Cyberdéfense et Stratégie 2019

Et si Internet s'effondrait ?

Ministère de la défense
DGRIS

2 Juillet 2019

ceis

TABLE DES MATIERES

1 RAPPEL DES OBJECTIFS

Cet événement annuel réunit les chaires de recherche en cybersécurité et cyberdéfense quelles que soient les disciplines qu'elles couvrent (sciences et techniques, sciences humaines et sociales, sciences cognitives…), le Commandement de la Cyberdéfense et le secteur privé dans l'objectif de fédérer la communauté de la recherche et de renforcer les synergies entre les différents acteurs « cyber ».

Il a donc vocation à :

- Valoriser les travaux et réflexions des chaires, notamment ceux en lien avec la thématique annuelle choisie, et souligner l'intérêt de leurs travaux pour les acteurs industriels du secteur ;
- Permettre aux différents acteurs d'échanger sur des sujets transverses, de confronter leurs approches et coordonner leurs travaux ;
- Relayer les besoins des acteurs industriels en R&D pour favoriser l'innovation ;
- Favoriser un rapprochement entre les chaires et les acteurs publics et privés pouvant participer à l'effort du ministère des Armées dans son soutien aux activités de recherche ;
- Réaffirmer le rôle moteur du ministère des Armées en recherche stratégique sur le cyberespace.

Le séminaire se déroule en plusieurs phases selon un programme articulé autour :

- D'une matinée réservée aux chaires et chercheurs et ayant pour objectif de les faire échanger et travailler sur des thématiques liées au sujet de l'année ;
- D'un après-midi ouvert au secteur privé pour permettre aux sociétés participantes de présenter leurs approches et d'échanger avec les chaires sur leurs besoins en recherche, ainsi que sur les opportunités de financement de projets portés par les chaires.

2 THÈME DE L'ANNÉE : ET SI INTERNET S'EFFONDRAIT ?

Depuis 20 ans, Internet a montré sa résilience, même si quelques attaques ou erreurs de manipulation ont provoqué des ralentissements ou coupures ponctuelles et localisées. Les infrastructures d'Internet ont d'abord résisté à l'erreur humaine, à l'image du routage BGP, véritable "ciment" du réseau, régulièrement fragilisé par des erreurs de manipulation. Elles ont ensuite résisté à toutes sortes d'attaques malveillantes, comme celle ayant affecté l'ICANN et le système DNS en février 2019 ou bien encore les nombreux "dénis de service distribués" (DDoS) générés par le botnet Mirai, qui a notamment coupé le Libéria du reste du monde en 2016. Elles ont enfin résisté à l'explosion des utilisateurs, des usages, des données et du trafic (près de 40% d'augmentation chaque année).

Alors est-il vraiment utile de se faire peur ?

La réponse est oui ! C'est justement par qu'Internet est devenu une "commodité" et les données le nouvel "or noir", que l'on a une fâcheuse tendance à oublier les câbles, les points d'échange, les protocoles de routage et d'adressage, les datacenters, bref les infrastructures qui sous-tendent cette évolution, qu'il faut craindre une panne massive pour mieux s'y préparer. C'est aussi parce que certains États, Russie en

tête, s'entraineraient à couper leur « portion » d'internet du reste du réseau et que « l'arsenalisation » de l'espace numérique est de plus en plus assumée, que la question mérite d'être posée.

L'hyper-connectivité, qui deviendra la norme avec la 5G et l'immixtion de l'IoT dans tous les domaines de l'activité humaine renforcent encore cette exigence. D'autant que la concentration de nombreuses infrastructures et la faible diversité "génétique" de certains équipements renforcent le caractère systémique des risques, non seulement en matière de confidentialité mais également de disponibilité.

Quels sont aujourd'hui les principaux talons d'Achille des infrastructures Internet en termes de vulnérabilités et de menaces ? Quelles sont les réponses politiques, juridiques, techniques et technologiques à apporter pour faire face à ces défis ? Doit-on revoir les protocoles clés du réseau ? Faut-il imaginer, sur le plan juridique, une protection spécifique du "cœur public" d'Internet ? A l'heure du retour des États-puissance et d'une montée de l'unilatéralisme, quel système de sécurité collective peut-on imaginer ?

3 PROGRAMME DE LA JOURNÉE

Horaire	Titre	Intervenant
8h30-8h45	Ouverture	Contre-amiral (2S) Pascal VEREL, Chargé de mission recherche, Commandement de la Cyberdéfense
	MENACES ET VULNÉRABILITÉS	
08h50-09h15	Introduction : Quand l'improbable se produit...	Angeline VAGABULLES, Auteure de *Cyber-attaque : Plongez au cœur du blackout*
09h15-09h35	Vulnérabilités et fragilités du cœur du réseau : le cas du BGP	Kavé SALAMANTIAN, Université de Savoie
09h35-10h00	Vulnérabilités et fragilités du cœur du réseau : le cas du DNS	Maciej KORCZYINSKI, Cybersecurity Institute
10h00-10h15	Focus sur la stratégie Russe	Kevin LIMONIER, Institut Français de Géopolitique
10h15-10h30	Focus sur la stratégie Chinoise	Aranone ZARKAN, CEIS
	RÉSILIENCE	
11h20-11h40	Quelles solutions techniques pour le mode dégradé ?	Joaquin GARCIA-ALFARO, Chaire IMT sur la cybersécurité des infrastructures critiques
11h40-12h00	Quel cadre règlementaire pour assurer la résilience au plan national ?	Claire ANDERSON, ANSSI
12h00-12h20	Quel cadre règlementaire pour assurer la résilience au plan international ?	Aude GERY, GEODE
12h20-12h40	Quels nouveaux protocoles de sécurité ?	Stéphane BORTZMEYER, AFNIC
13h00-14h30	DÉJEUNER : SIMULATION STRATÉGIQUE	
14h30-14h40	Introduction	Général Olivier BONNET DE PAILLERETS, Commandant de la Cyberdéfense
14h40-15h15	Présentation d'un scénario d'attaque	Louis CHASSE et Robert PECHE, COSMOCORP
15h15-15h35	Sécuriser les communications : vulnérabilités et l'opportunité des raisonnements avancés	Julien SIGNOLES, CEA List
15h35-15h45	*Pitches* de projets de thèse ou de recherche	Thibaud ANTIGNAC, CEA List Thomas CLÉDEL, IMT-Atlantique
16h00-16h20	Témoignage d'une communication de crise réussie	*Gérôme BILLOIS, Wavestone*
16h20-16h40	Les bonnes pratiques en matière de communication de crise	Stéphanie LEDOUX, Alcyconie
16h45-17h30	Table ronde : "Doit-on s'entraîner à la déconnexion ?"	François-Bernard HUYGUE, IRIS Stéphane BORTZMEYER, AFNIC Xavier HARTOUT, Adenium

4 ANALYSES THÉMATIQUES

La journée a été ponctuée de nombreuses démonstrations qui n'ont pas pu faire l'objet d'articles dédiés. Les supports de présentations disponibles ont été intégrés en tant qu'annexes à ce compte-rendu. Les interventions sous forme d'exposés ont été restituées ci-dessous.

4.1 LA SECURITE DU CŒUR D'INTERNET : LE CAS DU PROTOCOLE BGP

La résilience d'Internet repose sur la connectivité, c'est-à-dire sur la capacité des réseaux qui le composent à établir et maintenir entre eux des connexions et à communiquer et échanger des paquets de données. C'est parce que ces réseaux sont denses et parfois redondants, c'est à dire qu'ils prennent nativement en compte plusieurs routes possibles pour acheminer des données entre deux points, que la structure d'Internet est résiliente.

Des défauts de résilience peuvent cependant subvenir, mais ils sont le plus souvent dus à des stratégies d'acteurs tentants de supprimer ou d'ajouter des routes, qu'à la structure même d'Internet. Pour le comprendre, il faut notamment s'intéresser au protocole BGP, un élément central de la connectivité.

A. Enjeux géopolitiques de la donnée

On a parfois l'impression qu'Internet se résume aux applications utilisées quotidiennement (Facebook, Google Maps, Waze, Skype, etc.). Particulièrement opaques, celles-ci masquent en fait les infrastructures qui les sous-tendent : les serveurs sur lesquels elles sont basées, les câbles par lesquels passent les données, etc. Elles font oublier que les données qu'elles collectent et échangent transitent par différents réseaux.

En réalité, le cyberespace, c'est-à-dire l'ensemble des interactions qui ont lieu au-dessus de l'infrastructure physique d'Internet, est ancré dans la géographie. Il est soumis à des contraintes physiques, politiques et économiques. On constate par exemple que les câbles maritimes assurant le transit des données passent par des points névralgiques de l'espace géographique : Djibouti, Singapour, Fujaïrah, etc. On observe également que certains pays n'ont, pour des raisons politiques ou économiques, pas développé d'infrastructures leur permettant d'échanger directement des données avec leurs voisins, comme c'est le cas de l'Iran et de l'Irak. De même, une donnée envoyée de la France vers le Japon pourrait, par exemple, être surveillée par des acteurs russes à Fujaïrah[1] où de nombreux câbles, dont des câbles russes par exemple, s'interconnectent au sein de hubs dédiés.

Ainsi, la situation géopolitique des États constitue autant de contraintes économiques ou politiques pour les opérateurs de réseaux et les amènent à faire transiter les données par un chemin plutôt que par un autre.

[1] South East Asia–Middle East–Western Europe 4 (SEA-ME-WE 4), en.wikipedia.org

B. Internet, un réseau de réseaux

Internet est un réseau de réseaux. Il est constitué de « systèmes autonomes » : un système autonome – en anglais, *Autonomous System* (AS) – est une autorité administrative (entreprise, FAI, université, organisme gouvernemental) qui gère son réseau indépendamment des autres. Ces systèmes autonomes sont interconnectés les uns aux autres et constituent ainsi ce que l'on appelle Internet.

Un système autonome ne partage pas sa topologie ou ses informations avec les systèmes autonomes voisins. Il ne partage avec eux que le minimum d'informations nécessaires pour permettre le routage des données. Le protocole qui permet aux différents systèmes autonomes d'interagir est le protocole BGP (*Border Gateway Protocol*). Le fonctionnement de BGP est basé sur des « annonces » aux réseaux voisins. Pour simplifier, BGP permet à un AS :

- D'annoncer une nouvelle route : un opérateur annonce qu'il est possible d'accéder, à travers son réseau, à une adresse donnée ;
- De supprimer une route : un opérateur annonce que son réseau ne prend plus en charge le chemin vers une adresse donnée.

L'annonce de nouvelles routes repose sur des critères souvent politiques ou économiques : un opérateur n'accorde l'autorisation de passer par son réseau que s'il pense pouvoir en tirer un bénéfice.

Aujourd'hui, un paquet de données qui transite entre deux points (entre deux pays par exemple) traverse en moyenne onze acteurs indépendants de l'Internet, c'est-à-dire onze acteurs qui peuvent décider à chaque instant d'intervenir sur leur réseau, affectant par la même l'acheminement des paquets de données.

Pour être résilient, un opérateur de réseau se connecte à plusieurs autres AS afin de multiplier et diversifier ses choix de chemins pour acheminer un paquet de données d'un point à un autre. L'opérateur décide à chaque instant, en fonction d'impératifs politiques et économiques, du chemin qu'il juge optimal pour relier deux points. Si l'un des chemins est supprimé par cet opérateur ou par un autre, les autres chemins peuvent-être utilisés en remplacement. Dans ces conditions, le simple fait de parvenir à communiquer (donc à échanger des paquets de données) avec un lieu situé à des milliers de kilomètres démontre la flexibilité et de la structure d'Internet et sa capacité à contourner les obstacles.

C. Le cœur d'Internet, levier d'influence

Les interactions entre AS peuvent être représentées sous forme de graphes de connexion qui schématisent la topologie d'Internet. On associe souvent Internet à une « méduse » :

- Tout d'abord, Internet a un cœur, formé par un ensemble d'opérateurs qui sont fortement interconnectés et qui ont confiance les uns dans les autres. La densité des interconnexions entre ces opérateurs permet de traverser le cœur d'Internet en passant par un ou deux opérateurs au maximum ;
- Autour du cœur, la première coquille est constituée d'opérateurs connectés à au moins 1 ou 2 des AS qui constituent le cœur ;
- La seconde coquille est quant à elle constituée des AS qui sont connectés à la première coquille et peuvent exceptionnellement avoir établi un lien avec l'un des AS du cœur.

Le chemin le plus court pour relier deux points passe par ces différentes « coquilles », jusqu'au cœur, qui joue le rôle d'aiguilleur. Grâce à sa très forte densité de connexions, il offre une grande diversité de routes possibles entre deux points. Or, le cœur d'Internet est aujourd'hui principalement composé d'acteurs américains, ce qui constitue un levier de puissance considérable pour les autorités de ce pays. Le cas de Huawei illustre bien le moyen de pression que représente, pour les autorités américaines, ce contrôle sur le cœur d'Internet. Cette entreprise chinoise s'est vue privée de son accès à certains acteurs majeurs comme Microsoft en raison de différends entre la Chine et l'administration américaine, affaiblissant par la même sa position commerciale.

D. Les nouveaux scénarios d'attaques

Aujourd'hui, environ 200 000 changements de chemins et de routage sur le réseau sont annoncés chaque minute. Si certains de ces changements sont légitimes, c'est-à-dire qu'ils sont opérés par les opérateurs propriétaires des plages d'adresses IP (*Internet Protocol*) en question, d'autres au contraire, constituent des « détournements BGP » quand ils sont opérés par un opérateur intervenant sur une plage d'adresses IP qui ne lui est pas attribuée. Dans ce cadre, on peut définir un hijack BGP comme un détournement du trafic d'un opérateur par un autre opérateur. Le but est de faire transiter le trafic par le réseau de l'attaquant plutôt que par celui de l'opérateur légitime.

On peut citer trois exemples de *hijack* BGP récents :

- **Le cas de Pakistan Telecom[2]**

  Les autorités pakistanaises ont tenté de priver les individus connectés depuis le territoire national de l'accès à YouTube. Elles ont donc cherché à dérouter le trafic pakistanais de YouTube vers Pakistan Telecom. À la suite d'une erreur de configuration des autorités pakistanaises, l'annonce s'est répandue dans le monde entier et le trafic mondial à destination de YouTube a été re-routé vers Pakistan Telecom qui s'est effondré sous la surcharge de trafic.

- **Le cas de China Telecom et Verizon[3]**

  En 2015, China Telecom a annoncé – officiellement comme une erreur de configuration – des routes vers Verizon plus courtes que toutes les autres routes. La totalité du trafic des téléphones américains Verizon (et donc des données qu'il transportait) a donc transité par la Chine avant de revenir aux États-Unis.

- **Le Canadian Bitcoin *hijack*[4]**

  En 2014, des attaquants ont détourné le trafic entre les mineurs et les *mining pools* de la blockchain du Bitcoin, interceptant ainsi 50 000 bitcoins.

---

[2] RIPE, *YouTube Hijacking: A RIPE NCC RIS case study*. www.ripe.net
[3] ORACLE Dyn, *China Telecom's Internet Traffic Misdirection*. dyn.com
[4] BGPmon, *The Canadian Bitcoin hijack*. www.bgpmon.net

De nouveaux scénarios d'attaques se dessinent, en particulier des combinaisons de *hijacks* ou de déni de service sur des sessions BGP. L'objectif est de déconnecter un pays ou un opérateur d'un pays, sans qu'une présence physique de l'attaquant sur le territoire ne soit nécessaire. Pour cela, il suffit de lancer simultanément un grand nombre de *hijacks* BGP et une attaque par déni de service. Le trafic est alors détourné sans que l'acteur légitime puisse réagir, puisqu'il subit une attaque par déni de service sur ses sessions BGP.

Une dizaine d'événements de ce type ont été observés ces trois dernières années. Tous ont duré moins de cinq minutes, laissant à penser qu'il ne s'agit que d'un *proof of concept* destiné à démontrer la faisabilité de ce type d'attaques.

4.2 QUELS CADRES REGLEMENTAIRES NATIONAL ET INTERNATIONAL POUR ASSURER LA RESILIENCE D'INTERNET?

Si la résilience des systèmes d'information doit être assurée sur le plan technique, elle doit être également envisagée d'un point de vue règlementaire, tant au plan national qu'international.

A. Le cadre règlementaire national

Il n'existe pas en France de cadre règlementaire prévoyant les mesures à adopter dans le cas d'un effondrement total d'internet. Cependant, deux dispositifs existants pourraient s'y appliquer :

- Le dispositif général de gestion de crise de l'État, qui peut être déclenché, en fonction de l'ampleur de la crise, pour certains incidents majeurs (ex. : attaque étatique contre l'infrastructure de l'internet – DNS, BGP – etc.) ;
- Des obligations réglementaires pesant sur certains opérateurs essentiels qui doivent permettre d'assurer la sécurité et la continuité de leurs systèmes (Loi de programmation militaire – LPM, Directive européenne sur la sécurité des réseaux et des systèmes d'information – NIS, etc.).

➢ Le dispositif de gestion de crise de l'État

La Cellule interministérielle de crise

Suite aux préconisations du Livre Blanc de 2008 sur la sécurité et la défense nationale relatives à une organisation intégrée de la gestion de crise au niveau de l'État, la circulaire n° 5567/SG du 2 janvier 2012 sur l'organisation gouvernementale pour la gestion des crises majeures[5] a mis en place une Cellule interministérielle de crise (CIC). Cette circulaire, qui définit les règles d'organisation et de fonctionnement de la CIC, précise notamment que cette cellule intervient, de manière générale, sous l'autorité du Premier Ministre en cas de crise majeure, afin notamment de disposer d'une capacité d'analyse permettant de faire face rapidement à la crise. Pour ce faire, la CIC est structurée en 3 entités :

[5] http://circulaires.legifrance.gouv.fr/pdf/2012/01/cir_34453.pdf

- La cellule de décision, qui met en relation le Premier ministre et le Président de la République ;
- La cellule de situation, qui réalise les analyses sur l'état de la crise ;
- La cellule de communication, qui a pour objet d'informer le public sur les avancées des autorités dans la gestion de la crise.

Ce dispositif a une vocation générale et n'est pas spécifiquement dédié aux incidents issus d'une cyberattaque. Néanmoins, la circulaire de 2012 est en cours de révision afin d'intégrer leurs spécificités.

Le plan PIRANET

La famille des plans PIRATE constitue un autre élément central du dispositif de gestion de crise de l'État en matière de cybersécurité, notamment via le plan PIRANET. Complémentaire du plan Vigipirate déclenché par le Premier ministre, le plan PIRANET encadre les interventions en cas d'attaques informatiques majeures contre les systèmes d'information, pouvant porter atteinte aux intérêts vitaux de la Nation. Le plan PIRANET :

- Est préparé et maintenu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), sous l'autorité du Secrétariat général de la défense et de la sécurité nationale (SGDSN) ;
- Définit l'organisation et les processus de gestion de crise permettant à l'État de prendre les dispositions nécessaires ;
- Prévoit l'application de mesures adaptées à une menace ou une attaque informatique d'ampleur.

Comme l'ensemble des plans PIRATE, le plan PIRANET fait l'objet d'exercices réguliers permettant aux équipes et personnels concernés de s'entraîner.

Au-delà du dispositif de gestion de crise de l'État et du plan PIRANET, le cadre règlementaire français comprend aussi des obligations à la charge de certains opérateurs vitaux, qui doivent permettre de d'éviter une crise majeure des systèmes d'information.

➢ <u>Les obligations à la charge des opérateurs : l'exemple du secteur des télécommunications</u>

Les textes relatifs aux obligations dans le secteur des télécommunications

La réponse à une crise cyber majeure repose, en grande partie, sur la préparation des opérateurs concernés et donc sur certaines obligations que ces derniers doivent respecter. Ainsi, dans le secteur des télécommunications, 3 textes s'appliquent et encadrent la résilience des opérateurs et de l'internet :

- Le code des postes et des communications électroniques (CPCE), dont l'article D98-5-III prévoit que les opérateurs sont tenus de prendre toutes les mesures appropriées pour assurer l'intégrité de leurs réseaux et garantir la continuité des services fournis ;
- La Loi de programmation militaire (LPM) du 28 novembre 2016, qui fixe pour les opérateurs d'importance vitale (OIV) des règles de sécurité et les modalités de déclaration de leurs systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur « Communications électroniques et internet » ;

- Les textes de transposition de la directive NIS (*Network and information security*), soit le décret n° 2018-384 du 23 mai 2018 et l'arrêté du 14 septembre 2018 qui concernent la sécurité des réseaux et des systèmes d'information des Opérateurs de services essentiels (OSE) notamment. Ces derniers textes présentent l'intérêt de s'appliquer à un cercle plus large d'opérateurs.

S'agissant plus particulièrement des systèmes d'information d'importance vitale (SIIV), les obligations sont à la fois organisationnelles et techniques[6] et concernent notamment :

- La politique de sécurité des systèmes d'information (PSSI) ;
- L'homologation des systèmes ;
- La cartographie des systèmes ;
- Le maintien en condition de sécurité (MCS) des systèmes ;
- La journalisation des connexions ;
- La détection des incidents ;
- Le traitement des incidents de sécurité ;
- Le traitement des alertes ;
- La gestion des identités et des accès ;
- L'administration des systèmes ;
- La défense en profondeur des systèmes ;
- etc.

Si les obligations sont donc actuellement à la charge de certains opérateurs seulement, l'application de la directive NIS, qui touche un plus large cercle d'opérateurs puisqu'elle concerne la catégorie plus vaste des « opérateurs de services essentiels », pourrait amener à élargir ces obligations à l'ensemble des entreprises. Cette initiative pourrait s'avérer difficile à réaliser en pratique, car elle s'accompagne de nouvelles exigences liées au contrôle du respect de ces obligations et de l'application éventuelle de sanctions le cas échéant. Une ouverture contrôlée des obligations à l'ensemble des développeurs de logiciels pourrait néanmoins être envisagée pour assurer une meilleure sécurité des outils utilisés au quotidien par les particuliers, les administrations et les entreprises.

L'ANSSI prévoit cependant déjà des recommandations et des mesures de sensibilisation à destination des opérateurs qui ne sont pas qualifiés « d'importance vitale » ou de « service essentiel ».

Les acteurs de la préparation et de la gestion de crise dans le secteur des télécommunications

3 acteurs principaux peuvent être mentionnés dans la préparation et la gestion de crise dans le secteur des télécommunications :

- L'Autorité de régulation des communications électroniques et des postes (ARCEP) qui fixe les règles sur la disponibilité des réseaux ;
- L'ANSSI qui fixe des exigences de sécurité, contrôle leur bonne application et qui intervient en cas de crise ;

[6] https://www.ssi.gouv.fr/administration/protection-des-oiv/les-regles-de-securite/

- Le Commissariat aux communications électroniques de défense (CCED) qui facilite le contact entre l'État et les opérateurs de communications électroniques déclarés auprès de l'ARCEP.

Notons que si l'ANSSI et le CCED agissent aux côtés des opérateurs lors de la crise, l'ARCEP n'intervient, elle, qu'en amont.

L'essentiel du cadre règlementaire conçu pour assurer la résilience de l'Internet au plan national se concentre donc sur l'avant-crise et sa préparation. Si cette règlementation demeure relativement généraliste, elle a pour objectif de pouvoir faire face à tout type de crise et doit donc pouvoir s'adapter.

Les autorités telles que l'ANSSI ou le CCED qui interviennent en cas de crise auprès des opérateurs ne remplacent pas ces derniers. Les opérateurs sont donc eux aussi acteurs à part entière du dispositif.

B. Le cadre règlementaire international

La stabilité du cyberespace et la résilience des systèmes d'information constitue aujourd'hui un véritable enjeu de droit international, puisqu'il est désormais admis par les États que ce dernier s'applique au cyberespace. La question du cadre règlementaire permettant d'assurer la résilience de cet espace amène donc à s'interroger sur les mesures prévues ou à l'étude pour assurer la sécurité des systèmes d'information, dans l'objectif plus large de sécuriser l'espace numérique mondial.

La question d'un cadre règlementaire international pour assurer la résilience d'Internet soulève néanmoins de multiples difficultés. Parmi les défis qui doivent être relevés en matière de régulation internationale du cyberespace :

- La diversité des initiatives, provenant à la fois d'organisations internationales ou régionales, d'États, ou encore d'acteurs privés, donc d'acteurs aux intérêts et objectifs différents voire divergents ;
- La pluralité des sujets ou thématiques concernées, qui comprennent à la fois les technologies, le rôle des organisations internationales, ou encore les comportements des États et des acteurs privés ;
- Le débat sur le caractère contraignant des normes de droit international dont la mise en œuvre dépend grandement de la bonne volonté des États ;
- La mainmise des États sur les enjeux liés à la gouvernance de l'Internet et les difficultés à imaginer une gouvernance partagée, notamment avec les acteurs privés (multi-stakeholder) .

L'ensemble de ces considérations montre qu'il reste difficile de définir un cadre règlementaire international pour assurer la résilience du cyberespace. Ces difficultés s'expliquent principalement par :

- Les interprétations différentes des États sur l'application du droit international ;
- L'existence de situations non régulées par le droit international et qui nécessitent la création de nouvelles normes (l'arrangement de Wassenaar a été révisé pour intégrer la problématique des logiciels d'intrusion informatique par exemple) ;
- L'absence d'une véritable coopération internationale en matière de collecte et d'échange de preuves numériques.

Pourtant, malgré ces difficultés, certains dispositifs spéficiquement conçus pour assurer la résilience des systèmes d'information et la stabilité du cyberespace permettent aux États de continuent à œuvrer pour réguler cet espace.

- Les dispositifs actuels

Plusieurs dispositifs consacrés par le droit international contribuent à assurer la stabilité du cyberespace. Ils visent notamment à faciliter la coopération entre les États en matière de protection des infrastructures numériques, afin de faire se développer entre ces États un intérêt mutuel à œuvrer pour la résilience d'Internet. Il s'agit à la fois de mesures dites « de confiance », de normes de comportements dans le cyberespace, ou des dispositifs relatifs aux capacités de protection des systèmes d'information.

Par exemple, la résolution du Conseil de sécurité l'ONU sur la protection des infrastructures essentielles contre les attaques terroristes prend notamment en considération les risques pesant sur les infrastructures de l'internet, et incite les États à élaborer des « stratégies de réduction des risques ».

On peut également citer l'Arrangement de Wassenaar, récemment révisé, qui tend à favoriser les transferts de technologies liées à la cybersécurité et à la cyberdéfense pour permettre aux États de renforcer la sécurité de leurs systèmes d'information essentiels.

D'autres dispositifs de droit coutumier, comme l'obligation de vigilance et de *due diligence*, obligent quant à eux les États à veiller et à prévenir toute violation du droit international par des acteurs privés se trouvant ou utilisant leurs territoires, y compris les cyberattaques par des acteurs privés qui visent les infrastructures vitales d'un État.

- Les perspectives

La complexification du cyberespace et les impératifs de résilience qui y sont associés posent de nouvelles problématiques en termes de régulation internationale. Alors que cet espace s'est initialement construit hors du contrôle des États, l'intervention de ces derniers à travers une gouvernance plus étroite du cyberespace est peu à peu devenue, ces dernières années, nécessaire pour assurer la sécurité de l'Internet et donc sa résilience. La régulation internationale tend ainsi à devenir plus politique mais aussi plus technique, car elle s'accompagne de défis technologiques comme celui de la généralisation internationale du chiffrement, notamment dans le cadre du respect des droits de l'homme sur Internet et notamment ceux relatifs au respect de la vie privée ou à la liberté d'expression. L'intégration des logiciels d'intrusion dans le régime international des exportations des biens à double usage constitue un autre exemple de la prise en compte par le droit international des spécificités techniques liées au cyberespace.

Ces considérations politiques et techniques rendent particulièrement difficiles les négociations sur l'application du droit international au cyberespace. Néanmoins, les États souhaitent, dans le cadre notamment des nouvelles négociations à l'ONU, faire évoluer la réflexion, par exemple en intégrant davantage certains organismes techniques internationaux tels que l'UIT ou l'ICANN à la réflexion sur l'élaboration des règles internationales applicables au cyberespace.

4.3 GEOPOLITIQUE DES RESEAUX : L'EXEMPLE DE LA RUSSE

Comme beaucoup d'autres acteurs, la Russie déploie dans le cyberespace des stratégies d'influence à l'égard de certains acteurs régionaux, le plus souvent menées par des acteurs non officiels, plus ou moins indépendants du gouvernement russe mais bénéficiant de son soutien.

« Cartographier » le cyberespace permet d'observer et de comprendre ces stratégies.

Pour ce faire, les données techniques (ou métadonnées) issues de certains outils initialement conçus pour d'autres usages (type *Nmap* par exemple), ainsi que les dynamiques des flux de données au niveau régional et international, peuvent être interprétées et analysées pour faire office de « capteurs géopolitiques ». Les métadonnées permettent ainsi de déduire les caractéristiques de la stratégie de contrôle et d'influence menée par la Russie envers d'autres États et de comprendre les rapports de force et les luttes de pouvoir qui s'y jouent.

Trois types de capteurs géopolitiques peuvent être utilisés : les protocoles BGP[7], les données RIPE[8] et les outils de cartographie de réseaux.

A. L'étude des protocoles BGP pour appréhender des rapports de force

Internet est composé de réseaux indépendants appelés « Systèmes autonomes » (*Autonomous Systems* – AS), tous administrés par une autorité (ou opérateur) qui en définit la politique de routage (les règles de circulation des informations entre les ordinateurs connectés à cet AS). BGP est un protocole de routage dit « inter AS » : il est utilisé pour faire circuler l'information entre les réseaux. Il permet donc de connecter des ordinateurs d'AS différents et par là-même d'opérateurs différents.

On remarque, à l'étude des représentations graphiques des routes BGP de l'Internet mondial[9], que les liens entre les AS reflètent les relations géopolitiques internationales. Comme dans l'espace physique, certains territoires, frontières et grandes dynamiques se dessinent en effet. On y distingue par exemple le « cœur de l'Internet », caractérisé par son réseau dense d'AS et de routes BGP, situé en Europe de l'Ouest et aux États-Unis et, en s'éloignant en cercles concentriques, des régions plus périphériques qui n'ont que peu de connexions avec le cœur d'Internet, comme la Crimée.

L'étude des liens que tissent les routes BGP et les transferts de données entre l'Ukraine et la Russie illustre de façon particulièrement parlante les symétries entre la disposition des infrastructures techniques, les flux de circulation des données et la situation politique ou géopolitique sur le terrain.

Deux zones de tensions géopolitiques entre la Russie et l'Ukraine transparaissent ainsi des analyses des interactions entre les AS de Crimée et du Donbass. Les autorités russes, lors de l'annexion de la Crimée,

---

[7] BGP : *Border Gateway Protocol* : protocole de passerelle chargé de la circulation des données.
[8] *Regional Internet Register*, organisme qui alloue les blocs d'adresses IP (adressage IPv4, IPv6) et des numéros d'Autonomous System dans sa zone géographique.
[9] Voir Annexe

ont pris possession des *Internet exchange points*[10], les câbles qui reliaient l'Ukraine continentale à la Crimée, afin d'exercer leur souveraineté. Ces câbles ont été coupés et la connectivité a été re-routée de la Crimée via la Russie et plus non via l'Ukraine.

Il en est de même pour la région du Donbass : les câbles qui reliaient cette région à l'Ukraine sont restés sous contrôle ukrainien jusqu'à l'été 2018, date à laquelle ils ont été détruits et re-routés via la Russie. Les AS qui relient ces deux pays semblent aujourd'hui contrôlés par des acteurs entretenant des liens avec les séparatistes et l'Armée russe, une façon pour la Russie de faire rentrer le cyberespace du Donbass séparatiste sous son contrôle via une prise de contrôle de la couche BGP.

Cette stratégie semble également faire écho aux grands principes énoncés dans la loi pour la sécurisation et le contrôle du « Ru.net »[11] (terme qui désigne ce que la Russie considère comme son espace Internet propre). Celle-ci prévoit en effet des mesures permettant de déconnecter le Ru.net du reste de l'Internet mondial en cas d'agression extérieure, notamment venant des États-Unis, dans l'objectif de maintenir la stabilité de l'Internet russe. La faisabilité d'une telle déconnexion est cependant encore à prouver.

B. L'analyse des données de latence du réseau RIPE pour observer les zones d'influence

Parmi les composantes du réseau RIPE, le réseau de sondes Atlas mesure la latence d'Internet et effectue des calculs de *traceroute*, c'est-à-dire d'analyse des trajets des paquets de données via des serveurs. L'étude de ces éléments permet d'identifier les grandes zones d'influence géopolitiques sur lesquelles les États tentent d'exercer leur puissance et leur pression sur d'autres acteurs via le contrôle des infrastructures et des réseaux de circulation des données.

Par exemple, la carte des latences indique le temps moyen que met un paquet de données pour se rendre d'un point à un autre. Plus les données sont acheminées rapidement, plus en on peut en déduire que le nombre d'intermédiaires entre les deux points est limité et donc qu'il existe entre eux des accords de transferts de données. L'étude des latences permettrait donc d'établir une sorte d'échelle kilométrique du cyberespace, qui n'est pas indicative de la réalité géographique mais des réalités géopolitiques.

L'exemple de la Géorgie est à ce titre particulièrement illustratif. On constate en effet que les paquets de données sont plus rapidement transférés de Tbilissi, la capitale, à Sofia, en Bulgarie, que de Tbilissi à Soukhoumi, entité autonome de la Géorgie qui lui est territorialement rattachée mais qui est sous contrôle politique russe. A ce titre, Tbilissi est donc plus proche de Sofia qu'elle ne l'est de Soukhoumi car en l'absence d'accord de transfert entre la Géorgie et la région de Soukhoumi – sous contrôle russe pour des raisons politiques – il n'existe pas d'infrastructure permettant le transfert de données direct entre Soukhoumi et Tbilissi. Les données acheminées de Tbilissi à Soukhoumi transitent en effet d'abord par Sofia, passent par l'Europe Occidentale, par la mer Baltique, puis par la Russie pour arriver enfin à Soukhoumi.

[10] Infrastructure physique permettant aux fournisseurs d'accès d'échanger du trafic Internet entre leurs réseaux de systèmes autonomes sur la base d'accords mutuels

[11] Voir https://omc.ceis.eu/russie-une-nouvelle-loi-pour-la-securisation-et-le-controle-du-runet/

C. L'utilisation d'outils de cartographies de réseaux pour identifier les points stratégiques de passage de données

Certains capteurs techniques peuvent être détournés de leur usage initial à des fins de recherches sur les stratégies d'influence des États. C'est le cas de l'outil *Nmap*[12], un scanner de ports libres originellement conçu pour détecter les ports ouverts et obtenir des informations sur les services hébergés, notamment sur les systèmes d'exploitation. Cet outil peut être utilisé par les chercheurs pour cartographier les réseaux et identifier et comprendre les points stratégiques de passage de données.

D. Conclusion

Comme le montre l'exemple russe, les stratégies géopolitiques déployées dans le monde physique trouvent donc leur prolongation dans le cyberespace. Le contrôle et la surveillance des réseaux et des points de connectivité deviennent alors une priorité pour des acteurs étatiques de plus en plus amenés à les utiliser comme moyens d'actions politiques et comme fondement tactique à des actions coercitives d'influence.

De même, les routes empruntées quotidiennement par des milliards de paquets de données peuvent être observées et analysées dans une perspective géopolitique pour affiner la compréhension des enjeux stratégiques du cyberespace et des positionnements respectifs des différents acteurs.

4.4 ORGANISATION DE L'INTERNET CHINOIS : DE LA CENSURE A LA STRATEGIE DE CONTROLE

L'État chinois est en tension permanente entre la nécessaire informatisation de la société et la volonté de contrôle de l'Internet. C'est pourquoi la Chine a développé une vision souveraine du cyberespace selon laquelle il incombe aux États de contrôler l'ensemble des éléments qui sous-tendent l'Internet (infrastructures, connexions, contenus, etc.). L'objectif, idéalement, est de filtrer l'Internet comme peut l'être une frontière physique. Le *Great Firewall*[13] participe d'ailleurs de ce filtrage. Avec 772 millions d'utilisateurs Internet et 753 millions d'utilisateurs de l'Internet mobile en décembre 2017, l'État chinois a développé des structures et une organisation propre pour la vérification des flux et des contenus dans le cyberespace, toujours en lien avec des organes étatiques ou partisans.

A. Un système décisionnel centralisé

La définition des politiques publiques relatives à Internet émane du Conseil des Affaires d'État et du Comité pour la cybersécurité et l'informatisation du Comité central du Parti communiste chinois (中国共

[12] https://nmap.org/

[13] Combinaison de mesures législatives et technologiques mises en œuvres par la République Populaire de Chine pour réguler l'Internet sur le plan national.

产党中央网络安全和信息化委员会)[14]. Ces politiques sont relayées par des structures étatiques, par des ministères tels que le ministère de la Sécurité publique (MSP) chargé de la protection nationale et spécialisé dans la surveillance des contenus et activités pouvant porter atteinte à l'ordre social,[15] et le ministère de l'Industrie et des Technologies de l'Information (MIIT), mais également par des organes partisans tels que l'Administration de l'Internet chinois (CAC), qui dépend du Comité pour la cybersécurité et l'informatisation.

En matière de cybersécurité, l'État chinois a mis l'accent sur les infrastructures critiques. La loi sur la cybersécurité de 2017 oblige les sociétés à prévoir les incidents sur leurs réseaux et impose que les matériels utilisés par les infrastructures critiques soient vérifiés par la MSP. Depuis juin 2017, un catalogue d'équipements établi par la CAC évalue leur conformité aux normes fixées par les institutions de certifications chinoises.

D'autre part, des institutions étatiques et partisanes sont désignées pour assurer le contrôle des contenus dans le cyberespace et le contrôle des matériels informatiques (routeurs), notamment de cybersécurité (pare-feux, etc.). Pour étendre son contrôle, l'État chinois s'appuie sur les sociétés éditrices de logiciels et productrices de matériels.

B. Le rôle des sociétés privées dans le contrôle de l'internet chinois

Les fournisseurs d'accès à Internet chinois (FAI) notamment *China Telecom* et *China Unicom* font office de relais de l'application des lois relatives aux contenus. Les autorités leur communiquent par exemple les adresses IP et les noms de domaine à bloquer, souvent via un blocage DNS. Les sociétés privées utilisent par ailleurs les filtres de mots-clefs fournis par l'État pour vérifier les contenus sortant et entrant dans le cyberespace chinois. Les applications de discussion (*WeChat*) ou les plateformes de blogs en ligne (*Weibo*) exercent ainsi elles-mêmes une partie de la censure.

Si les sociétés privées sont considérées comme des relais, c'est notamment en raison des liens étroits que l'État et le Parti entretiennent avec un grand nombre d'entre elles. Certaines sont des entreprises publiques dont le dirigeant est également secrétaire du « comité de Parti » de l'entreprise. C'est le cas de la société de *cloud computing* et de gestion du *Big Data* INSPUR, dirigée par SUN Pishu. Dans d'autres cas, le dirigeant de la société prend part à l'élaboration des politiques publiques, XIAO Xinguang, le PDG de la société de cybersécurité et de cyberdéfense ANTIY, est également membre du comité national de la Conférence consultative politique du peuple chinois.

L'organisation du contrôle de l'Internet en Chine semble donc continue, entre les institutions et les acteurs privés et jusque dans la société.

[14] Ancien groupe dirigeant du comité central du Parti communiste.
[15] Il s'agit essentiellement des *Fake news*, des rumeurs, de la fraude, de l'extorsion, du sabotage et du vol de données.

C. Le contrôle de l'internet par ses utilisateurs

La Chine a fait de chaque individu un censeur en puissance. Le contrôle de l'Internet par ses utilisateurs passe par la mise en place de structures de délation au sein des ministères de la Sécurité publique et de l'Industrie et des Technologies de l'Information mais aussi sous la tutelle du Comité pour la cybersécurité et l'informatisation. Les utilisateurs sont en mesure d'identifier un contenu malicieux ou immoral en se fondant sur les critères prévus par la loi qui définissent les contenus violents, pornographiques, portant atteinte à l'image de la Chine ou de son président entre autres.

La loi d'août 2017 sur la gestion des forums et la loi de septembre 2017 sur la gestion des informations des comptes publics d'utilisateurs rendent les individus responsables de toutes les posts publiés sur leur plateforme. Ces lois imposent également aux utilisateurs de fournir une pièce d'identité pour la création de comptes en ligne mettant, de fait, fin à toute possibilité d'anonymat dans le cyberespace. Ces lois renforcent l'auto-censure des individus dans le cyberespace.

D. Conclusion

Le contrôle de l'Internet chinois s'effectue donc à tous les niveaux de la société. Le degré avancé de contrôle de l'Internet chinois est évidemment commandé par la nature du régime politique. Néanmoins, que les sociétés privées chinoises participent du verrouillage de l'Internet chinois pousse à s'interroger sur la projection éventuelle de ce contrôle de l'Internet. En d'autres termes, la censure sur le territoire national serait-elle, à l'international, en passe de muter pour devenir une stratégie de contrôle et de récolte de données ?

4.5 GESTION ET COMMUNICATION DE CRISE

Les récentes crises générées par des cyber-attaques d'ampleur contre des entreprises ont rappelé que les conséquences pour les activités et l'image des organisations victimes peuvent être considérables et durables. Ainsi, les couts des dommages causés par l'attaque NotPetya en 2017 ont été estimés à près de 10 milliards de dollars à l'échelle internationale. L'entreprise Merck aurait subi 600 à 870 millions de dollars de dommage à elle seule, et a été contrainte dans les mois qui ont suivi l'attaque à un arrêt opérationnel de longue durée lié à des ruptures d'approvisionnement, obligeant même la société à puiser dans certains stocks stratégiques aux États-Unis.

Dans ce contexte, et alors que le risque de cyberattaques contre les entreprises est en augmentation constante[16], se doter de capacités de gestion et de communication de crise et des fonctions associées s'avère de plus en plus essentiel.

On peut distinguer 5 étapes dans la gestion et la communication de crise.

[16] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

A. Anticipation

Certaines mesures et processus simples permettent de renforcer au quotidien la résilience du SI d'une organisation, et ainsi de se prémunir contre les crises ou d'en contenir la propagation quand elles surviennent.

- Il s'agit d'abord d'appliquer les mesures basiques d'hygiène informatique, par exemple effectuer les correctifs de sécurité, cloisonner certains flux sur le SI, gérer les droits d'accès de façon rigoureuse…Ces mesures qui sont parfois difficiles à faire appliquer ont pourtant fait leurs preuves, puisqu'on constate que les structures qui les ont mises en œuvre sont celles qui ont le mieux résisté, voire qui ont simplement survécu à une crise.
- Il peut également s'agir de renforcer la diversité et la flexibilité des systèmes. Par exemple, intégrer au parc informatique des équipements fonctionnant sous Mac OS ou Linux permet de limiter le risque de propagation des malwares à l'ensemble du parc, ces derniers étant en grande majorité conçus contre des systèmes fonctionnement sous Windows ou ne ciblant qu'un seul OS. Il peut également être utile de prévoir la possibilité de couper certains pans du réseau, par exemple en ayant recours à des applications stockées dans un Cloud.
- Il convient ensuite d'être particulièrement vigilant à tous les outils qui peuvent avoir un effet d'amplification de la crise, comme par exemple les annuaires centraux type Active Directory, les antivirus, etc.
- Enfin, revoir et mettre à jour régulièrement les plans d'alerte et de continuité d'activité et étendre le système de gestion de crise à la cybersécurité reste essentiel.

B. Préparation

Les récentes attaques ont rappelé que ni les équipes IT de l'entreprise victime ni les autorités appelées pour y répondre ne sont généralement suffisamment préparées pour faire face à des attaques d'envergure. L'inadéquation entre la nature de l'attaque et la réponse apportée par les autorités ukrainiennes envoyant leurs forces spéciales pour investir les locaux d'où était partie l'attaque NotPetya[17] en 2017, l'a bien illustré.

D'autre part, la survenance d'une crise est encore trop souvent synonyme de panique. Pour l'équipe dirigeante d'abord, qui voit la crise se diffuser sans la comprendre ni pouvoir remédier eux-même à la situation. Pour les équipes techniques ensuite, qui se voient privées d'outils d'administration, de schémas réseaux, de consoles pour reprendre la main sur les équipements affectés, ou de journaux pour investiguer.

Pour éviter ses écueils, une organisation doit, régulièrement, se préparer à réagir rapidement et efficacement en cas de crise. Plusieurs mesures et processus peuvent y contribuer.

[17] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

- **L'entrainement des personnels, et surtout des équipes opérationnelles** (par exemple via des simulations de crise ou des exercices de mise en situation) permettent d'apprendre à mieux gérer les imprévus et de mieux appréhender les étapes à suivre en cas de crise majeure. Ils permettent aussi de sensibiliser la chaîne décisionnelle à la nécessité de prévoir un budget pour la cybersécurité.
- **La mise en place d'un système de gouvernance et de gestion de crise externe** et gérée par un autre fournisseur. D'abord parce que la remédiation à une attaque cyber nécessite la mobilisation d'une multiplicité d'expertises et de compétences techniques différentes et complémentaires dont ne dispose pas toujours l'entreprise touchée, ensuite parce que les attaques endommagent par définition le SI nominal de l'organisation affectée, qui peut donc ne plus être en mesure de gérer la crise via son propre SI.

Le volet **« communication de crise »** de l'entreprise doit également participer de ces efforts d'anticipation. La communication de crise se prépare en amont, notamment sur les réseaux sociaux tels que Twitter et Facebook, de plus en plus utilisés par les entreprises pour communiquer avec le public au détriment de voies plus traditionnelles telles que la presse. L'utilisation de ces réseaux, dont les publications atteignent instantanément un public vaste et varié, permet à l'entreprise, si elle réussit en amont à construire et fidéliser un réseau de *followers*[18] suffisant, de communiquer aisément et rapidement en temps de crise pour informer le public mais aussi ses propres employés de son déroulement et de sa résolution.

Par ailleurs, **le porte-parole** occupe une place majeure lors d'une crise. Représentant de la société pour le public et les médias, ce rôle doit être attribué au préalable à un membre du personnel qualifié et entraîné à ce type d'exercice. Un guide de questions-réponses permet de définir des éléments de réponse que le porte-parole peut aisément assimiler pour, le jour de la crise, faire passer rapidement les bons messages.

C. Réponse et gestion de crise

Face à une crise aux effets potentiellement dévastateurs, une organisation doit assurer la continuité de ses activités et très rapidement envisager à la fois la reconstruction de son système d'information et limiter les atteintes à sa réputation et à son image auprès de ses employés, de ses clients et du grand public. Dans ce cadre, la gestion et la communication de crise sont essentiels pour limiter les impacts d'une cyber-attaque.

➢ <u>Investigation</u>

Sur le plan technique, les équipes dédiées doivent investiguer la cause de l'attaque (malware, chemin d'entrée de l'APT, failles dans le système d'information, etc.) notamment pour :

- Identifier le « **patient zéro** », à l'origine de la diffusion du malware au sein du système d'information de l'entreprise ;

[18] Personnes suivant, par le biais de réseaux sociaux, le compte de l'entreprise.

- Définir les **éléments de remédiation** (vulnérabilités du système affecté) dans le but de protéger et reconstruire tous les domaines du système d'information (serveurs, postes de travail, etc.) ;
- Collecter des éléments de preuve permettant à l'entreprise de se ménager des possibilités d'action judiciaire et assurantielle.

Les équipes de l'entreprise affectée sont souvent accompagnés dans ces efforts par des organisations dédiées, comme les CERT, les agences nationales de protection des SI, comme l'ANSSI en France, lorsqu'il s'agit d'opérateurs d'importance vitale, ou des acteurs privés spécialisés.

➢ Remédiation

Dans l'immédiat post-crise, les organisations affectées doivent d'abord trouver de nouveaux moyens de communiquer, par exemple en ayant recours à des applications de messageries moins sécurisées mais grand public et utilisées par le plus grand nombre. Des mesures permettant d'empêcher la propagation de la crise aux pans du SI qui auraient été épargnées peuvent également être appliquées, et dans certaines situation l'arrêt du réseau peut aussi s'avérer utile.

Dans un second temps, une structure de gestion de crise doit être mise en place. Elle peut par exemple comprendre :

- Un comité de crise au niveau de la direction générale, chargée de la prise de décision et de la résolution d'éventuels points de blocage ;
- Une équipe intervenant sur l'aspect « business » chargée à la fois de trouver des moyens de continuer à faire fonctionner l'organisation sans système informatique, et d'autre part de décider de l'ordre et de la chronologie du redémarrage des différents réseaux de l'organisation ;
- Une équipe IT chargée de l'investigation et de la définition d'un plan de défense pour sécuriser le SI et du plan de reconstruction.

➢ Communication

La communication demeure une priorité lorsqu'un incident survient, car elle permet d'éviter qu'il ne se transforme en crise médiatique s'il est mal géré et que la communication est défaillante ou inadaptée. Une réponse coordonnée et préparée des éléments de communication peut ainsi permettre de limiter les incidents, et d'éviter une perte de temps et financière tout autant qu'une atteinte à la réputation et à l'image de l'entreprise. Pour ce faire, plusieurs bonnes pratiques permettent de gérer au mieux la communication de crise dans les premières heures :

- Fixer en amont les **objectifs de la communication** : s'agit-il d'alerter la population/les employés/les investisseurs, de la rassurer, etc. ?
- Identifier et avoir recours aux **bons canaux de communication** (les réseaux sociaux, par exemple) pour positionner l'entreprise concernée comme l'interlocuteur principal et le détenteur d'informations fiables.
- **Doser la réactivité et la régularité** de la communication, c'est-à-dire ne pas se précipiter, ni trop attendre, ni communiquer trop peu ou trop souvent, pour témoigner de la mobiliser des équipes de gestion de crise.

- Ne pas minimiser la crise et être, autant que possible, transparent et honnête, et notamment **assumer** les éventuels dysfonctionnements. Pour autant, il est essentiel de rester factuel et cohérent, et ne communiquer que les éléments vérifiés sans émettre d'hypothèses sur lesquelles il sera difficile de revenir le cas échéant.
- Ne pas négliger la **communication interne**, qui permet de rassurer les équipes et d'éviter la panique au sein même de la société qui fait déjà face à la crise. D'autre part, les employés de l'entreprise touchée peuvent, s'ils sont correctement informés par leur hiérarchie des mesures et des actions concrètes qu'elle mène, faire office de relais pour diffuser ces informations via les réseaux sociaux, auprès de proches à la recherche d'informations ou « d'i*nsiders* ».

D. Reconstruction

La reconstruction du système d'information et le retour à la normal est un travail de long terme (on estime à 3 semaines en moyenne le temps de redémarrage), d'autant plus complexe que le SI a été construit en plusieurs étapes. Le reconstruire pour revenir à la normale nécessite notamment de réinstaller tous les postes de travail. Plusieurs solutions permettent d'accélérer le processus comme par exemple :

- Confier aux collaborateurs la réinstallation de leurs postes de travail, grâce à des clés USB, ce qui permet aussi de les impliquer dans la résolution de la crise ;
- Le recours à des services cloud et de virtualisation, qui permettent de cloner certains systèmes.
- Les fournisseurs et partenaires de l'entreprise affectée peuvent également représenter des relais d'accélération de reconstruction du système d'information, notamment parce qu'ils possèdent parfois des bases de données qui auraient été perdues sur le système affecté, etc.

E. La sortie de crise

Ce processus de gestion de crise et de retour à la normale doit s'accompagner sur le long terme d'efforts pour renforcer la cybersécurité et la résilience de la société. Même reconstruit, le nouveau SI pourra à son tour faire l'objet d'attaques, et une organisation se doit d'être proactive pour trouver sans cesse de nouvelles solutions et protéger au mieux ses systèmes ainsi que ses données et celles de ses clients.

La résolution de la crise et la démobilisation des équipes de gestion de crise doivent être actées, c'est-à-dire communiquées, à la fois interne auprès des collaborateurs et plus largement auprès des fournisseurs et du grand public.

5 ANNEXES

Annexe 1 : Liste des participants (confidentielle et non diffusable)

Annexe 2 : Brochure du programme de la journée

Annexe 3 : Scénario de la simulation stratégique

Annexe 4 : Supports de présentation des intervenants