatique
  - Brouiller les pistes quand il s'agit d'attribuer les actes à un Etat
  - Présence au sein des conflits internationaux
    - ✓ Russie et Cyber Berkut
    - ✓ Syrie et Syrian Electronic Army

ceis

Tendances identifiées et facteurs clés d'évolution

2.4 Attribution : la dimension juridique tient un rôle essentiel

- **Dimension juridique au cœur des stratégies cyber des Etats**

- **Objectif** : le virus *Stuxnet* ne doit être ni perçu, ni démasqué par les acteurs
  - S'assurer que le virus ne viole par le droit des conflits armés
  - Prévoir des garanties
    - ✓ Anonymat
    - ✓ Discrétion des effets du virus passant pour de simples dysfonctionnements
    - ✓ Eviter de causer des dommages suffisamment graves et quantifiables pour être qualifié d'agression
  - L'influence sur les perceptions des acteurs peut passer par l'absence de perception

ceis

Tendances identifiées et facteurs clés d'évolution

2.5 L'attribution et le cas de la dissuasion

- **Stratégie de communication des Etats** : dissuader l'ennemi d'attaquer
  - Opération *Stuxnet* : juste équilibre entre la force de frappe nécessaire à son efficacité et la discrétion nécessaire à sa durée de vie

- **Discours dual des Etats-Unis**
  - Nier toute implication dans la création du virus *Stuxnet*
  - Faire circuler des informations précises sur la conception du virus

- **Vers une nouvelle forme de dissuasion plus « ouverte » des Etats-Unis ?**
  - Publication d'offres d'emploi tournées vers l'offensif
  - Récents projets de la DARPA

ceis

Tendances identifiées et facteurs clés d'évolution

2.6 Le passif et la crédibilité d'un Etat : l'exemple américain

- **Judiciarisation des cyberconflits par les Etats-Unis**
  - Campagne de communication visant à exposer publiquement les agissements des ennemis
  - Stratégie bien reçue des industriels et de la société civile américaine
  - Perception très négative de la part des officiels menant à des réactions sévères

- **<u>Conséquences :</u>**
  - Perception globale négative de l'activité américaine dans le cyberespace
  - Violation de la vie privée
  - Maîtrise exagérée des infrastructures du cyberespace

ceis

Tendances identifiées et facteurs clés d'évolution

2.7 L'indépendance économique, stratégique, diplomatique et son influence sur les postures

- **Liberté d'action et marge de manœuvre importante de certains Etats (Chine, Brésil) vis-à-vis des Etats-Unis**
  - Indépendance financière, économique, scientifique et en matière de renseignement
  - Rupture des négociations diplomatiques et des échanges commerciaux
  - Indépendance en matière d'infrastructures

- **Manque d'indépendance d'autres Etats (Allemagne)**
  - Dépendance de la coopération entre l'Allemagne, les Etats-Unis et le Royaume-Uni
  - Fin de toute prétention allemande d'enquêter sur les révélations d'E. Snowden

ceis

Tendances identifiées et facteurs clés d'évolution

2.8 Le rôle des entreprises privées

- **Possibilité de faire partie d'un axe de coopération et de jouer un rôle à l'échelle internationale**

- **Maîtrise de la totalité des couches physiques, logiques et sémantiques du cyberespace :**
  - Gestion des infrastructures physiques du cyberespace
  - Gestion des protocoles ou des données et services

- **Renforcement des capacités des Etats par les entreprises de cybersécurité**
  - Etats-Unis et Crowdstrike
  - Russie et Kaspersky

- **Pivot essentiel des entreprises privées sur l'impact des prises de positions des Etats**

ceis

2.9 Le ROI de l'usage de l'arme informatique

- **<u>Avantages :</u>**
  - Faible coût
  - À la portée de tous
  - Effets redoutables

- **Son faible coût est à relativiser**
  - Possession du matériel, de l'infrastructure et des talents humains
  - Arme informatique capable de causer des dégâts suffisants pour remplacer l'arme traditionnelle
  - Non réutilisable : une phase de redéveloppement est toujours nécessaire
  - Pas de garanties des effets

- **Incertitude de l'intérêt des Etats pour cette arme**

Tendances identifiées et facteurs clés d'évolution

2.10 La riposte à la LIO n'est pas nécessairement de la LIO

- **Ripostes politiques, diplomatiques, économiques, techniques et juridiques**

- **<u>Objectifs</u>**
  - Logique de riposte ouverte
    - ✓ Légitimer les activités de riposte de type LIO
    - ✓ Légitimer la surveillance et la maîtrise accrue des réseaux
  - Logique d'action clandestine
    - ✓ Communiquer sur des valeurs chères à la société civile (neutralité du net, liberté d'expression)

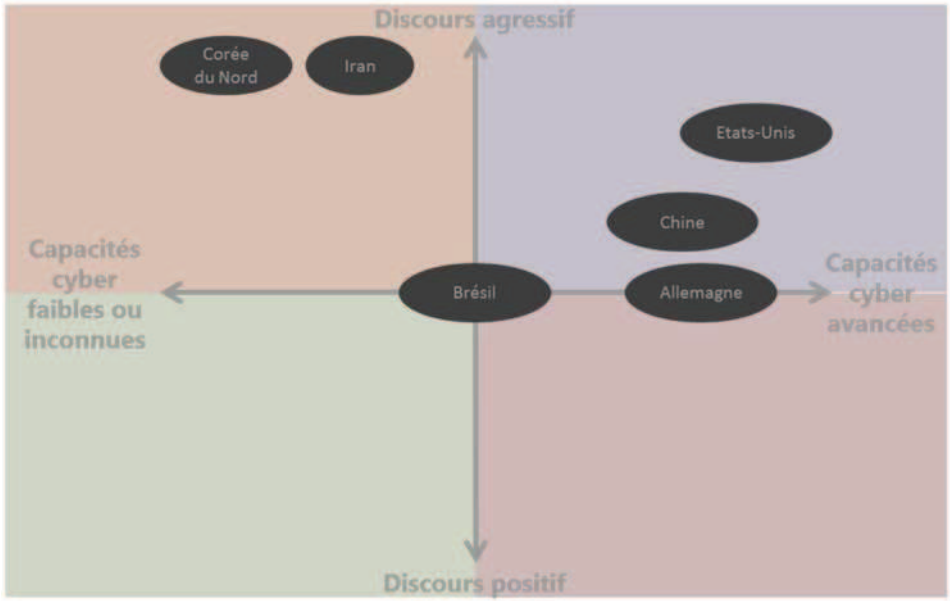
- **<u>Stratégie</u>** : communiquer sur les canaux traditionnels de réponse lors de rivalités étatiques afin de préparer une riposte sous-jacente bien plus nocive
  - Montée en puissance du Brésil en LIO

ceis

Conclusions : postures et perspectives

1.1 Capacités cyber effectives vs. Discours et stratégie de communication

- **Analyse sur deux critères**
  - Nature du discours : vocabulaire employé par les officiels, sa dimension négative ou positive, son agressivité, sa fermeté et son caractère conciliant
  - Capacités cyber effectives du pays : travaux menés dans le cadre de l'Observatoire du Monde Cybernétique



ceis

Conclusions : postures et perspectives

1.2 Risques et conséquences par pays

	RISQUE	COMMENTAIRES
ALLEMAGNE	Moyen	▪ Capacités réelles ▪ Déclarations anti-NSA
BRESIL	Moyen à court terme Fort à long terme	▪ Montée en puissance de ses capacités cyber ▪ Posture avantageuse vis-à-vis des autres BRICS
CHINE	Fort Très fort avec ses alliés	▪ Capacités importantes
COREE DU NORD	Très fort à long terme	▪ Capacités faibles ▪ Indépendance par rapport à la communauté internationale
ETATS-UNIS	Fort	▪ Capacités considérables ▪ Investissements dans la formation, la recherche et le développement
IRAN	Fort	▪ Montée en puissance de ses capacités cyber ▪ Attribution de nombreuses opérations ▪ Volonté de contre-attaquer suite à *Stuxnet*

ceis

CEIS

SOCIETE ANONYME AU CAPITAL DE 150 510 €

SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain - 75007 Paris

Tél. : 01 45 55 00 20 - Fax : 01 45 55 00 60

ceis