Amélioration de la cyber sécurité d'un système d'information par augmentation du niveau de confiance

Cyril Sanchez

École d'ingénieur du
Conservatoire national des arts et métiers – Paris

AMELIORATION DE LA CYBER SECURITE D'UN SYSTEME D'INFORMATION PAR AUGMENTATION DU NIVEAU DE CONFIANCE.

Mémoire pour le titre d'Ingénieur Diplômé par l'État – spécialité Informatique, soutenu en 2020 par

Monsieur SANCHEZ Cyril

RÉSUMÉ

L'objectif de ce mémoire est de définir la meilleure stratégie à appliquer pour sécuriser le système d'information étudié. Pour cela, l'architecture du système d'information à protéger sera mise en perspective par l'étude des menaces cyber pesant sur ce système et par l'analyse du cadre législatif encadrant le cyberespace tant au niveau international que national.

La menace la plus probable provient des groupes malveillants soutenus par des états. Ces acteurs disposent de moyens importants leurs permettant de mettre en œuvre des Techniques, des Tactiques ainsi que des procédures complexes, efficaces et difficilement détectables. De plus, la structure du cyberespace donne la possibilité à ces organisations de mettre en œuvre des techniques d'anonymisation rendant extrêmement complexe l'attribution de ces attaques. C'est cette immunité qui encourage les cyberattaquants à mener des actions décomplexées.

L'étude de la régulation internationale du cyberespace fait émerger des divergences importantes dans la vision qu'en ont les états. Les faiblesses législatives qui en découlent sont un avantage supplémentaire pour les hackers dans leur quête de clandestinité.

Dans ce contexte, la France met en œuvre depuis une quinzaine d'années une politique volontariste de cyberdéfense. Elle se matérialise à travers deux axes principaux. Le premier est une législation contraignante en matière de sécurité des systèmes d'information et notamment pour les organismes désignés par l'état comme d'importance vitale. Le second est la création d'organismes étatiques dédiés à la cyberdéfense.

Le système d'information à protéger est accessible depuis Internet et du fait de son évolution historique est constitué de différentes briques de sécurités hétérogènes qui ne répondent pas à une politique de sécurité centralisée. Pour contrer au mieux les capacités d'anonymisation des cybers attaquants, la stratégie choisie va consister à augmenter le niveau de confiance dans le système d'information. Pour cela, trois axes d'amélioration sont identifiés : la confiance dans les connexions, l'authentification et enfin les journaux d'évènement.

Les technologies mises en œuvre pour atteindre ces objectifs sont les Réseaux Privés Virtuels[1], les Infrastructures de Gestions de Clés et enfin des systèmes complémentaires pour protéger les journaux d'évènements. L'association de ces technologies rend l'intrusion du système d'information plus complexe en limitant la liberté d'action du cyber attaquant. De plus, la journalisation des évènements va permettre d'analyser avec précision les actions menées en cas d'événement de sécurité et enfin la gestion centralisée de la sécurité va simplifier la tâche des administrateurs

[1] RPV ou Virtual Private Network en anglais

ABSTRACT

This thesis aims to define the best strategy to secure the Information System I'm currently working on. In order to succeed, we'll consider this IS architecture in regard to the potential cyber threats weighing on this system and to the legislative framework governing cyberspace at both international and national levels.

The most likely threat comes from malicious groups backed by States. These actors benefit from significant resources which allow them to have complex, efficient and hard to detect techniques, tactics and procedures. Moreover, the cyberspace structure allows these organizations to implement anonymization techniques aiming to make these attacks attributions extremely complex. This precise immunity encourages cyber hackers to launch uninhibited actions.

The study of the cyberspace international regulation reveals some consequent differences within the way States consider these issues. And the resulting legal weaknesses constitute an additionnal advantage for these hackers.

In this context, France has been implementing a proactiv cyber defense strategy for the past fifteen years. This policy is organized into two main directions. The first one consists on a restrictive legislation regarding IS security, especially for the structures French state considers as of vital importance. The second one is the creation of state agencies dedicated to cyber defense.

The IS we aim to protect through this thesis is accessible from the internet and, because of its historical evolution, is based on different heterogeneous security bricks which are not linked to a centralized security policy. In order to resist to the anonymization capacities of cyber hackers, the most accurate strategy will be to increase the level of trust in the information system. To do so, three improvement axes have been identified: trust in connections, authentification and events logs.

The implemented technologies to reach these goals are the Virtual Private Networks, the Public Key Infrastructures and finally the additional systems to protect events logs. The association of these technologies will make the intrusion into the IS more complex, by limiting the cyber hackers' freedom of action. Moreover, the event logging will allow an accurate analysis of the led actions in case of a security event. Finally, centralized management of the security issues will simplify the administrators' tasks.

" L'essentiel dans l'éducation, ce n'est pas la doctrine enseignée, c'est l'éveil. "

Ernest Renan

REMERCIEMENTS

Je tiens à remercier l'ensemble des personnes qui m'ont soutenu lors de la rédaction de ce mémoire et sans qui j'aurais eu les plus grandes difficultés à concilier ces travaux avec mes obligations professionnelles et personnelles.

En premier lieu, Brice, mon directeur de mémoire, qui a toujours été présent pour répondre à mes interrogations et qui m'a fait bénéficier de ses connaissances qui semblent parfois sans limite ;

Sandrine, qui m'a aidé à exprimer mes idées avec clarté et qui m'a soutenu dans les moments de doute ;

Lucas et Sébastien, qui m'ont fait bénéficier de leur expertise technique face aux incertitudes que je rencontrais ;

Franck, qui m'a fait découvrir le diplôme d'IDPE ;

Et enfin mes enfants, qui ont pendant un an vu leur papa passer du temps à travailler sur le « mémoire » au lieu de jouer avec eux sans jamais se plaindre.

TABLE DES MATIERES

INTRODUCTION

Ces trois dernières décennies ont été les témoins d'une véritable révolution numérique mondiale, bercées par la montée en puissance d'Internet. Celle-ci s'observe en premier lieu chez les particuliers, avec près de 2,87 milliards d'utilisateurs d'ordiphones sur la planète, mais également au sein des entreprises, qui n'hésitent plus à confier leurs fonctions les plus critiques à des services dématérialisés hébergés sur Internet.

Pourtant, au-delà de son succès incontestable, la croissance exponentielle de ce nouvel espace d'échange d'informations et de richesses constitue également de nouvelles opportunités pour des groupes malveillants. Ces attaques informatiques, toujours plus nombreuses et complexes, peuvent alors avoir des conséquences catastrophiques sur la population, les entreprises et même les états.

Afin de contrer ces agressions, les principaux acteurs du cyberespace (états, organisations, entreprises, etc.) s'organisent progressivement, développent des outils de plus en plus performants, et tentent de légiférer ensemble.

Dans ce contexte, il convient de définir les priorités à donner aux différentes orientations techniques et stratégiques visant à accroitre significativement la cybersécurité des systèmes d'information.

Afin de mener ce travail, nous analyserons d'abord la nature et l'évolution de la menace pesant sur Internet. Puis nous nous intéresserons aux avancées de la régulation internationale dans le cyberespace, ainsi que sur l'organisation de la lutte informatique défensive en France, en particulier au sein du ministère des armées. Nous illustrerons enfin l'ensemble de ces éléments et les problématiques qui en découlent au travers du système d'information dont on m'a confié la responsabilité. Nous recommanderons alors une stratégie précise et des moyens adéquats visant à atteindre un niveau de sécurité optimal.

I. Etude de la menace

Devenu un lieu Incontournable pour les échanges mondiaux (économie, culture, recherches, etc.), le cyberespace est aujourd'hui un milieu critique pour les états comme pour les sociétés. Peu sécurisé pendant de longues années, il a permis aux cybers attaquants de mener des actions offensives pour atteindre des objectifs variés. Depuis une quinzaine d'années, la prise en compte de la cyber défense dans les SI a permis aux différents acteurs utilisant Internet de se protéger d'une partie des actions malveillantes. Malgré cela, les groupes malveillants restent une menace importante pour les systèmes utilisant Internet.

Cette première partie a pour objectif de décrire les menaces pesant sur les systèmes d'information à protéger. Pour cela, il sera énuméré dans un premier temps les différents types de cyber attaquants, puis suivra une analyse de la complexification des attaques informatiques pour enfin identifier les raisons et moyens permettant aux hackers de mener des attaques anonymes.

A. Les cybers attaquants

1. Profils des attaquants

Au fur et à mesure de la croissance du cyberespace, le profil des cyber attaquants a fortement évolué. Les hackers informaticiens, faisant cela à l'origine presque par jeu, ont laissé place à des groupes étatiques ou mafieux dont les objectifs diffèrent du simple challenge.
Leur identification est complexe pour 2 principales raisons :

- L'utilisation de techniques rendant quasi impossible la remonté de l'attaque par les services de police ;
- La volonté d'éviter de commettre des méfaits dans, ou contre, les pays dans lesquels ils résident et donc de s'abriter derrière le banditisme transfrontalier.

C'est dans ce conteste que les sociétés THALES et VIRINT[2] se sont associées pour mener une étude qui a débouché sur « The CyberThreat Handbook ». Dans ce rapport, les profils identifiés dans des cybers attaques sont les suivants :

- Etats nation (49% des attaques)

Groupes d'attaquants parrainés par un état. Leurs actions sont significatives car ils sont dotés de moyens financiers conséquents et d'un excellent niveau technique. De plus,

[2] https://www.thalesgroup.com/fr/group/journaliste/press-release/cyberthreat-handbook-thales-et-verint-presentent-leur-whos-who-des

les attaques ne sont pas menées au hasard et ciblent avec précision les victimes de leurs actions malveillantes.

- Hacktivistes (26% des attaques)

Les motivations des groupes « hacktivistes » sont essentiellement idéologiques. C'est pour cela que les victimes de leurs offensives sont ciblées. En revanche ces groupes disposent de peu de moyens et, hormis quelques exceptions, possèdent des compétences techniques plutôt moyennes.

- Cybercriminels (20% des attaques)

Les cybercriminels disposent, à l'image des états, de moyens financiers importants et d'un très bon niveau technique. La différence réside dans les cibles qui doivent seulement répondre à un critère de rentabilité.

- Terroristes (5% des attaques)

Ces groupes d'attaquants ont à leur disposition les moyens financiers nécessaires à l'atteinte de leurs objectifs. En revanche leurs actions sont souvent conduites de façon opportuniste afin de limiter le niveau technique nécessaire.

En résumé :

Statistiquement, on constate que les groupes parrainés par des états constituent la plus grande menace qui pèse sur le système d'information à protéger. Le défi technique à relever en est d'autant plus important.

2. Les objectifs & les cibles

Afin de pouvoir se protéger et mesurer les risques encourus par le système d'information, et notamment ceux décrit dans la norme ISO 27001 ou dans l'instruction générale Interministérielle 1300 (DIC), il est indispensable d'identifier les objectifs poursuivis par les cybers attaquants. Dans sa Revue stratégique de cyber défense datée du 12 février 2018, le SGDSN décrit les 4 principaux objectifs[3] poursuivis par les cybers attaquants.

[3] www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

- Le renseignement qui porte atteinte à la confidentialité :

Discrète, sa récupération peut être motivée par :

- L'appât du gain en faisant pression sur la société victime afin de ne pas divulguer les informations. (Extraction de base client par exemple)
- L'espionnage industriel ou politique, mené généralement par les états.

- La désinformation qui porte atteinte à la véracité de l'information :

Utilisé par des groupes idéologiques ou des états, elle a pour objectif d'influencer un groupe plus ou moins important

- L'entrave qui porte atteinte à la disponibilité ou l'intégrité :

Il s'agit de la mise hors service d'un service ou d'un système d'information. Les effets peuvent déborder du cyberespace et se ressentir sur des infrastructures physiques (surtout si un système industriel est visé.) Selon la complexité de l'attaque, elle peut être menée par un groupe ou un état.

- Le trafic mafieux qui porte atteinte à la confidentialité :

L'objectif est de voler et/ou pouvoir mettre à disposition des biens ou services illégaux contre monétisation.

En résumé :

Il est intéressant de mettre en parallèle ces objectifs avec les cibles les plus fréquemment attaquées, les secteurs les plus ciblés étant ceux des services étatiques et notamment ceux de la défense, de la finance et de l'énergie.

A la vue de la nature du SI à protéger, les objectifs principaux des attaquants seront vraisemblablement le renseignement et l'entrave.

B. Augmentation de la complexité des attaques

Les acteurs du cyberespace ont au fur et à mesure de leur prise d'expérience fait évoluer leurs procédés pour mener des attaques informatiques. Elles peuvent être déclinées en trois domaines en utilisant l'analogie militaire des TTPs pour Tactiques, Techniques, Procédures.

1. L'évolution des tactiques

Afin de comprendre l'art de la tactique dans le cyberespace, voyons dans un premier temps sa définition :

> *« Art de diriger une bataille, en combinant par la manœuvre l'action des différents moyens de combat et les effets des armes, afin d'obtenir un résultat déterminé. »*[4]

Cet art est aussi appliqué par les groupes malveillants dans le cyberespace au même titre que des forces armées dans les différents milieux physiques (terrestre, maritime, aérien…).

Les tactiques mises en œuvre sont de plus en plus complexes et font appel à des combinaisons de différentes techniques et outils leur permettant d'atteindre un objectif clairement identifié. Les tenants et aboutissants de la tactique dans le milieu cyber peuvent être illustrés par quelques exemples :

Attaque par hameçonnage ciblé (Spearfishing) :

Pour mesurer l'augmentation de la complexité des attaques, il est possible d'analyser l'évolution de la technique malveillante qu'est le « fishing » et de montrer comment elle a évolué ces vingt dernières années. Pour exemple, le passage de campagne de fishing massif à des envois plus ciblés démontre une adaptation des TTPs qui s'apparente aux techniques de ciblage utilisées dans le domaine marketing qui, par la personnalisation du message délivré, permettent aux hackers d'augmenter la probabilité de réussir leur méfait (social engineering).

[4] Dictionnaire LAROUSSE

Hameçonnage massif	Hameçonnage ciblé
Création d'un courriel piégé	Etude des cibles
Mise en œuvre d'un serveur de contrôle	Création de courriels personnalisés
Envoi massif du courriel	Mise en œuvre d'un serveur de contrôle
	Usurpation de la boîte aux lettres des correspondants réguliers des cibles ou création d'une couverture crédible
	Envoi de courriels ciblés

Tableau 1 – Comparatif entre l'hameçonnage massif et l'hameçonnage ciblé

Cet exemple illustre la professionnalisation de la tactique mise en œuvre. Cette évolution va diminuer les chances d'être détectée par la victime et va dans le même temps augmenter la probabilité de réussir l'hameçonnage.

Opération Olympic Games :

Il existe des tactiques malveillantes extrêmement complexes nécessitant un haut niveau de planification. A titre d'illustration, le cas référencé le plus marquant de cette tendance est l'opération Olympic Games dans laquelle a été utilisé le virus STUXNET contre les systèmes industriels nucléaires iraniens en 2010. Sans entrer dans le détail de l'opération en elle-même, sa complexité est définie par les points suivants :

- Utilisation de 4 vulnérabilités « zéro days » ;
- Maîtrise en procédés industriels (SCADA) ;
- Programmation d'une date d'auto-destruction du code malveillant ;
- Infection d'un réseau isolé d'Internet (Air gap)
- Attaque étalée sur plusieurs années.

Dans cet exemple, à la vue du coût de ce type d'attaque, le groupe malveillant qui en est à l'origine est surement soutenu par un état.

En résumé :

Ces tactiques élaborées rendent les contre-mesures plus difficiles à mettre en œuvre et, qui plus est, ne les limitent pas au domaine technique.

2. Augmentation de la complexité des outils techniques utilisés

Le développement exponentiel du réseau Internet, la mise en œuvre de technologies complexes et la prise en compte de la composante cyber sécurité dans les développements ont naturellement poussé les hackers à adapter leurs outils offensifs.

Pour y parvenir, plusieurs leviers peuvent être utilisés par les attaquants ne disposant pas de capacités de développement.

Le premier est une conséquence indirecte de l'évolution du nombre d'acteurs dans le domaine de la cyber sécurité (CERT[5], Agence étatique, Sociétés spécialisées) et de l'ouverture et de la transparence dont font preuve ces entités.

En effet, **ces structures rendent fréquemment publique des vulnérabilités ou des outils (framework)** sous couvert d'actions légales de test de pénétration informatique (PENTEST) en vue de faciliter la sécurisation des SI existants. Disponibles et faciles à mettre en œuvre, ces outils peuvent se révéler très efficaces aux mains des groupes précédemment décrits qui ont de fait la capacité de les utiliser au profit d'objectifs malveillants.

Avantages :

- Facile d'accès
- Gratuit
- Soutenu par une grande communauté de passionnés
- Utilisation anonyme

Faiblesses :

- Mode de fonctionnement connu (Signatures IDS)
- Limité à des « one day », des vulnérabilités déjà connues

Le second moyen pour mettre en œuvre une capacité malveillante complexe est de **faire appel à des groupes mafieux** qui peuvent mettre à disposition leurs capacités contre paiement. Ces services peuvent se trouver assez facilement sur le « darknet » moyennant quelques recherches. En utilisant des cryptomonnaies et les moyens d'anonymisation de leur connexion, les commendataires peuvent rendre leurs actions extrêmement difficiles à tracer et leur identité quasiment impossible à établir.

Avantages :

- Accès rapide à une expertise
- Discrétion

[5] Computer Emergency Response Team

Faiblesses :

- Coût
- Maîtrise des actions menées

En résumé :

La complexité de ces attaques met en avant la nécessité de mettre en œuvre des stratégies de défense en profondeur du SI

3. Mise en œuvre des procédures d'actions offensives

La professionnalisation des attaques informatiques par des groupes organisés ou des états a naturellement conduit à la mise en œuvre de processus[6] permettant d'augmenter les chances de réussite. On peut distinguer 4 phases[7] :

- Le ciblage / caractérisation : Cette phase préliminaire à toute action a pour objectif d'étudier l'architecture cible en identifiant les points d'accroche (vulnérabilités). Des travaux permettent ensuite d'identifier l'exploitabilité de ces faiblesses en fonction des outils dont le groupe ou l'état dispose.

- L'intrusion : Dans cette partie, les attaquant exploitent des vulnérabilités techniques ou humaines afin de prendre pied dans l'architecture cible. Dès que cela est fait, une première analyse peut permettre de valider la pertinence de la cible.

- La latéralisation : Les attaquants vont s'attacher à sécuriser les accès utilisés pour pénétrer la cible. Ensuite une phase de recherche d'accès de secours sera éventuellement faite dans le cas une intrusion sur le long terme

- L'exploitation : C'est dans cette phase que les attaquants vont atteindre leurs objectifs.

Chaque étape de ce processus permet aux groupes qui les mettent en œuvre d'identifier avec efficacité les faiblesses de leurs cibles ainsi que les éventuels outils de sécurité déployés. Cette professionnalisation des actions offensives rend la défense d'autant plus complexe.

En résumé :

Pour défendre au mieux un système d'information, il apparait nécessaire de stopper au plus tôt la menace

[6] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[7] www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

C. Des attaques décomplexées

Les attaques informatiques sont nombreuses et menées sans appréhension des conséquences. Actuellement toutes les entités présentes dans le cyberespace sont susceptibles de subir des attaques qu'elles soient des sociétés ou des états...

La France est régulièrement la cible de cyber attaquants dont les motivations peuvent être variées. Quelques exemples :

- Dans le domaine de l'espionnage industriel, AREVA en 2011 ;
- Une campagne de désinformation a été menée en 2017 à l'encontre du candidat Emmanuel MACRON durant les élections présidentielles ;
- A des fins mafieuses, une attaque via un cryptovirus a été menée contre l'hôpital de Rouen en 2019 et a provoqué la paralysie de son système d'information.

Dans ces quelques exemples, les commanditaires et les attaquants n'ont pas encore été identifiés et ne sont donc pour l'instant pas inquiétés par la justice. Cette impunité est due notamment à la structure « des Internets » et aux techniques d'anonymisation utilisées.

1. La construction des Internets

Du fait de sa modélisation et de son évolution, Internet rend complexe l'identification formelle d'une communication. En effet, avec peu d'effort, il est possible de s'y « déplacer » discrètement.

a) La structure

Par habitude, nous abordons le cyberespace comme une seule entité, «l'Internet ». Mais cette entité est en fait complexe et protéiforme, ce qui facilite la mise en œuvre de mécanismes d'anonymisation. Internet est constitué d'innombrables réseaux interconnectés entre eux[8]. On y trouve des réseaux opérateurs pour le transport des données, des data centers, des réseaux d'entreprises et d'états, des outils industriels (SCADA), des réseaux privés, des IOT[9], etc.

[8] Bonnemaison, A., & Dossé, S. (2014). *Attention : Cyber ! : Vers le combat cyber-électronique.* Economica.

[9] Internet of Things ou L'Internet des objets (IdO)

La multitude de réseaux, des interconnexions, des matériels et des acteurs ainsi que leurs évolutions rapides et permanentes rendent la cartographie intégrale d'Internet quasiment impossible. Ce constat nous éclaire sur les possibilités laissées aux cybers attaquants pour avancer dans l'ombre.

b) L'adressage

Les mécaniques d'adressage du protocole IP sont indispensables pour communiquer sur Internet. Dans sa version 4, ce protocole est limité et ne permet pas de répondre aux besoins et évolutions futurs. La réponse technique repose actuellement sur la version IP V6. Celle-ci permet entre autres d'associer une adresse unique pour chaque appareil se connectant sur Internet et représente potentiellement une aubaine pour identifier plus facilement la source d'une communication. Malheureusement, sa mise en œuvre est encore loin d'aboutir. En attendant et pour répondre à cette problématique, plusieurs principes ont été mis en œuvre sur IP V4 comme les adresses IP publiques dynamiques ou encore le principe du NAT qui permet de connecter de nombreux appareils derrière une seule IP publique. Les opérateurs GSM ont, par exemple, recours à ce moyen pour permettre à leurs très nombreux abonnés de se connecter à Internet avec un nombre limité d'adresses publiques.

En résumé :

Ainsi, la multiplication des réseaux (plus ou moins bien sécurisés), la gestion des adresses IP volatiles et la multiplication des appareils connectés sur Internet, facilitent le travail d'anonymisation des attaquants.

2. Les techniques d'anonymisation

Afin de se prémunir d'une éventuelle riposte ou judiciarisation, les personnes, groupes, entreprises ou états ont développé de nombreux moyens pour exploiter le cyberespace de façon anonyme[10].

a) Le cheminement

Clef de voute de l'anonymisation des actions malveillantes, les techniques visant à rendre une connexion anonyme se basent essentiellement sur deux principes :

[10] Pernet, C. (2014). *Sécurité et espionnage informatique - Guide technique de prévention - Connaissance de la menace APT (Advanced Persistent Threat) et du cyber espionnage.* Eyrolles.

Le rebond : L'objectif est d'utiliser des intermédiaires entre l'émetteur de l'information et le destinataire. Cela a pour conséquence de masquer l'adresse IP d'origine et de rester ainsi anonyme. Pour mettre en œuvre ce concept, le cyber attaquant peut utiliser des intermédiaires qu'il a compromis ou tout simplement profiter de services mis à disposition du grand public. Plus le nombre de rebonds est important et plus l'anonymisation sera efficace.

Le chiffrement : Afin de garantir la confidentialité d'une communication, les échanges doivent être chiffrés. La mise en œuvre de ces mécanismes dépend du type de chiffrement (symétrique ou asymétrique), de l'algorithme (AES, RSA, etc...), de la taille et des moyens de génération des clefs et enfin de la qualité de l'implémentation.

Il est facile de trouver sur Internet des prestataires qui mettent à disposition des services répondant plus ou moins efficacement aux critères de rebond et de chiffrement. Nous allons faire un point sur les moyens les plus fréquemment utilisés dans le cyberespace.

(1) Le serveur mandataire :

Mis à disposition gratuitement ou pour des sommes modiques, ce moyen est généralement utilisé pour profiter de services de navigation WEB plus ou moins anonymes (port 80 et 443) et consiste à utiliser une adresse IP différente de celle d'origine.

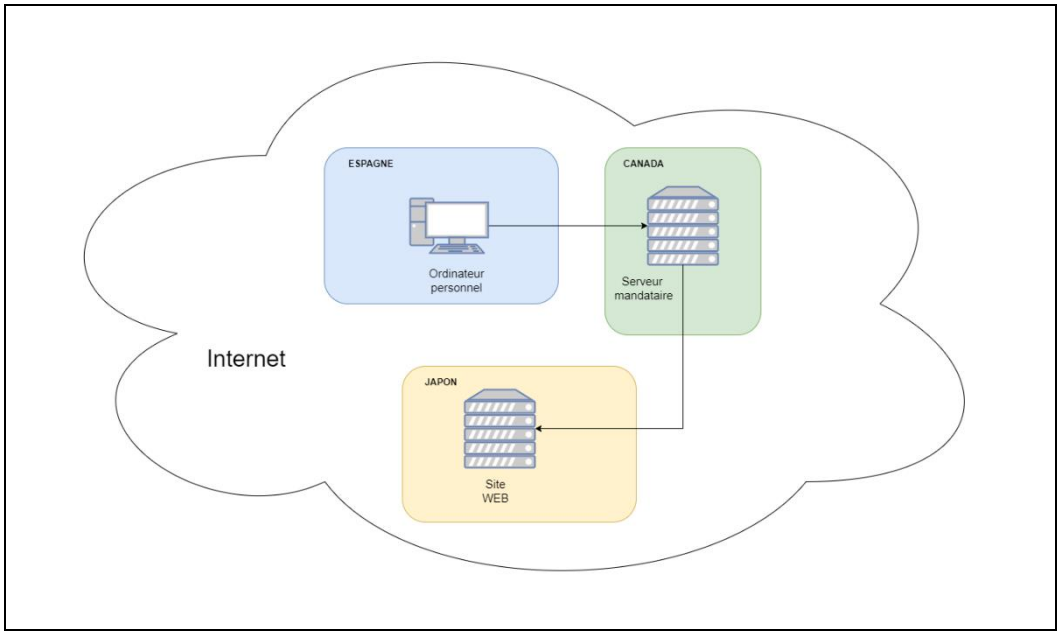

Figure 1 – Exemple d'emploi d'un serveur mandataire.

Avantages :

- Facile à configurer
- Grande disponibilité

Inconvénients :

- Chiffrement de bout en bout optionnel (port 80)
- Limité à certains services

(2) Réseau privé virtuel[11] (VPN):

Le principe de base est de créer un tunnel chiffré entre le client et le serveur du prestataire de service. Dès que le VPN est actif, les services utilisés par le client sont émis comme ayant pour origine le serveur du prestataire à l'image du proxy décrit précédemment. Les deux principales différences sont une connexion chiffrée dès l'émetteur et un panel de services utilisables plus important. Les technologies les plus utilisées pour monter ces tunnels sont TLS et IPSEC

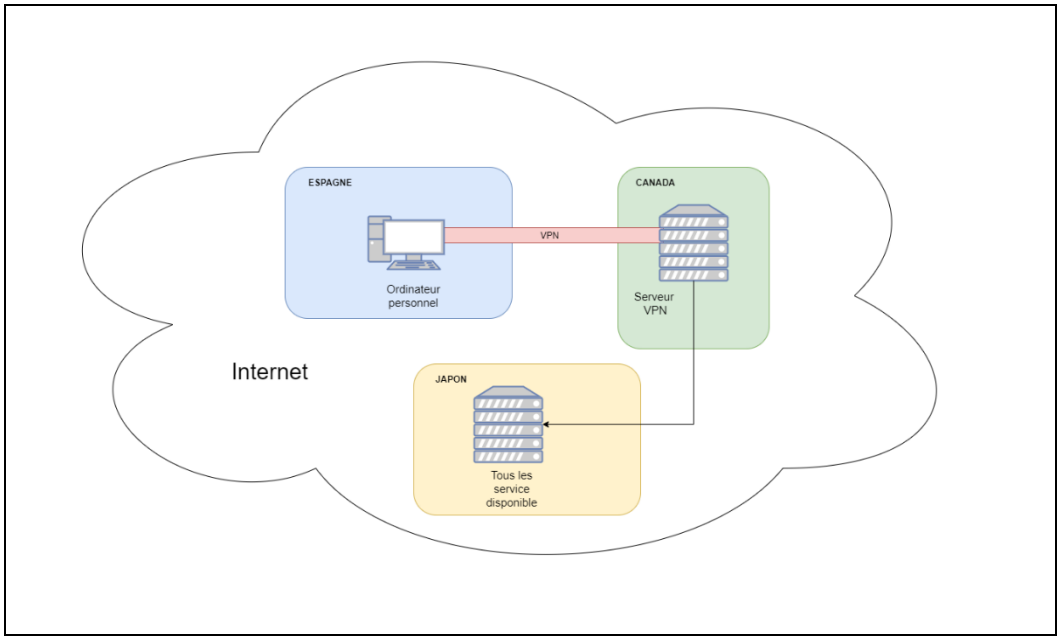

Figure 2 – Exemple d'emploi d'un VPN

Avantages :

- Chiffrement de bout en bout
- Possibilité d'utiliser tous les services (hors éventuelles limitations par le prestataire)

[11] RPV ou Virtual Private Network (VPN) en anglais

Inconvénient :

Difficulté technique si le prestataire ne fournit pas une application dédiée

(3) Les infrastructures d'anonymisation :

Il existe des architectures dédiées à l'anonymisation présentes en "libre-service" sur Internet[12]. Initialement prévues pour contourner la censure dans les pays non démocratiques, elles sont aujourd'hui utilisées pour mener des actions informatiques malveillantes. A ce jour, le réseau TOR est le plus utilisé même si des alternatives existent comme FREENET et I2P. TOR[13] est un logiciel tout-en-un qui intègre le montage d'un tunnel constitué de 3 rebonds aléatoirement sélectionnés (dans un groupe de plusieurs milliers) ainsi qu'un chiffrement largement éprouvé par la communauté. Ce montage dit « en oignon » permet de garantir une anonymisation de l'émetteur par remplacement de son adresse IP source à chaque rebond, rendant ainsi extrêmement difficile son suivi sur ce réseau.

Le réseau TOR :

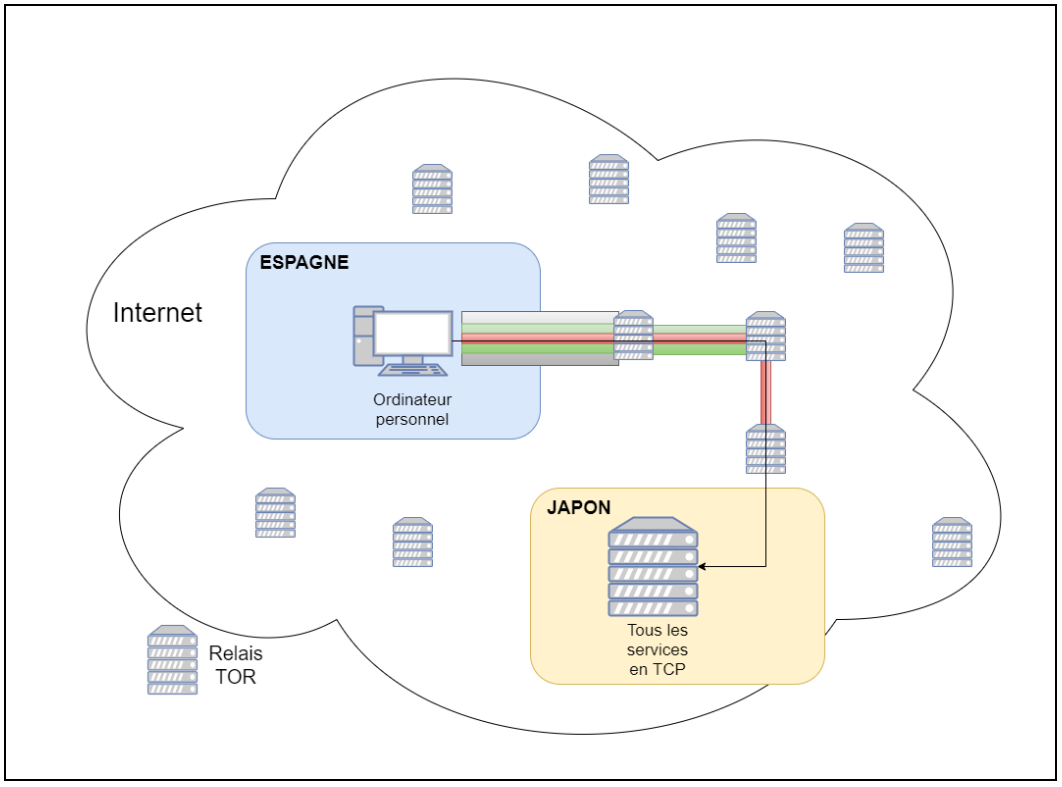

Figure 3 – Exemple d'emploi du réseau TOR

[12] https://fr.wikipedia.org/wiki/Anonymat_sur_Internet
[13] *The onion router*

Avantages :

- Chiffrement de bout en bout
- Anonymat garanti
- Compatible avec les services TCP
- Nombre de rebonds

Inconvénients :

- Incompatible avec les services UDP
- Débit et latence

En résumé :

Comme nous venons de le voir, les moyens disponibles pour améliorer plus ou moins efficacement l'anonymat d'une connexion sont nombreux et dans la plupart des cas gratuits et faciles à mettre en œuvre.

b) Les relais de commande

Afin de garantir un fonctionnement optimal d'une attaque, deux éléments sont nécessaires au plus près d'une cible.

Le premier est le serveur de pilotage des outils ou C&C (Command and control), il permet d'utiliser des outils comme des scanners de port directement sur la cible ou de piloter des MALWARE déjà présents dans la structure cible. Le second est le serveur permettant de recueillir les informations extraites du système d'information compromis par l'attaque.

On peut naturellement se poser la question de l'utilité de placer ces deux serveurs (un seul peut cumuler les deux rôles) directement devant la cible. Les proxy et VPN public ainsi que les réseaux d'anonymisation ont des adresses IP disponibles directement sur Internet. De fait, les responsables de la sécurité des SI passent en liste noire ces @IP pour se protéger d'une partie de la menace.

Afin de rester anonyme, il existe au moins deux méthodes visant à obtenir des serveurs anonymement.

La première consiste simplement à compromettre un serveur présent sur Internet et à l'utiliser discrètement pour ses propres besoins. La seconde consiste à louer ce type de service et à le régler avec une cryptomonnaie difficile à tracer.

c) Le code informatique

Lorsqu'une personne ou une équipe développe un programme malveillant (MALWARE), elle le fait avec un style qui lui est propre, parfois identifiable et dans lequel se glissent éventuellement des erreurs ou des malfaçons. Pour éviter cela, les hackers emploient des méthodes simples en réutilisant des outils d'audit ou des MALWARE publics en vue de les utiliser pour leurs propres besoins et en les modifiant à la marge. Efficaces, ces méthodes se limitent à l'exploitation de vulnérabilités connues mais sont encore loin de l'efficacité procurée par une vulnérabilité non connue (zéro day[14])

[14] Vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu

II. Cadre juridique applicable et description du système à sécuriser

Internet est aujourd'hui un outil omniprésent et incontournable pour le bon fonctionnement de notre société. Une action malveillante peut ainsi avoir des impacts majeurs dans différents domaines et notamment sur l'économie, la politique, la santé, l'énergie, etc.

Dans la première partie de ce mémoire, nous nous sommes attachés à décrire l'évolution des menaces pesant sur les systèmes d'information connectés à Internet ou le constituant. Dans ce cadre, les états tentent de s'organiser et de s'adapter pour maitriser et sécuriser ce nouvel espace public.

Cette deuxième partie visera donc d'abord à analyser les tentatives de régulation du Cyberespace à l'échelle internationale, puis se concentrera sur l'organisation de la Lutte Informatique Défensive (LID) au niveau national. Nous étudierons enfin l'architecture d'un SI particulier et en identifierons les stratégies spécifiques de cybersécurité.

A. Le cyber espace à l'international

Le droit s'applique au niveau des états mais également au niveau international dans le cadre de structures coopérantes ou d'association de pays (ONU, Union Européenne). Cependant, la notion de frontière dans le cyberespace permettant de définir ou non l'application d'un droit national est complexe et récente. Les difficultés à légiférer et à s'organiser au niveau international rendent l'application du droit dans le cyberespace difficile et inégal entre les états, facilitant la tâche aux cyberattaquants.

1. La notion de frontière

Depuis l'avènement de l'ordre westphalien, un pays ou un état peut être défini par son territoire et les frontières associées, son cadre juridique et la reconnaissance des autres états. Mais la notion géographique de frontières pose des difficultés si on souhaite la transposer à l'échelle du milieu faiblement matériel qu'est le cyberespace.

Comme l'explique Olivier KEMPF [15]dans son livre *Introduction à la cyberstratégie*[16], la notion géographique n'est pas suffisante et il propose trois niveaux possibles constitutifs de frontières :

- La couche physique qui représente le matériel nécessaire à la construction et au support. Elle prend la forme des fibres optiques trans-océaniques, des routeurs ou encore des datacenters.

- La couche logicielle qui représente la partie « soft » c'est-à-dire le code informatique. Il est présent dans le matériel actif, la gestion des *clouds* ou tout simplement les systèmes d'exploitation des ordinateurs ou ordiphones.

- La couche sémantique qui représente la langue utilisée. Sa première représentation est visible au travers des noms de domaines.

C'est actuellement la couche physique du cyberespace qui se rapproche le plus de la notion de frontière utilisée dans les conventions internationales. En effet, le matériel est installé sur le territoire d'un état précis, donc placé sous sa juridiction.

La couche logicielle est, elle, bien plus complexe à situer, le fonctionnement des systèmes en mode distribué s'affranchissant par exemple de la localisation du matériel. De plus, le fonctionnement d'un code informatique est souvent laissé à la discrétion de son éditeur, sans qu'un état ne puisse réellement l'influencer (cf. Le refus de Microsoft de fournir le code de Windows à l'Union Européenne au titre de la propriété intellectuelle).

La couche sémantique crée des frontières autour d'une langue. Mais en dehors de celles qui sont inhérentes à un état précis, comme la Chine et l'Iran par exemple, ces frontières sont poreuses et perméables.

Les premières négociations internationales ont ainsi eu lieu entre 2004 et 2017, sous l'égide du « Groupe des Experts Gouvernementaux en cybersécurité » (GGE) des Nations-Unies, pour réguler le cyberespace. Ces négociations ont notamment permis de définir des principes de droit international dans le cyber espace :

- L'interdiction d'attaquer les infrastructures critiques d'un état tiers en temps de paix ;
- L'interdiction d'attaquer les structures de réponse aux incidents (CERT, CSIRTS, etc.) d'un état tiers ;
- L'obligation de porter assistance à un état attaqué par un groupe situé dans un autre état si celui-ci en fait la demande.

Comme nous venons de le voir, la notion de frontière reste complexe dans le cadre du cyberespace. De plus, l'échec des négociations du GGE en 2017 et sa dissolution

[15] Ancien général de l'armée de terre, spécialiste des questions de stratégie dans le cyberespace

[16] Kempf, O. (2015). *Introduction à la cyberstratégie* . Economica

montrent les réticences des états à adopter une vision commune, notamment sur les points suivants :

- Un État peut-il mettre en place des contre-mesures en cas de cyber-agression ?
- Comment le droit humanitaire international doit-il s'appliquer au cyberespace ?
- Une cyberattaque remplit-elle les critères d'une attaque armée, permettant d'enclencher la légitime défense ?

Les cyberattaquants exploitent ce manque de vision commune entre les états et les vides juridiques associés pour mener à bien leurs actions sans crainte de représailles, à l'image de certaines zones de non-droit présentes sur la planète résultant de la faillite d'un état (Somalie).

En résumé :

Nous constatons que la notion de frontière dans le cyberespace reste très complexe à définir et empêche les différents états de converger vers des solutions communes en la matière. Face à ce défi, de nombreuses initiatives moins ambitieuses voient le jour à travers des accords internationaux, mais restent toutefois encore insuffisantes.

2. Les accords internationaux

A défaut de trouver un consensus mondial au travers des instances internationales de l'ONU, des pays partageant une vision commune de la cybersécurité s'organisent. En effet, l'évolution permanente du cyberespace et sa place croissante à tous les niveaux de notre société (institutions, économie, recherche, santé…) rendent sa régulation indispensable. Les organisations étatiques et non-étatiques doivent donc impérativement s'organiser pour protéger leur fonctionnement. Les initiatives ayant un impact majeur sur le cyberespace sont les suivantes :

a) Conférence sur la cybercriminalité

Également appelée Conférence de Budapest, elle a été organisée par le Conseil de l'Europe en 2001 (les comités d'experts ont été désignés en 1997). Ce protocole, ratifié dans plus d'une soixantaine de pays, vise deux objectifs principaux :

- Harmoniser le droit pénal dans la lutte contre le racisme, la xénophobie et la pédophilie sur Internet
- Améliorer la coopération Internationale dans les domaines précédemment cités

Malgré le consensus auquel devraient aboutir les domaines abordés par cette convention, l'absence de nombreux pays (comme la Russie ou le Brésil par exemple) fragilise l'efficacité de ce type de dispositif dans un espace où les frontières ont peu de valeur.

b) Organisation de la cyberdefense à l'OTAN

Pour rappel, l'Organisation du Traité de l'Atlantique Nord est forte de 29 membres et ses prises de position en matière de cybersécurité ont un impact mondial. C'est pour cette raison qu'il est important de mesurer son implication dans ce domaine. Depuis 2016, l'OTAN accroit ses exigences en matière cyberdéfense.

Organisation à vocation militaire, la première avancée majeure en la matière a été la reconnaissance du cyberespace comme un milieu d'opération, au même titre que l'air, la terre, la mer et l'espace. Dans ce cadre, elle soutient que le droit international s'applique au cyberespace.

Depuis, toutes les décisions de l'OTAN visent au renforcement des capacités cyber (offensives comme défensives) mais restent insuffisantes pour une régulation mondiale du cyberespace. En effet, comme l'ONU, l'OTAN n'est pour l'instant pas en mesure d'avancer des propositions dans ce domaine qui permettraient d'obtenir un consensus mondial. Qui plus est, sa position de force armée ne facilite pas ses négociations avec certains pays d'importance mondiale comme la Russie ou la Chine.

c) Global Commission on the Stability of Cyberspace

Le GCSC [17] est une initiative commune du gouvernement néerlandais, du Centre d'Etudes Stratégiques de La Haye et de l'Institut européen Est-Ouest, lancée en 2017. Elle est composée de 26 commissaires issus de la société civile, de gouvernements et de l'industrie. Elle vise principalement la proposition de normes dont chaque état pourrait s'inspirer pour les adapter à leur législation.

[17] Global Commission on the Stability of Cyberspace

Figure 4 – Objectifs du GCSC

Comme le reconnait elle-même la commission, ses axes de travail restent extrêmement génériques afin d'avoir une chance de trouver un consensus. Le dernier rapport de novembre 2019 énumère ainsi huit propositions de normes visant à faire progresser la régulation du cyberespace et le rendre ainsi plus sûr pour l'ensemble de ses utilisateurs. Pour autant, leur orientation trop généraliste visant à atteindre un consensus entre pays, empêche le GCSC d'apporter toute réponse à des problématiques spécifiques et concrètes. Ce contexte législatif international trop flou ne suffit donc pas encore à constituer une barrière suffisante face aux cyberattaquants.

De nombreux autres travaux comme la directive NIS de l'Union Européenne ou les propositions de Microsoft en 2017 pour une « convention de Genève du numérique » tentent de faire évoluer la sécurité dans le cyberespace. Ces initiatives aux résultats parfois encourageant restent néanmoins insuffisantes pour encadrer Internet dans sa globalité et donc de garantir un niveau de sécurité satisfaisant.

En résumé :

Face à une cybermenace présente à l'échelle internationale, les gouvernements agissent au niveau national afin de palier à l'échec partiel de la régulation mondiale du cyber espace. Des accords sont ainsi signés entre états afin de combattre conjointement les menaces cyber.

B. La Lutte Informatique Défensive en France

La France fait partie des pays les plus avancés au monde en matière de politique de cyberdéfense. Nous analyserons d'abord son organisation globale, puis nous étudierons plus spécifiquement les acteurs majeurs sur lesquels repose la cyberdéfense des armées françaises.

1. L'organisation

a) Les prémices

La prise en compte au plus haut niveau de l'Etat de la menace cyber a commencé au milieu des années 2000. Celle-ci prend la forme du rapport sur la sécurité des systèmes d'information du député Pierre LASBORDES, issu de travaux parlementaires menés en 2005. Ce document constate la faible prise en compte par la France des enjeux liés à la maitrise des systèmes d'information.

C'est en 2008, dans le livre blanc sur la défense et la sécurité nationale, que l'Etat a décidé de mettre en œuvre les moyens adéquats et une organisation ambitieuse. Le constat est le suivant :

> *« Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner. »*

C'est pour cette raison que la France doit se préparer à résister aux éventuelles cyberattaques.

> *« L'expertise de l'État en sécurité des systèmes d'information doit être fortement développée, entretenue et diffusée auprès des acteurs économiques et notamment des opérateurs de réseaux. La nature immédiate, quasi imprévisible, des attaques exige aussi de se doter d'une capacité de gestion de crise et d'après-crise, assurant la continuité des activités et permettant la poursuite et la répression des agresseurs. »*

Ces quelques lignes résument à elles seules la difficulté majeure d'anticiper et d'empêcher une attaque, mais également la nécessité de savoir en gérer les conséquences.

b) Le modèle Français de cyberdéfense

Le 7 juillet 2009, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est créée par décret[18] (nous décrirons ses missions ultérieurement). C'est à ce stade qu'est mis en œuvre le principe fondateur du modèle Français de cyberdéfense :

Il consiste à séparer le rôle de Lutte Informatique Offensive (LIO) de celui de Lutte Informatique Défensive (LID), ce dernier étant confié à l'ANSSI. L'objectif de cette distinction est de permettre aux partenaires privés et étrangers travaillant avec l'ANSSI de le faire en toute confiance, avec la certitude que l'agence ne se livre pas à un double jeu.

c) Passage à la vitesse supérieure

En 2013, la France a légiféré pour imposer des mesures de cybersécurité à certains organismes publics et privés. Ces structures sont regroupées sous la dénomination « Opérateurs d'Importance Vitale » (OIV). Elles constituent le noyau dur des infrastructures critiques françaises. La liste exacte n'est pas publique mais on sait qu'elle est structurée en différents secteurs tels que le transport, l'énergie, la santé, les télécommunications, etc.

Les mesures imposées se concentrent autour des principes suivants :

- Obligation de mettre en œuvre des mesures de sécurité édictées par l'ANSSI ;
- Obligation d'accepter d'éventuels audits par les services de l'état ;
- Obligation de déclarer tout incident.

Pour atteindre ces objectifs, les OIV peuvent bénéficier du soutien technique des organisations étatiques. De plus, si elles subissent des cyberattaques, l'état intervient pour les stopper et participe à la remise en service des infrastructures touchées afin de limiter au maximum leur impact. La France a été le premier pays à légiférer en ce sens pour imposer des mesures de cyberdéfense, et met tout en œuvre pour rester un leader dans le domaine. Nous pouvons par exemple citer :

- 2015 : Elaboration de la Stratégie nationale pour la sécurité du numérique
- 2018 : Création de la Revue stratégique de cyberdéfense
- 2020 : Création du Campus cyber

En résumé :

La France est un acteur investi et reconnu dans le domaine de la CYBERSTRATEGIE. Elle n'a de cesse de faire évoluer son organisation et sa législation pour répondre au mieux aux menaces CYBER.

[18] Décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009)

2. Les acteurs

Pour mettre en œuvre sa politique volontariste en matière de cybersécurité, la France a créé plusieurs structures. Nous décrirons succinctement les plus importantes au regard du système d'information qui sera étudié à la fin de cet écrit.

a) Le Secrétariat Général de la Défense et de la Sécurité Nationale

Le SGDSN a pour mission d'assister le Premier Ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. C'est là que sont élaborées, entre autres, les politiques nationales en matière de cybersécurité. La revue stratégique de cyberdéfense de 2018 en est un exemple. Cette stratégie de sécurité s'articule autour de cinq objectifs stratégiques :

- Garantir la souveraineté et assurer la sécurité des infrastructures critiques en cas d'attaque informatique majeure ;
- Protéger tous les citoyens et lutter contre la cybercriminalité ;
- Sensibiliser, former, informer ;
- Faire de la sécurité numérique un facteur de compétitivité ;
- Contribuer à l'avènement d'une souveraineté numérique européenne et au renforcement des capacités de pays alliés.

b) L'Agence Nationale de la Sécurité des Systèmes d'Information

L'ANSSI a été créée en 2009 pour répondre à la stratégie décrite dans le livre blanc sur la défense et la sécurité nationale. Ses missions ont évolué pour s'adapter aux menaces que les cyberattaquants font peser sur les systèmes d'information de la société française. A ce jour, ses missions sont les suivantes :

- Elle coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;
- Elle prescrit aux administrations et aux OIV des règles de sécurité préventives, en contrôle l'application et, en cas de crise majeure, peut leur imposer des mesures réactives ;
- Elle coordonne l'action gouvernementale en matière de défense des systèmes d'information et peut répondre, par des mesures techniques, aux attaques visant l'administration et les OIV, le cas échéant en neutralisant les effets de l'attaque.

Fer de lance des capacités de Lutte Informatique Défensive en France, cette agence dispose d'un grand nombre d'experts. Cette structure permet de considérablement améliorer la sécurité des OIV ainsi que celle de tous les organismes étatiques. Ainsi, dans le cadre du système d'information étudié pour ce mémoire, l'ANSSI a mis en œuvre une sonde visant à détecter les attaques les plus répandues. Pour aller plus loin, elle met à disposition des guides de bonnes pratiques explorant de nombreux domaines techniques.

c) Le commandement des forces de cyberdéfense (COMCYBER)

Créé en 2017, il est sous le commandement de l'Etat Major des Armées (EMA). Au même titre que l'ANSSI, il est responsable entre autres de la sécurité des systèmes d'information des armées déployées dans et hors du territoire Français. Ses missions sont les suivantes :

- La protection des systèmes d'information placés sous la responsabilité du chef d'Etat-Major des Armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information ;
- La conduite de la défense des systèmes d'information du ministère des Armées, à l'exclusion de ceux de la Direction Générale de la Sécurité Extérieure (DGSE), de la Direction du Renseignement et de la Sécurité de la Défense (DRSD) ;
- La conception, la planification et la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major " opérations " ;
- La contribution à l'élaboration de la politique des ressources humaines de cyberdéfense ;
- La contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération ;
- La définition des besoins techniques spécifiques de cyberdéfense ;
- La cohérence du modèle de cyberdéfense du ministère et sa coordination générale ;
- Le développement et l'animation de la réserve de cyberdéfense.

Cette organisation mise en œuvre par les armées a pour objectif de répondre aux besoins spécifiques de celle-ci dans le domaine de la cyberdéfense. En effet, les particularités des systèmes militaires (par exemple des systèmes d'arme), les conditions de déploiement particulières, et l'impérieuse nécessité de fonctionner en tout lieu et tout temps, nécessitent une structure spécifique que met en œuvre le

COMCYBER. Comme toute nouvelle organisation, un délai est nécessaire pour atteindre une pleine capacité de moyens. C'est précisément dans ce cadre de montée en puissance que cette étude est menée.

En résumé :

La France se dote depuis la fin des années 2000 d'une stratégie ambitieuse pour répondre aux menaces visant le cyberespace. Elle se donne les moyens humains, matériels et financiers pour atteindre ses objectifs. On constate en parallèle que, malgré tous ces efforts, l'évolution de la menace reste en constante augmentation. Cela s'explique notamment par l'évolution rapide des technologies, l'accroissement exponentiel du cyberespace et, nous l'avons vu précédemment, par une réglementation internationale faillible, ne permettant pas à des agences nationales de protéger à elles-seules les systèmes d'information étatiques.

C. Description du système d'information à protéger

1. La description

Le système d'information à protéger a pour objectif de permettre à un ensemble d'utilisateurs de rechercher des informations sur Internet en toute sécurité et de capitaliser les d'informations collectées dans différents outils tel que des bases de données ou des moteurs de recherche.

Le système d'information actuel est constitué de deux parties :

- Une zone démilitarisée (DMZ) mettant à disposition des services relais. Celle-ci est encadrée par deux pare-feu configurés pour interdire les connexions directes entre le système d'information et Internet, et cela dans les deux sens de communication ;
- Un réseau interne qui regroupe les postes utilisateurs et les serveurs mettant à disposition les services nécessaires à l'accomplissement des missions.

Les serveurs dans la DMZ et les services associés présents sont :

- La navigation Internet au travers d'un serveur mandataire (Proxy) qui autorise l'utilisation des ports 80 (http) et 443 (https).

- Un relai mail qui permet de communiquer avec d'autres organismes de la défense qui utilise seulement le port 25 (SMTP) pour se synchroniser.

- Un serveur dit « métier » qui réunit les services nécessaires au travail collaboratif. On y trouve :

    - Un partage de fichiers accessibles en SFTP
    - Une base de données
    - Une application WEB permettant le travail collaboratif (Confluence)

Dans le cadre de ce mémoire, nous allons nous concentrer sur les flux de données engendrant le plus de risques en matière de sécurité en considérant dans un premier temps les attaques venant de l'extérieur du SI.

Les flux de données légitimes initiés depuis le cyberespace sont ceux :

- Créés par le personnel travaillant en itinérance ;
- Engendrés par les connexions avec des organismes avec lesquels des ressources sont partagées.

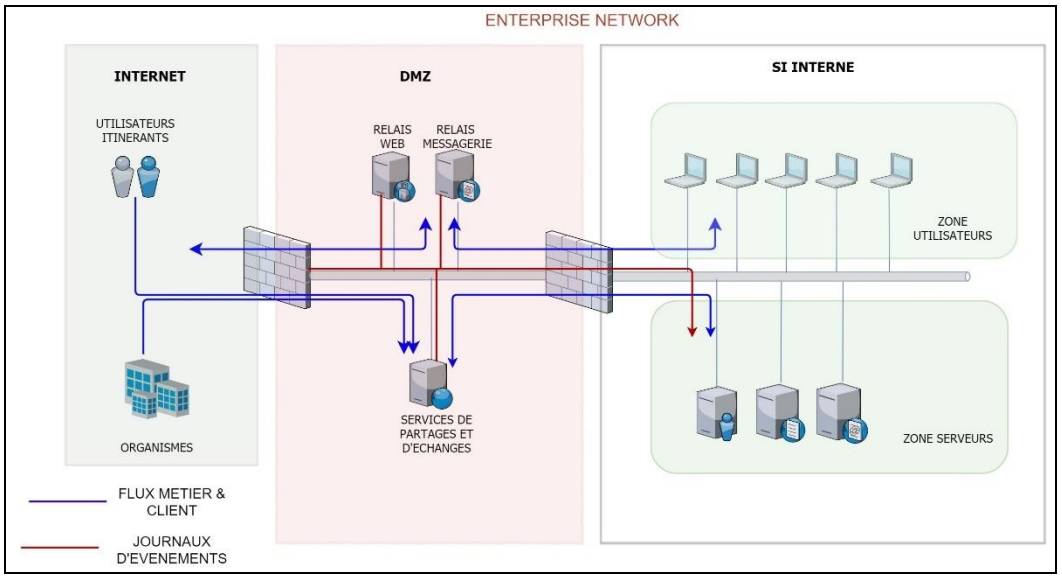

Figure 5 – Système d'information à sécuriser

2. Les vulnérabilités

Les principaux points constituant de potentielles faiblesses de sécurité dans l'architecture du SI sont :

- Elément indispensable pour un SI connecté à Internet, la DMZ n'est pas architecturée selon les bonnes pratiques actuelles et notamment celles définies par les directives de l'ANSSI ;
- Après étude de la nature des clients Internet devant travailler avec des données issues du SI métier, il n'apparait pas pertinent de partager des informations sur un serveur situé au sein même de la DMZ. Cette architecture expose inutilement des services métiers a de potentiels cyberattaquants alors qu'ils ne concernent que des utilisateurs ou des organismes de la défense

clairement identifiés.

- Les moyens d'authentification sur le serveur de partage sont gérés individuellement par les différentes applications et services hébergés. Mis en œuvre par différents administrateurs et implémentés au fur et à mesure des besoins, ils concourent à un déficit de sécurité dans la mesure où aucune stratégie globale n'a été mise en œuvre dans ce domaine. De plus, la plupart se limite à la mise en œuvre d'une authentification par couple identifiant - mot de passe.
- Dans le cadre de la mise en œuvre de mécanismes permettant la détection d'une attaque ou l'analyse a posteriori de celle-ci, il est indispensable de disposer de journaux d'évènements intègres. La façon dont ils sont transmis actuellement ne peut garantir un niveau de confiance suffisant.

En résumé :

Ce SI est le résultat de la somme des besoins exprimés au fur et à mesure de son déploiement et de sa montée en puissance. Le résultat est un amalgame disparate de services qui met en évidence des failles exploitables par des cyber attaquants.

3. Les choix de sécurisation

A la lumière des éléments précédemment décrits dans ce document, il est nécessaire de définir la stratégie visant à sécuriser le système d'information.

Les deux principaux facteurs participant à l'augmentation constante des actions malveillantes dans le cyberespace sont :

- La difficulté des états à se mettre d'accord pour réguler Internet afin de limiter la liberté d'action des groupes malveillants ;
- La mise en œuvre de techniques d'anonymisation par les attaquants.

Rappelons-le, la combinaison de ces deux éléments permet aux attaquants de mener leurs actions en toute impunité. Ainsi, afin de contraindre les assaillants et de limiter leur marge de manœuvre, il est nécessaire de les amener à douter de leur capacité à rester discret.

A cette fin, l'augmentation du niveau de confiance accordé au système d'information constitue un levier non négligeable dans le cadre de la sécurisation de l'infrastructure. Aux vues des faiblesses identifiées dans l'architecture actuelle, les axes d'approche sont les suivants :

- <u>Confiance dans les flux initiés depuis le cyberespace vers le SI</u>

La majorité des attaquants passeront par l'accès Internet pour prendre pied dans le système d'information. Pour limiter le risque, Il est nécessaire d'élever le niveau de confiance dans les flux initiés depuis Internet et autorisés à pénétrer dans le réseau.

- Confiance dans les moyens d'authentification

Avant de donner des droits et des accès à un système ou à un utilisateur, il est nécessaire de passer par une étape d'authentification. Les cyberattaquants tenteront de compromettre ces systèmes pour acquérir des droits leur permettant de commettre leurs méfaits. Il conviendra donc de veiller à mettre en œuvre des moyens garantissant une authentification efficace prouvant l'identité des utilisateurs.

- Confiance dans les journaux d'évènement

Les journaux d'évènement sont utilisés pour détecter une attaque ou pour l'analyser a posteriori. Ce sont donc des mécanismes visés par les pirates informatiques pour effacer leurs traces afin de ne pas être détectés ou identifiés. Dans ce cadre, garantir leur intégrité est primordial afin de conserver un mince espoir d'identifier l'origine d'une attaque.

Nous allons, dans la troisième partie de ce mémoire, définir l'architecture, l'organisation et les technologies nécessaires afin d'augmenter significativement le niveau de confiance dans le Système d'Information.

III. Sécurisation, implémentation et mise en œuvre

A. Confiance dans les moyens d'authentification

Afin de cerner tout l'intérêt des travaux relatifs aux moyens d'authentification à leur amélioration, il est nécessaire d'appréhender ce qu'implique ce concept et comment il est mis en œuvre.

L'authentification est la méthode qui permet à un système informatique de vérifier l'identité d'une personne ou d'un autre système. A la différence de l'identification qui se limite la reconnaissance de l'identité, l'authentification permet de la vérifier. Pour cela, il existe plusieurs facteurs qui permettent d'y parvenir

- Ce que je connais (Mot de passe, code PIN, etc.) ;
- Ce que j'ai (carte à puce, périphérique USB, etc.) ;
- Ce que je suis (biométrie) ;
- Ce que je peux produire (geste, signature, etc.).

Dans le cas de l'utilisation d'un seul facteur pour l'authentification, il s'agit d'une « authentification simple ». Dès que l'on passe à deux ou plus, cela devient une « authentification forte ».

En résumé :

L'authentification est une méthode indispensable pour élever le niveau de confiance dans le SI ; la qualité de son implémentation influencera grandement l'efficacité du SI.

1. Description d'une IGC et de ses composantes

a) Le certificat électronique

Une IGC est un système d'information qui permet notamment de générer des « pièces justificatives » appelées certificats, nécessaires à l'authentification d'utilisateurs ou de systèmes tiers.

Le rôle d'un certificat électronique est de lier une clef de chiffrement publique unique à son propriétaire.

Un certificat comprend à minima et obligatoirement :

- Une clef publique ;
- L'identité du propriétaire ;
- La signature de l'autorité de certification gageant les deux données précédentes.

La mise en forme du fichier contenant un certificat suit la norme X509. Ci-dessous la liste des informations qu'il contient :

- La version du certificat ;
- Le numéro de série ;
- Le nom de l'Autorité de Certification qui l'a validé ;
- Les dates de début et de fin de validité ;
- L'objet de l'utilisation du certificat ;
- Des informations au sujet de la clé publique (algorithme de chiffrement et clé publique proprement dite) ;
- L'identifiant unique du signataire et/ou du détenteur du certificat (en option)
- Les extensions au certificat (en option) ;
- **La signature de l'émetteur du certificat ;**
- **L'algorithme de signature ;**

Lorsqu'il est présenté pour valider une connexion, la procédure de vérification d'un certificat est la suivante :

- Vérification de la signature de l'autorité de certification ;
- Vérification de la date de validité ;
- Vérification que l'usage est conforme à la certification ;
- Vérification que le certificat n'est pas révoqué.

Elément indispensable à la mise en œuvre d'un SI de confiance, les certificats sont généralement associés à une IGC qui permet de les concevoir, de les distribuer et de les utiliser.

b) L'Infrastructure de Gestion de Clés

Une Infrastructure de gestion de clés est utilisée pour gérer des certificats numériques X509. Elles ont deux principaux objectifs :

- Etablir un environnement de confiance entre deux entités ayant besoin de communiquer ensemble
- Créer un lien personne/organisme avec une ou plusieurs clefs de chiffrement

Pour cela, une IGC permet de mettre en œuvre plusieurs services :

- Enregistrement des utilisateurs ;
- Vérification des attributs (propriétés des utilisateurs) ;
- Génération des certificats ;
- Publication des certificats valides et révoqués ;

- Identification et authentification des utilisateurs ;
- Archivage.

Enfin, l'IGC est composée des éléments de base suivants :

- Autorité de certification ;
- Autorité d'enregistrement ;
- Service de publication ou autorité de validation ;
- Annuaire contenant les clefs publiques, les certificats distribués ainsi que les listes de certificats révoqués.

Une IGC est donc un outil qui permet d'augmenter la sécurité du SI par l'utilisation de mécanismes complémentaires de l'identification tels que l'authentification forte, la signature électronique et le chiffrement de données.

c) En quoi l'IGC répond à ma problématique ?

La gestion actuelle des secrets dans le SI étudié est actuellement décentralisée et hétérogène :

- Décentralisée : chaque service gère de façon autonome sa fonction d'authentification ;
- Hétérogène : les authentifications sont possibles soit par clé, soit par mot de passe.

Le rôle intrinsèque d'une IGC est de créer de la confiance entre les utilisateurs et les services mis à disposition mais également de centraliser la gestion des certificats utilisés pour l'authentification tout en simplifiant leur gestion par les administrateurs.

En résumé :

En permettant de centraliser les méthodes d'authentification et en utilisant des mécanismes de chiffrement, l'intégration d'une IGC devient un élément indispensable pour atteindre l'objectif d'une augmentation du niveau de confiance dans le SI.

2. Choix d'une Infrastructure de Gestion de Clés, intégration et bonnes pratiques

a) Analyse comparative des différentes solutions d'IGC

Il est important de souligner que la mise en œuvre d'une IGC peut être complexe et chronophage. De plus, pour un cyber attaquant, cette infrastructure sera une cible prioritaire. Il faut donc garantir un maintien en condition opérationnelle de grande qualité pour en assurer la sécurité.

Afin de sélectionner le logiciel à déployer, trois contraintes propres à la structure étudiée doivent être prises en compte dans cette étude :

- La solution logicielle étudiée doit être développée nativement sur Debian afin d'éviter tout effet de bord non prévisible et faciliter le travail des administrateurs (formés sur ce système d'exploitation)
- Le logiciel doit être Open Source pour garantir que le code puisse être « vérifié » à chaque mise à jour. Ce travail colossal est effectué par une communauté attachée à la sécurité. Les utilisateurs en bénéficient donc naturellement.
- Dans le cadre de projets open source, il est indispensable de vérifier que ceux-ci sont suivis par une équipe professionnelle. Cela permet de garantir la mise à disposition de correctifs en cas de découverte de failles de sécurité ainsi qu'une évolution du produit dans le temps.

	EJBCA	XCA	EASY-RSA	OPENXPKI
Natif Debian 10				
Open source				
Suivie du projet				

Tableau 2 – Tableau comparatif entre différentes solutions d'IGC

Choix technique :

Comme nous pouvons le constater sur ce tableau, EASY-RSA et OPENXPKI répondent aux contraintes de sélection. EASY-RSA est sélectionné en raison de sa simplicité et son abondante documentation.

b) Position de l'IGC dans le SI étudié

Afin de limiter les coûts, les différents composants de l'IGC (hors AC[19]) sont installés sur le même serveur qui sera lui-même situé dans la zone serveur du réseau interne. Dans le futur, quand cette infrastructure sera bien maitrisée par les administrateurs,

[19] Autorité de certification

les différents rôles devront être séparés pour plus de sécurité et redondés pour davantage de disponibilité. En ce qui concerne l'AC, et afin de protéger la clef privée utilisée pour signer les certificats, elle sera installée hors ligne. Dans un premier temps, les certificats seront utilisés pour l'authentification. Dans ce cadre, le processus de mise à disposition d'un certificat sera le suivant :

- Expression d'un nouveau besoin auprès de l'équipe d'administration ;
- Génération de la demande XXX ;
- Génération du couple de clés (Privée/publique) ;
- Génération du certificat et signature de celui-ci par l'AC ;
- Fourniture du certificat au client ;

c) Préconisation pour la création des clés

Dans le cadre de la mise œuvre de l'IGC, la cryptographie mise en œuvre sera asymétrique (fonctionnement basé sur un couple de clés publique/privée). Afin de ne pas affaiblir les moyens cryptographiques, il est primordial de générer correctement les clés. Comme énoncé dans l'un des principes de Kerckhoff[20], « la sécurité résultant de l'utilisation d'un crypto système ne doit pas reposer sur le secret de ses principes de conception ou du paramétrage du dispositif ». Il suggère ainsi que la sécurité doit uniquement reposer sur une clé secrète. L'ANSSI, référent national dans le domaine de la cyber protection, met à disposition des préconisations précises sur la taille des clés à utiliser en fonction de l'algorithme de chiffrement, RSA dans notre cas :

> *RègleFact-1. La taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2030.*
>
> *RègleFact-2. Pour une utilisation au-delà de 2030, la taille minimale du module est de 3072 bits.*

Choix technique :

Afin de ne pas trop alourdir le processus cryptographique et étant encore assez éloigné de l'échéance de 2030, il sera utilisé une longueur de clé de 2048 bits.

Pour générer des clés dans de bonnes conditions, le système doit disposer d'un Générateur de Nombres Pseudo Aléatoires GNPA[21] de qualité. Dans les systèmes Debian, l'entropie utilisée par le GNPA (/dev/uramdom) se base sur de nombreux paramètres (Input/Output, utilisation des disques durs, frappes clavier, déplacement

[20] Aug. Kerckhoffs. (1883, Février). JOURNAL DES SCIENCES MILITAIRES ; LA CRYPTOGRAPHIE MILITAIRE. Récupéré sur https://www.petitcolas.net/kerckhoffs/la_cryptographie_militaire_ii.htm

[21] Aussi appelé pseudorandom number generator (PRNG) en anglais.

de la souris, instruction RDRAND des processeurs Intel, etc.). Ce GNPA est actuellement considéré comme fiable. Il faut cependant rester vigilant sur les éventuelles faiblesses intégrées par erreur dans une mise à jour comme cela a été le cas en 2006 sur les systèmes Debian et détectée seulement en 2008.

B. Confiance dans les flux

Pour protéger un système d'information connecté sur Internet, il est nécessaire de travailler sur la partie du réseau qui gère l'interconnexion. Elle est la plus exposée et c'est par elle que les cyber-attaquants vont commencer leurs travaux de pénétration. Dans ce cadre, nous allons nous concentrer sur « la porte d'entrée » du réseau, c'est-à-dire la DMZ et sur les moyens permettant de contrôler au mieux les flux entrant en garantissant un bon niveau de confiance.

1. DMZ dédiée par sens de flux

Actuellement la DMZ gère les flux de données entrant et sortant. Dans cette configuration, le pare-feu connecté sur la partie publique est configuré afin de d'accepter des connexions initialisées depuis internet et depuis la DMZ. Dans le cadre d'une attaque informatique, cette architecture facilite le travail du cyberattaquant qui peut utiliser les ports autorisés pour pénétrer le réseau et éventuellement exfiltrer des données.

Afin de limiter la liberté d'action des groupes malveillants et simplifier la gestion des flux, une solution consiste à mettre en œuvre deux DMZ :

- Une pour les flux entrants
- Une pour les flux sortants

Cette architecture apporte les avantages suivants :

- Une difficulté supplémentaire pour l'attaquant ;
- Une simplification des configurations des pare-feu ;
- Une simplification de la supervision.

L'architecture envisagée est la suivante :

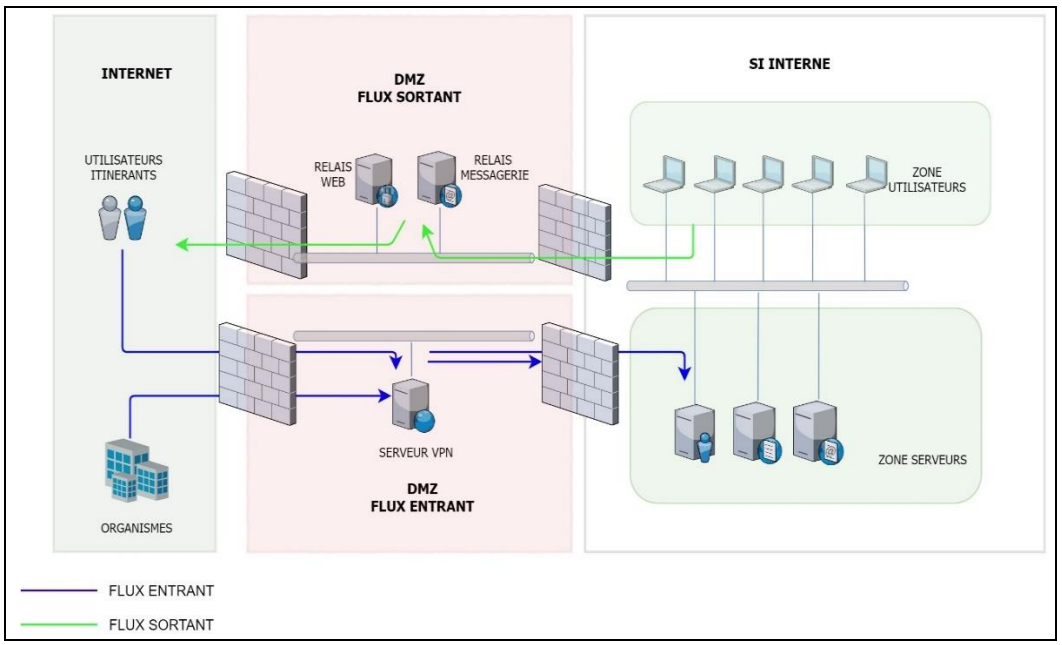

Figure 6 – Passage à deux DMZ avec représentation des flux réseaux associés

2. Description et choix du Réseau Privé Virtuel

a) Description du RPV

Le RVP (Réseau Privé Virtuel) ou VPN (Virtual Private Network) est une technologie permettant de connecter directement deux ordinateurs ou systèmes d'information au travers de réseaux qui permettent le routage mais qui ne sont pas forcément maitrisés. Peu employé dans le modèle initial d'internet, leur avènement est la réponse logique à l'accroissement des besoins en confidentialité et intégrité des données.

Exemple de mise en œuvre :

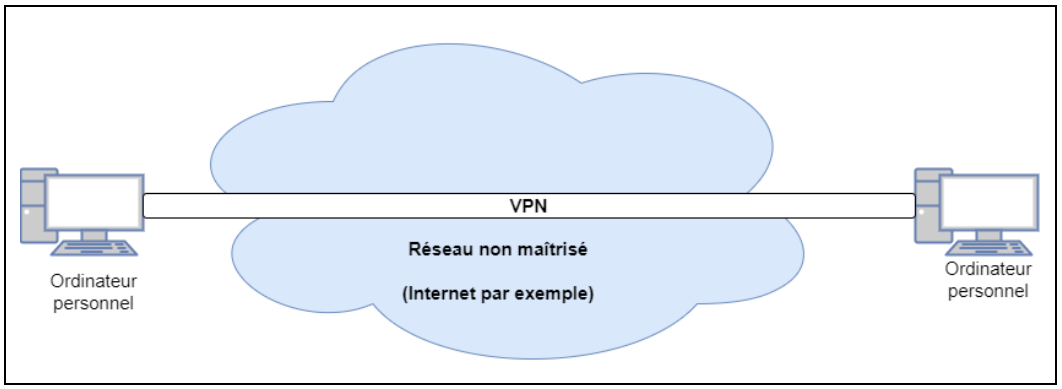

Figure 7 – VPN entre deux postes distants

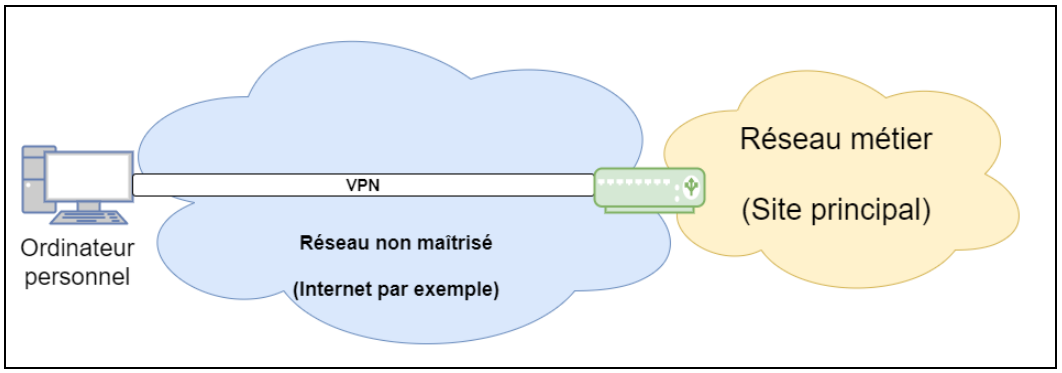

Figure 8 – VPN entre un poste nomade et un site

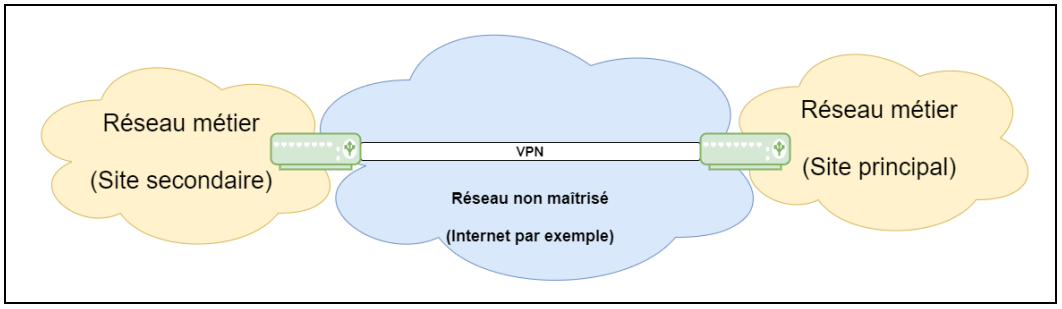

Figure 9 – VPN entre deux sites distants

b) En quoi un VPN répond à notre problématique ?

Comme nous l'avons abordé dans la première partie, les états, et tout particulièrement le domaine de la défense, font partie des cibles les plus régulièrement visées par les cyberattaquants. Dans ce cadre, il est indispensable de sécuriser les échanges en provenance d'Internet. Le VPN est donc la clef de voute en vue d'augmenter le niveau de confiance dans le SI pour les raisons suivantes :

- Les communications transitant par le VPN sont chiffrées, garantissant ainsi leur confidentialité. Ceci permet de se protéger dans la phase de ciblage préalable à l'attaque ainsi que contre les actions d'espionnage par interception des flux.

- Un VPN peut intégrer des protocoles garantissant l'intégrité de la transmission. Cette propriété peut entre-autres protéger le système d'information des attaques de type « man in the middle »

- La phase d'authentification obligatoire au montage du VPN permet de garantir la légitimité de la connexion.

Ainsi, l'ensemble de ces services augmente la confiance dans les échanges de données, contribuant à atteindre l'objectif fixé.

c) Comparaison de technologie VPN

Afin de pouvoir définir au mieux les technologies VPN envisageables, il nous faut lister les objectifs et les contraintes à prendre en compte :

- Connecter des clients nomades du le réseau métier ;
- Interconnecter des sites distants ;
- Garantir l'intégrité, la confidentialité et la non-répudiation de la connexion ;
- Intégrer le concentrateur VPN sur un serveur avec un système d'exploitation linux.

Tableau comparatif de solutions existantes :

	PPTP	L2TP	IPSEC	SSL/TLS	IP MPLS	SD WAN	DMVPN
Lien Nomade vers site							
Lien inter-sites							
Confidentialité							
Intégrité							
Non répudiation							
Déploiement autonome sur serveur LINUX							

Tableau 3 – Tableau comparatif entre différentes solutions de VPN

Une analyse rapide du tableau met en avant 2 technologies qui répondent à l'ensemble des critères de sélection IPSEC et SSL/TLS.

d) Pourquoi IPSEC

L'objectif de la mise en œuvre d'une technologie VPN est d'augmenter le niveau de confiance du système d'information. IPSEC et SSL/TLS sont à ce jour les deux technologies les plus utilisées dans le cadre de la mise en œuvre de VPN. Notre choix se portera cependant sur IPSEC qui semble plus mature et sécurisé pour les raisons suivantes :

- Les opérations de sécurité sont exécutées dans un environnement contrôlé (noyau du système d'exploitation). TLS pour sa part lance ces mêmes actions

dans l'environnement utilisateur beaucoup plus susceptible d'être la cible d'une action malveillante ;

- Les différentes fonctions de sécurité sont conçues et implémentées de façon plus robuste ;
- La gestion des éléments d'authentification est plus permissive par défaut dans TLS ;
- La mauvaise implémentation de TLS par des applications qui le mettent en œuvre en fait la cible de nombreuses attaques (Heartbleed, Crime, Freak, etc.).

e) Intégration de l'IGC pour gestion des certificats IPSEC

L'IGC prévu précédemment sera utilisée pour produire les certificats nécessaires à la mise en œuvre d'IPSEC.

Les éléments nécessaires à l'authentification sont les suivants :

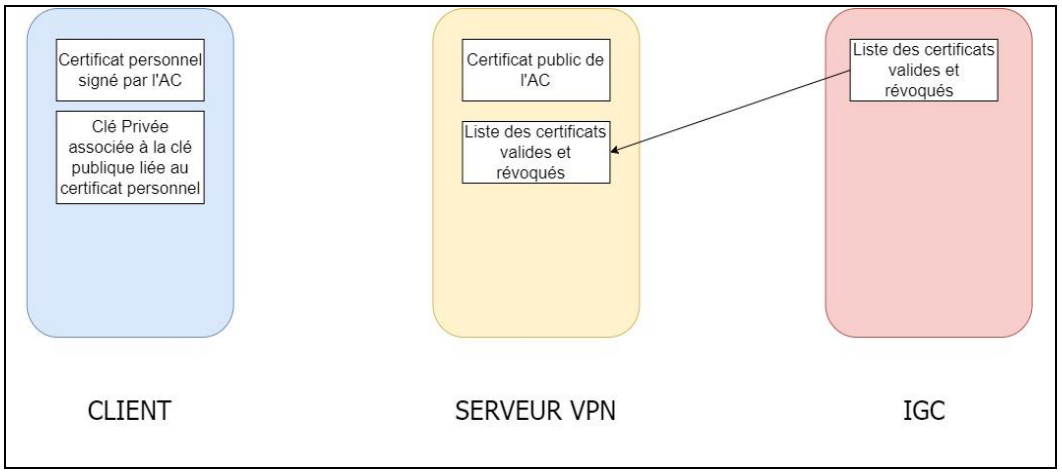

Figure 10 – Répartition des éléments issus de l'IGC nécessaires à l'authentification

Dans un premier temps, la liste des certificats valides et ceux révoqués sera mise à jour manuellement sur le serveur VPN. L'objectif est de limiter les flux autorisés entre la DMZ et le réseau Interne au minimum nécessaire (cf figure 5). Il sera envisageable dans un avenir proche de déporter dans la DMZ « entrante » un relai permettant de mettre à jour automatiquement sur le serveur VPN la liste des certificats. Cela permettra d'alléger le travail des administrateurs tout en garantissant un meilleur niveau de sécurité.

Maintenant que l'emplacement des éléments d'authentification est connu, voyons quel est son cycle d'utilisation dans le cadre du montage du tunnel IPSEC :

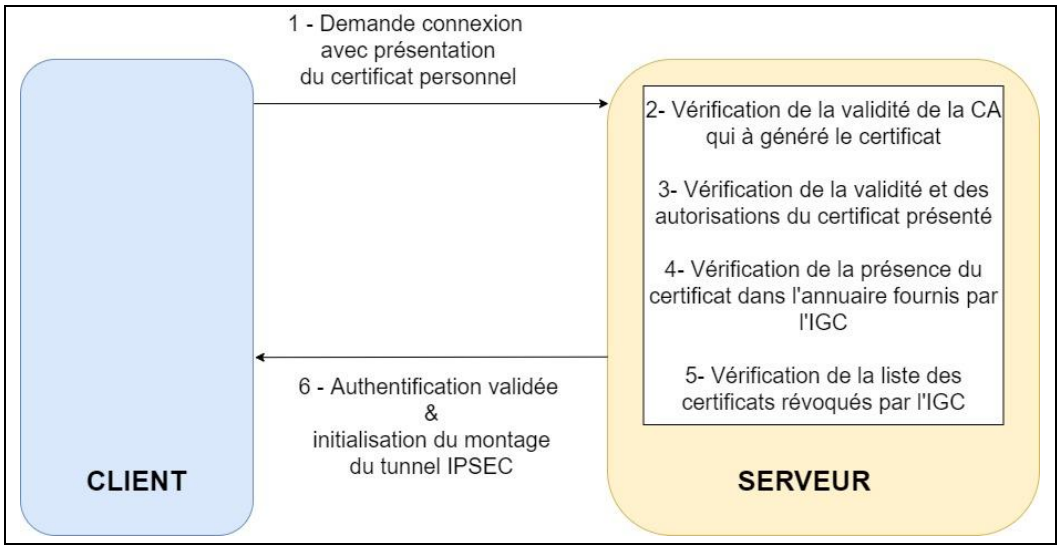

Figure 11 – Processus d'authentification avec certificats

En intégrant l'IGC dans le processus d'authentification d'IPSEC, le niveau de confiance augmente significativement. Dans l'avenir il sera nécessaire de l'étendre à d'autres services afin de rendre cohérente la politique de sécurité et ainsi encore améliorer la sécurité du système d'information.

3. Mise en œuvre d'IPSEC

IPSEC est une technologie VPN permettant une grande souplesse d'emploi en raison de sa maturité et des possibilités d'adaptation qu'il met à disposition.

a) Choix du protocole

IPSEC peut être mis en œuvre avec deux protocoles différents :

- AH « Authentication Header »

AH permet de garantir l'intégrité et l'authentification des paquets. Il met en œuvre des mécanismes de vérification de la trame IP en dehors de ceux déjà implémentés dans le protocole IP (TTL[22] par exemple). Ainsi, un paquet dans lequel des données ont été modifiées est considéré comme corrompu. Ce mécanisme créé parfois une incompatibilité avec les mécanismes de traduction d'adresses.

[22] Time to Live : Le TTL est une donnée placée au niveau de l'en-tête du paquet IP qui indique le nombre maximal de routeurs de transit.

- ESP « Encapsulation Security Payload »

ESP permet de garantir l'intégrité, l'authentification et la confidentialité des paquets. Pour garantir la confidentialité, il met en œuvre le protocole IKE qui sera abordé ultérieurement dans ce document. A la différence de AH, ESP protège uniquement le « payload », c'est à dire le contenu du paquet IP et non ses en-têtes. Il n'est donc pas incompatible avec les mécanismes de traduction d'adresse mais sa configuration et son déploiement sont plus complexes.

Choix technique :

L'emploi d'IPSEC se fera avec le protocole ESP qui permet de garantir la confidentialité et l'intégrité des informations. Le protocole ESP permet éventuellement de désactiver le contrôle d'intégrité pour gagner en performance, cependant la plupart des recommandations existantes déconseillent de le désactiver.

b) Le mode d'utilisation

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IPSEC dans deux modes distincts :

- Le mode transport :

Dans le mode transport, les données associées à ESP viennent s'ajouter sur le paquet IP initial (c'est à dire celui qui aurait été envoyé en l'absence d'IPSEC).

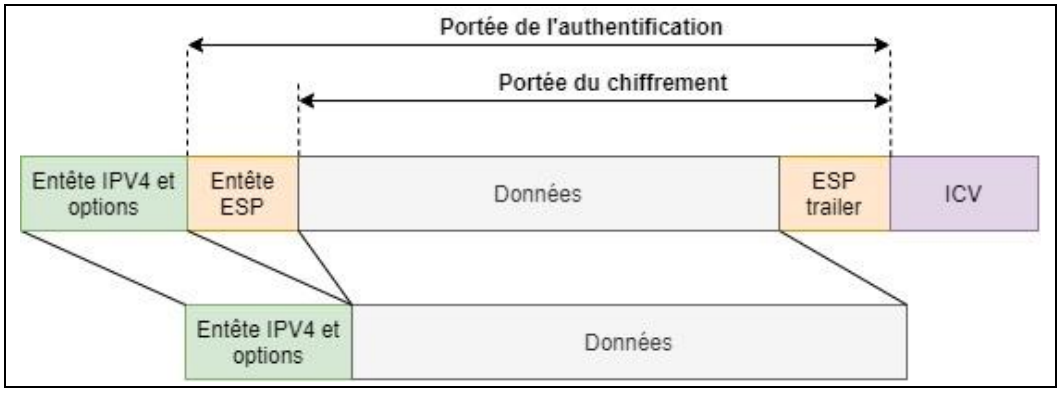

Figure 12 – Représentation de la trame IPSEC en mode transport

Dans l'utilisation d'ESP en mode transport, ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité.

- Le mode tunnel :

Dans le mode tunnel, un nouveau paquet IP est généré pour contenir un paquet ESP, lui-même contenant les paquets IP initiaux sans modification. Le paquet contient alors deux entêtes IP. La première « externe » est utilisée dès son émission pour le routage en « zone publique », la seconde sera traitée de façon confidentielle par le destinataire.

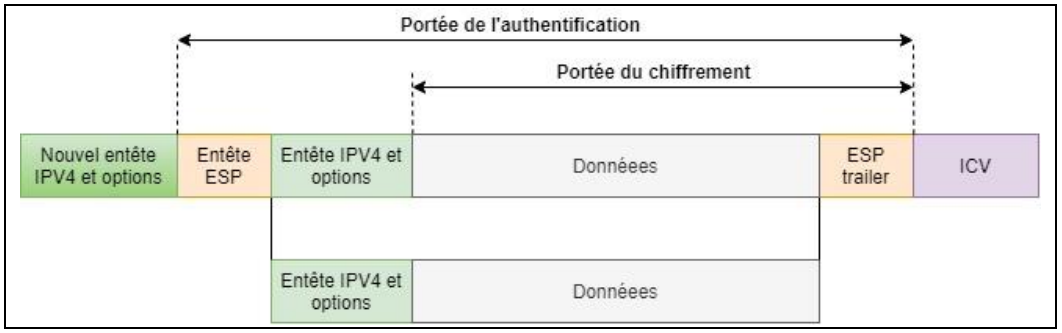

Figure 13 – Représentation de la trame IPSEC en mode tunnel

Dans l'utilisation d'ESP en mode tunnel, ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité.

Choix technique :

Le mode tunnel est parfaitement adapté à un accès distant sur un réseau privé. En effet, il masque les adresses IP internes qui sont la plupart du temps non routables au travers du réseau public.

c) Les « Security Policy »

Les Security Policy (SP) sont des fichiers de paramétrage des services IPSEC qui regroupent les informations nécessaires à la configuration d'un lien unidirectionnel donné. On y retrouve les informations suivantes :

– l'utilisation obligatoire ou facultative ou de la non-utilisation d'IPsec ;
– le mode utilisé, tunnel ou transport ;
– le choix du protocole AH ou d'ESP.

L'ensemble des SP sont regroupés dans une SPD : « Security Policy Database ». À l'image des règles de flux d'un pare-feu, les SP ont pour but de spécifier les flux que l'on veut autoriser et ceux que l'on veut interdire.

Choix technique :

- Les Security Policy peuvent permettre un usage facultatif ou optionnel d'IPSEC qu'il faut éviter d'implémenter. Ces fonctionnalités donnent l'opportunité aux cyber attaquants de baisser le niveau de sécurité pour obtenir des opportunités.

- Malgré la possibilité technique de fonctionnement asymétrique, on préfèrera lorsque c'est possible avoir une politique uniforme entre le lien aller et le lien retour.

d) Les « Security Association »

Chaque lien unidirectionnel dispose d'une « Security Association » (SA), elle contient les données de contexte telles que :

– les hôtes source et destination ;
– le mode (transport/tunnel) et les protocoles (AH/ESP) employés ;
– les algorithmes cryptographiques employés ;
– les clés associées à ces algorithmes.

Les premiers éléments (hôtes aux extrémités, mode, protocole) sont conditionnés par les SP en vigueur : un système ne doit pas avoir de SA qui violent ses SP.

Choix technique :

Afin de limiter les opportunités offertes aux cyber attaquants, les algorithmes et les tailles de clés employés doivent être spécifiés dans la SA.

e) La gestion des secrets

IPSEC donne la possibilité de gérer les clefs de chiffrement de deux façons différentes :

Mise à la clé manuelle : Les algorithmes et les clés peuvent être paramétrés manuellement. Fortement déconseillée, cette méthode exige en effet une configuration fastidieuse, la clé étant idéalement différente pour chaque couple d'hôtes. De plus, dans cette utilisation, il devient très compliqué de renouveler les clés à un rythme compatible avec les bonnes pratiques cryptographiques.

Utilisation du protocole IKE : La négociation dynamique des algorithmes et clés d'une SA peuvent se faire grâce au protocole IKE, actuellement utilisable dans sa version 2

Choix technique :

Pour simplifier la mise en œuvre des bonnes pratiques en matière de Sécurité des Systèmes d'Information (SSI) et dans le domaine cryptographique, l'utilisation du protocole IKE a été retenue. Conformément aux préconisations de l'ANSSI, l'utilisation du protocole IKE[23] sera limitée à l'échange de clés.

f) Le protocole IKE :

Le protocole IKE intervient dans les échanges de secrets nécessaires à l'établissement du lien sécurisé. Pour cela, le protocole fonctionne en deux phases. La première utilise des algorithmes cryptographiques qui ne sont pas nécessairement les mêmes que ceux définis dans la SA. Les paramètres du canal sécurisé négocié lors de la première phase sont parfois désignés sous le terme ISAKMP SA ou encore IKE SA. Ils sont utilisés pour protéger la seconde phase dont les paramètres sont appelés IPSEC SA qui sont les SA négociés lors de la seconde phase et utilisés pour protéger le trafic « utile ».

Authentification des correspondants :

L'authentification lors de la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pre-Shared Key ») soit par utilisation d'un chiffrement asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes.

Choix technique :

Afin de garantir un haut niveau de sécurité, l'authentification sera réalisée à l'aide de d'un mécanisme de cryptographie asymétrique. De plus, une Infrastructure de Gestion de Clés (IGC ou PKI) sera déployée pour améliorer l'authentification.

Négociation des SP :

Le protocole IKE permet aussi de négocier les SP. Ce mécanisme, la plupart du temps inutile dans les liens inter-sites, prend toutefois tout son sens dans les situations de mobilité. Dans ce cas, en effet, l'adresse IP du client nomade n'est pas connue. Il est alors très utile de pouvoir adapter ce paramètre de la SP à la volée au moyen de la négociation IKE.

[23] Internet Key Exchange.

Choix technique :

Dans le cas des liens inter sites dont les IP ne varient pas, les SP seront gérées de façon statique. Pour les postes nomades, dont les IP peuvent changer, une négociation des SP au travers d'IKE sera autorisée.

g) Compatibilité avec la technologie NAT[24]

L'utilisation du protocole ESP offre une compatibilité avec les technologies de transfert d'adresse. Il faudra pour cela activer le mécanisme de NAT-Traversal.

C. Confiance dans les journaux d'évènement

Les journaux d'évènements sont une brique indispensable dans la construction de la cyberdéfense d'un système d'information. Seul « témoin » objectif des actions qui sont menées sur le réseau ou dans les systèmes, ils sont utilisés pour atteindre trois objectifs :

Premièrement, pour la capitalisation et la détection des attaques, les LOG[25] sont tous envoyés vers un point unique afin d'être analysés. Ceci afin de disposer d'une « vision » globale du système d'information à protéger. Les outils qui les exploitent dans cet objectif sont fréquemment appelés des SIEM[26].

Deuxièmement, dans le cadre d'une détection d'attaque, les journaux d'évènement étant rassemblés et analysés permettront de mieux contrer l'adversaire ou de comprendre ses motivations.

Troisièmement, les journaux d'évènement sont étudiés a posteriori d'une action malveillante pour identifier au mieux les systèmes compromis et la tactique mise en œuvre par les cybers attaquants.

Tous les journaux d'évènement doivent être stockés dans une zone sûre du système d'information.

Ne seront traités dans ce mémoire que les LOG issus des serveurs présents dans la DMZ « flux entrant ».

[24] network address translation
[25] Diminutif de « logging » qui signifie journaux d'évènement
[26] Security Information and Event Management ou Gestion de l'information et des événements de sécurité

1. Sécurisation à la génération

a) Pourquoi sécuriser à la génération

Les journaux d'évènement sont la première cible lors d'une attaque informatique pour deux principales raisons :

- Les groupes malveillants corrompent ou suppriment les journaux d'évènement afin de masquer leur présence ou simplement afin de ne pas laisser de trace permettant d'identifier leurs actions ;

- Les journaux d'évènement peuvent servir de sources de renseignements aux hackers afin de cartographier le réseau plus rapidement.

Dans ce cadre, il faut pouvoir utiliser en toute confiance les journaux d'évènement à des fins de cyberdéfense. La première étape consiste donc à garantir, au plus tôt, leur intégrité et leur confidentialité.

b) Les moyen mis en œuvre

Pour atteindre cet objectif, il faut implémenter deux mécanismes complémentaires.

Le premier consiste à intercepter les journaux d'évènement générés dans notre cas par RSYSLOG avant qu'ils ne sortent du serveur. Pour cela il est possible d'utiliser une fonction d'IPTABLES (utilitaire contenu dans le framework NETFILTER), NFQUEUE. Le second consiste à mettre en œuvre des mécanismes permettant de garantir la confidentialité et l'intégrité des journaux d'évènement.

(1) Interception des journaux d'évènement

NETFILTER dispose d'une option appelée NFQUEUE. Celle-ci permet de récupérer des paquets (en entrée ou en sortie) et de les envoyer dans une file d'attente. Depuis celle-ci, il est possible de filtrer ou modifier les paquets à l'aide d'un programme lancé dans l'environnement utilisateur.

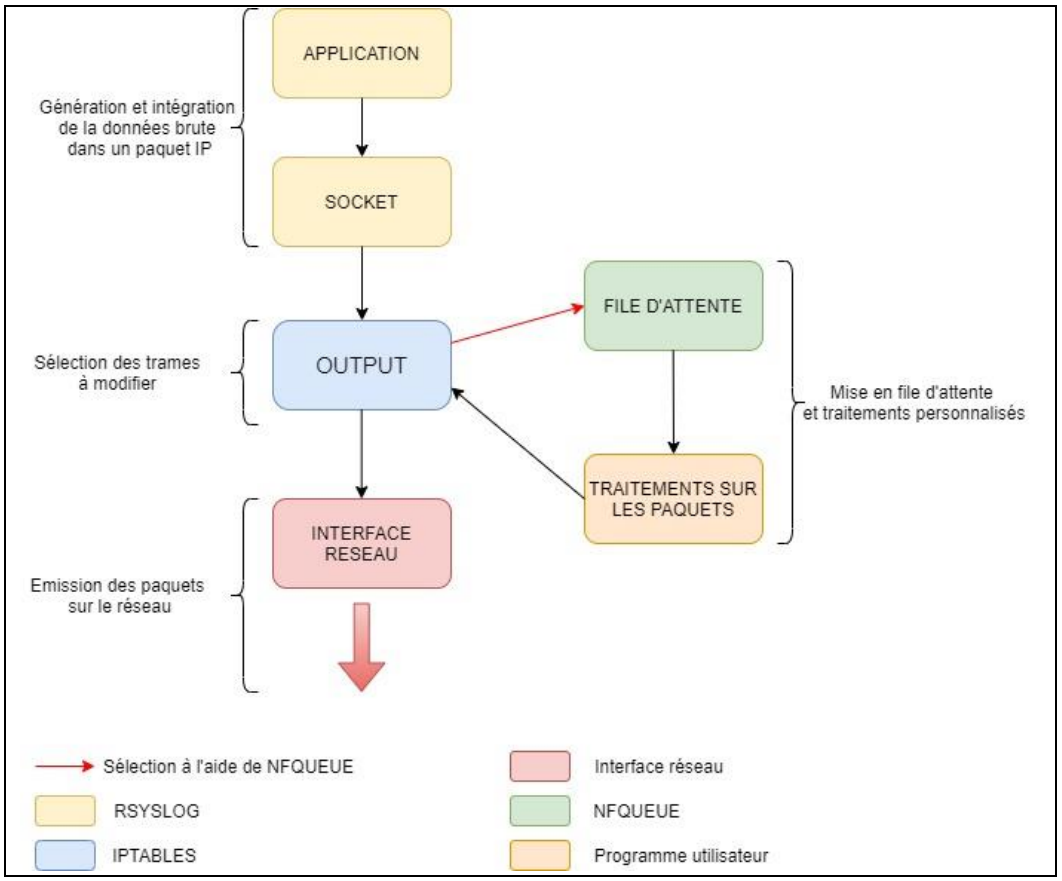

Figure 14 – Cheminement du LOG entre la génération et l'émission sur le réseau

La commande à passer dans IPTABLES pour récupérer les paquets émis par RSYSLOG afin de l'envoyer dans une file d'attente est la suivante :

```
# iptables -I OUTPUT -p udp --dport 514 -j NFQUEUE --queue-num 1
```

(2) Protection des journaux d'évènement

Afin de garantir la confiance dans les journaux d'évènement, il est indispensable d'assurer la confidentialité et l'intégrité. Pour cela, un chiffrement et un contrôle d'intégrité vont être appliqués aux messages afin d'atteindre l'objectif de confidentialité et de garantir l'intégrité.

C'est lors du passage dans la file d'attente NFQUEUE abordée précédemment que la trame va être chiffrée et qu'un CRC va être utilisé. Ci-après le processus de modification du paquet IP de l'émission à la réception.

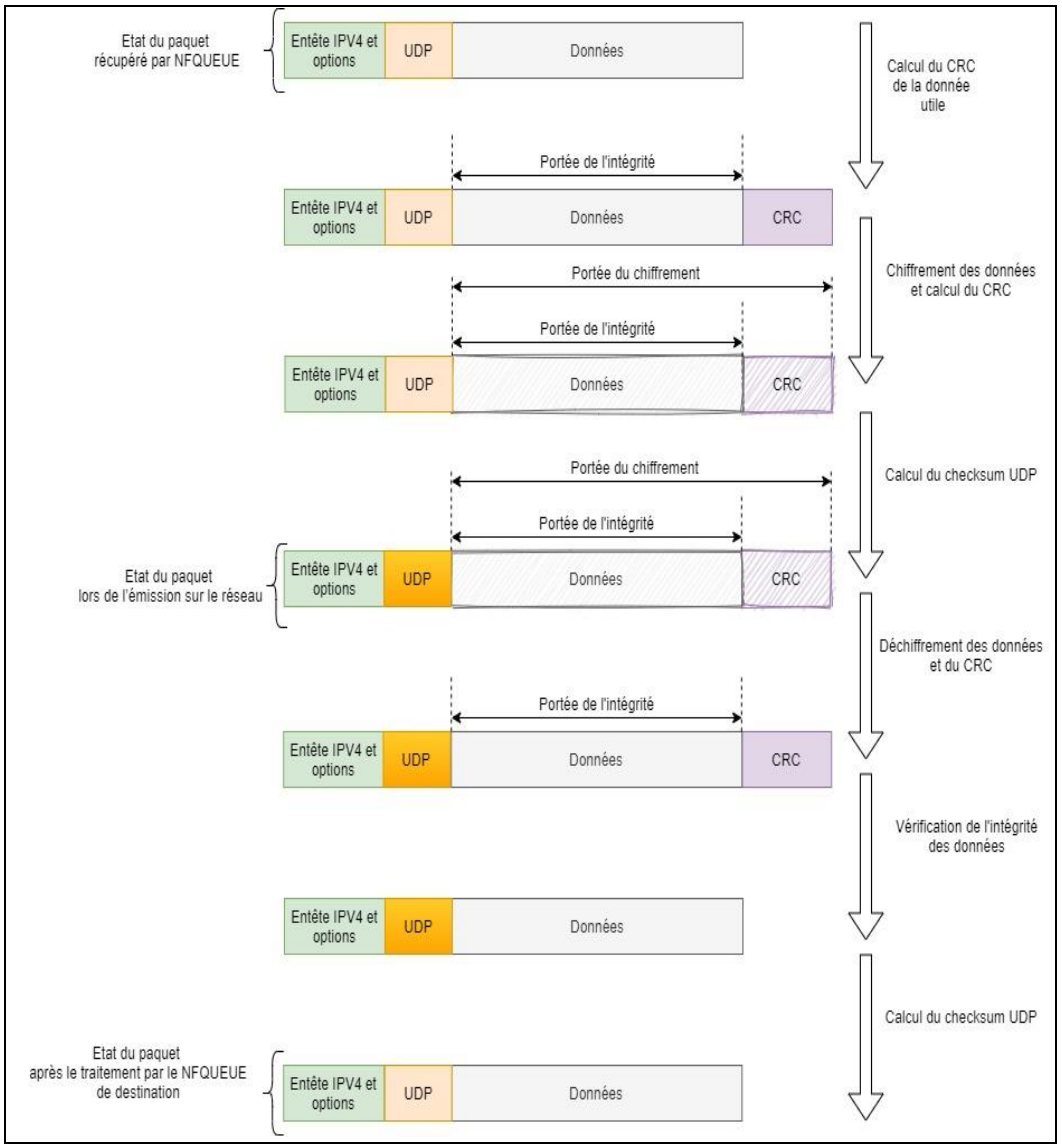

Figure 15 – traitement de la trame IP pour garantir la confidentialité et l'intégrité

Le binaire nécessaire à la mise en œuvre de ces actions n'a pas pu être terminé durant la rédaction du mémoire et sera terminé ultérieurement.

2. Sécurisation au transfert

Comme cela a été évoqué, il est nécessaire d'envoyer les journaux d'évènement vers un environnement sécurisé afin d'y être exploités. La difficulté va consister à passer une somme conséquente de données de la DMZ vers le réseau métier sans pour autant créer de failles de sécurité. Pour cela, il est nécessaire de mettre en œuvre un moyen technique garantissant de ne pas pouvoir extraire de données issues du réseau interne.

(1) Le transfert unidirectionnel

Pour garantir le transfert d'informations de la zone à risque (La DMZ) vers la zone sensible (le réseau métier), il est possible d'utiliser des moyens de transfert unidirectionnels physiques et asynchrones communément appelés « diodes optiques ». Ces systèmes garantissent par leur construction physique l'impossibilité d'établir une communication bidirectionnelle entre deux réseaux.

Le schéma du modèle présenté lors du Symposium sur la sécurité des Technologies de l'Information et des Communications en 2016[27] (SSTIC) est révélateur du mode de fonctionnement :

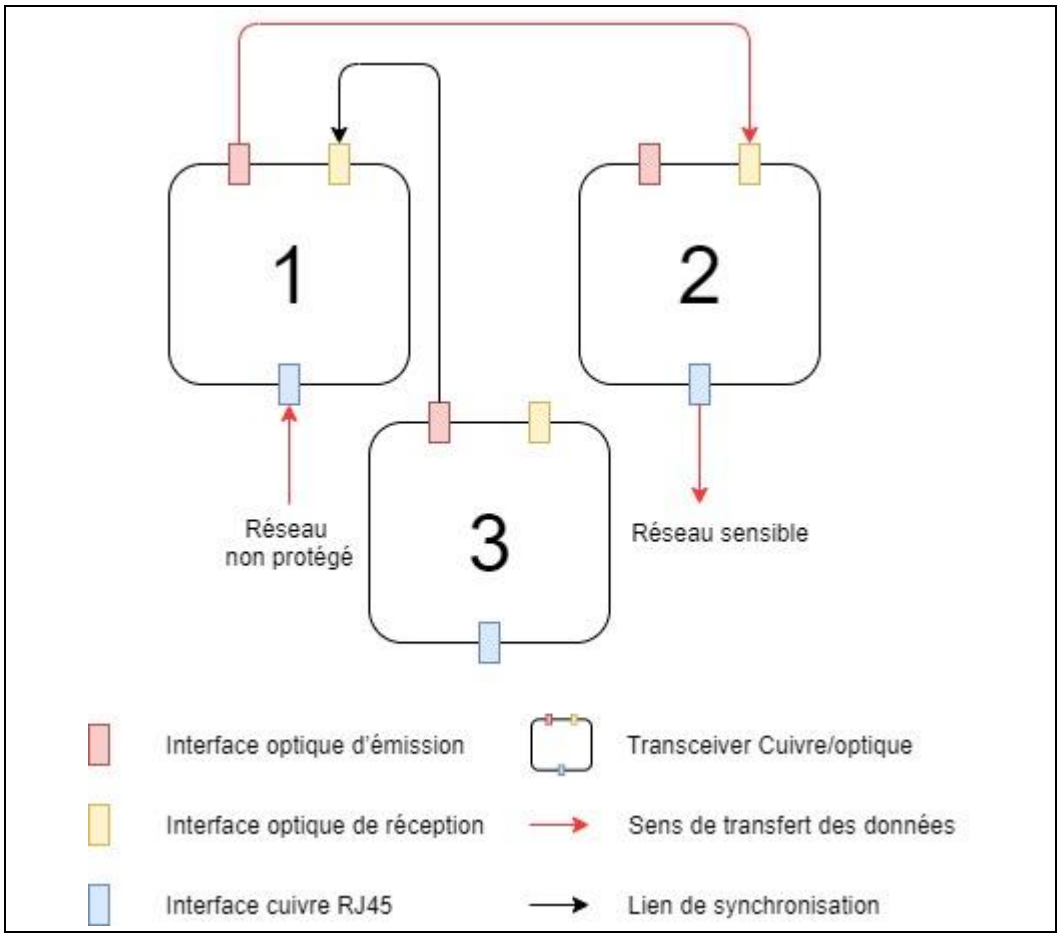

Figure 16 – Représentation d'un système de diode optique à base de transceivers Fibre Optique/Cuivre

[27] https://static.sstic.org/videos2016/SSTIC_2016-06-02_P10.mp4

Transceiver 1 : Il reçoit les données du réseau non protégé sur son interface cuivre et les renvoie via son interface fibre optique d'émission vers le transceiver 2.

Transceiver 2 : Il reçoit les données du transceiver 1 sur son interface fibre optique de réception et les renvoie vers le réseau sensible via son interface cuivre. **Son interface fibre optique d'émission n'est pas connecté**.

Transceiver 3 : Il n'est connecté à aucun réseau, son interface fibre d'émission est connecté sur la réception du Transceiver 1. Cela est indispensable pour gérer la synchronisation et simuler un lien « UP ».

Avec ce type d'architecture à base de transceivers optiques, (convertisseur optique / RJ45) on constate qu'il est physiquement impossible de faire passer des données de la zone sensible à la zone non protégée.

Des industriels ont développé des solutions à base de prisme optique permettant d'obtenir un format compact et de ne pas utiliser d'alimentation électrique. Au ministère des armées, la solution préconisée pour ce type de liaison est fabriquée par la société THALES sous la dénomination ELIPS-SD.

Figure 17 – Diode THALES ELIPS-SD

(2) Intégration dans le réseau

Pour limiter la mise en œuvre des diodes réseau au strict nécessaire, tous les journaux d'évènement d'une DMZ sont envoyés vers un serveur unique « Relais LOG ». Il est le seul à être connecté au réseau interne via la diode optique. Tous les journaux d'évènement sont ensuite réceptionnés sur un serveur présent dans le réseau métier qui a pour fonction de les déchiffrer et d'en vérifier l'intégrité. Dès qu'ils sont considérés comme intègres, les LOG sont stockés et éventuellement mis à disposition d'applications tierces.

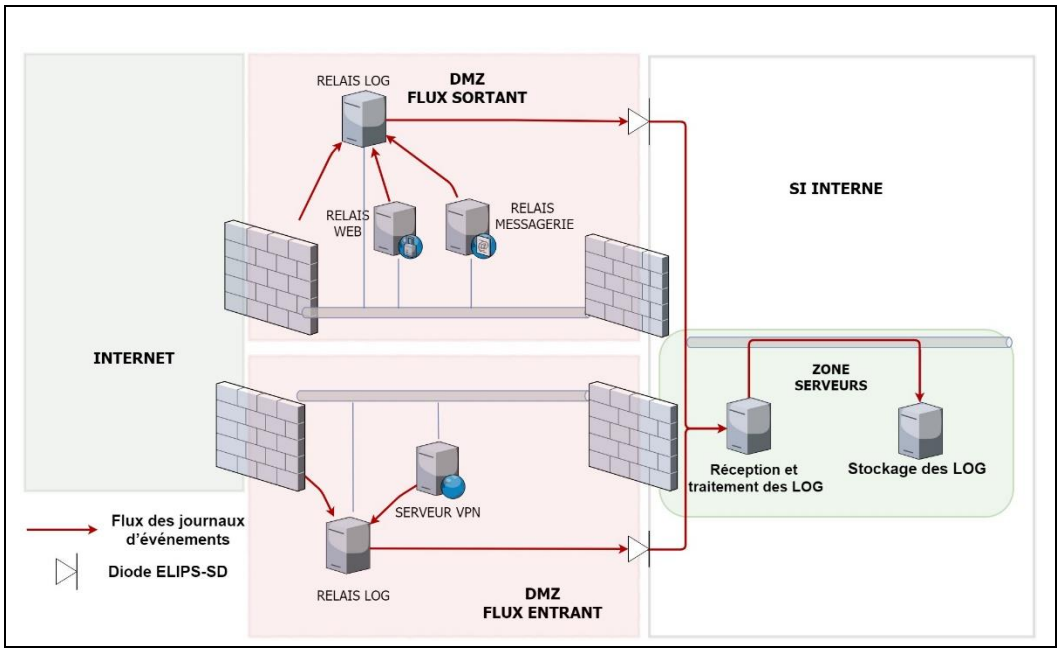

Figure 18 – Gestion des journaux d'évènements

Limitation technique :

Afin de pouvoir utiliser une diode, il faut absolument utiliser le protocole UDP qui n'est pas connecté à la différence de TCP. Dans cette architecture les journaux d'évènement sont gérés par RSYSLOG qui fonctionne en UDP.

CONCLUSION

L'étude de la menace pesant sur le cyberespace a mis en lumière l'intérêt que représentent les systèmes d'information gouvernementaux pour les groupes malveillants soutenus par des états. Il a également été démontré au cours de ce mémoire que l'évolution récente des TTP[28] et de la structure « des Internets » favorisent l'anonymat des cybers attaquants et accentuent ainsi leur sentiment d'impunité.

Afin de limiter cette liberté d'action, les états tentent de légiférer ensemble. Le constat est contrasté entre les avancées substantielles obtenues par des organismes comme l'OTAN, et l'échec de l'ONU à faire avancer ce sujet épineux.

Face à ces difficultés, la France légifère depuis une quinzaine d'années afin de protéger ses infrastructures vitales, et a également créé des organismes étatiques dédiés à l'optimisation de la cyberdéfense de la nation.

Dans ce contexte, et suite à l'analyse des faiblesses identifiées dans le système d'informations dont j'ai la responsabilité professionnelle, il apparait pertinent d'opter pour une stratégie de défense visant à augmenter la confiance dans les domaines clés suivants :

- Les connexions réseaux émanant du cyberespace : L'objectif est de simplifier l'identification des flux dits « légitimes ». Pour atteindre cet effet, l'ensemble du flux entrant passe désormais par une DMZ dédiée et est limité à la technologie VPN IPSEC.

- L'authentification : Afin d'y parvenir, une infrastructure de gestion de clés a été mise en œuvre. Celle-ci permet d'augmenter la difficulté d'usurpation d'une identité tout en facilitant la mission des administrateurs via une gestion centralisée.

- Les journaux d'évènement : Pierre angulaire dans la détection d'intrusions, les mécanismes mis en œuvre permettent d'en garantir l'intégrité.

[28] Tactics, Techniques, and Procedures

L'architecture finalisée est la suivante :

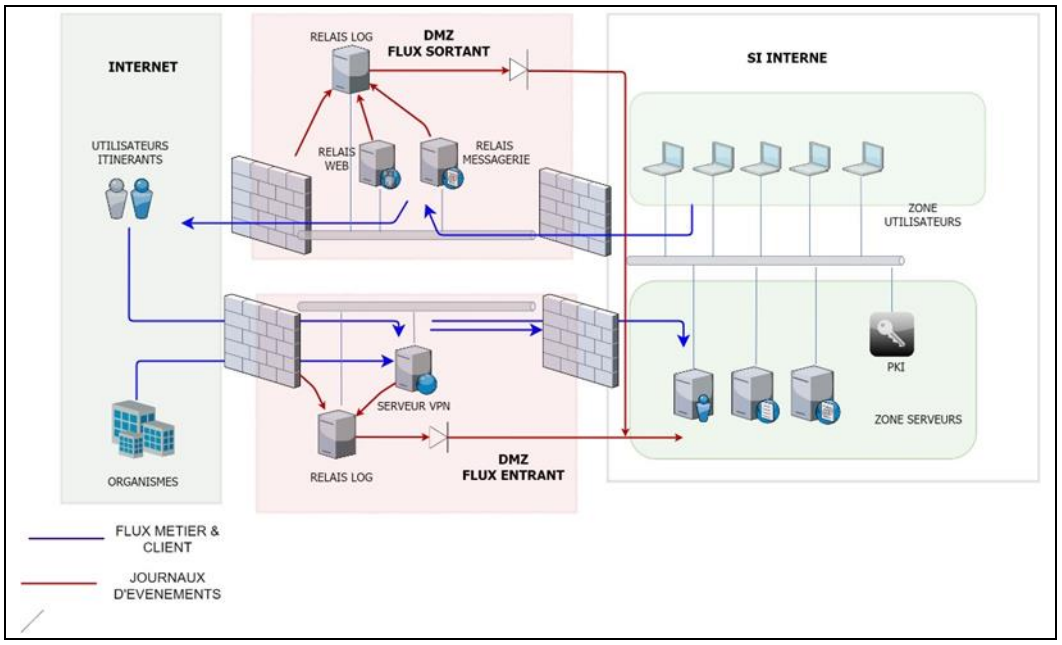

Figure 19 – Structure finale du système d'information

L'ensemble de ces modifications optimisent de façon significative le niveau de sécurité du système d'information. Elles permettent également de disposer de fondations solides pour les futures évolutions en matière de cyberdéfense. Celles-ci pourraient se matérialiser de la manière suivante :

- Les connexions : Mise en œuvre d'une duplication post concentrateur VPN (à l'aide d'un TAP[29] ou d'un miroir réseau) afin de mettre en œuvre un NIDS[30]. Ce dernier pourrait alors détecter les intrusions réseaux au plus tôt.
- L'authentification : Mise en œuvre d'une authentification forte sur les postes nomades (Carte puce avec code PIN[31]) et généralisation de l'utilisation des certificats dans l'ensemble du SI pour s'authentifier.
- Les journaux d'évènement : L'utilisation des LOG par des applications tierces comme un SIEM[32] permettrait de détecter les actions malveillantes au plus tôt.

A l'image de l'évolution des menaces, les méthodes de cyberdéfense doivent elles aussi se développer. Dans ce cadre, un Maintien en Condition Opérationnelle ainsi qu'une veille technologique sont indispensables tout au long de la vie du système d'information afin de garantir un niveau de sécurité optimal.

[29] Terminal Access Point
[30] Network Intrusion Detection System
[31] Personal Identification Number
[32] Security Information and Event Management

BIBLIOGRAPHIE ET RESSOURCES INTERNET

Agence Nationale de la sécurité des systèmes d'information. (2015, 08 3). *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.* Récupéré sur https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-ipsec-pour-la-protection-des-flux-reseau/

Agence Nationale de la sécurité des systèmes d'information. (2018, 10 17). *Recommandations sur le nomadisme numérique.* Récupéré sur https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

Anonymat sur Internet. (s.d.). Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Anonymat_sur_Internet

Aug. Kerckhoffs. (1883, Février). *JOURNAL DES SCIENCES MILITAIRES ; LA CRYPTOGRAPHIE MILITAIRE*. Récupéré sur https://www.petitcolas.net/kerckhoffs/la_cryptographie_militaire_ii.htm

Bonnemaison, A., & Dossé, S. (2014). *Attention : Cyber ! : Vers le combat cyber-électronique.* Economica.

Boyer, B. (2012). *Cyberstratégie, l'art de la guerre numérique.* Nuvis.

Debian. (2008, mai). *CVE-2008-0166*. Récupéré sur security-tracker.debian.org: https://security-tracker.debian.org/tracker/CVE-2008-0166

Global Commission on the Stability of Cyberspace. (2019, November 01). *Final report.* Récupéré sur cyberstability.org: https://cyberstability.org/report/

Hutchins, E. M., Cloppert, M. J., & Rohan M. Amin, P. (s.d.). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Récupéré sur Lockheed Martin Corporation: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Journal officiel de l'Union Européenne. (2016, 07 6). *The Directive on security of network and information systems.* Récupéré sur https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

Kaspersky. (2016, 03 11). *Exécutions des VPN et leurs particularités.* Récupéré sur https://www.kaspersky.fr/blog/vpn-execution/5359/

Kempf, O. (2015). *Introduction à la cyberstratégie .* Economica.

Ministère des armées. (2018, 10 17). *La cyberdéfense.* Récupéré sur https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

Organisation du Traité de l'Atlantique Nord. (2020, 03 31). *Cyberdéfense.* Récupéré sur https://www.nato.int/cps/fr/natohq/topics_78170.htm

Pernet, C. (2014). *Sécurité et espionnage informatique - Guide technique de prévention - Connaissance de la menace APT (Advanced Persistent Threat) et du cyber espionnage.* Eyrolles.

Secrétariat Général de la Défense et de la Sécurité Nationale. (2013, 12 02). *Recommandations de sécurité pour la mise en œuvre.* Récupéré sur https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf

Secrétariat Général de la Défense et de la Sécurité Nationale. (2018, 03 15). *REVUE STRATÉGIQUE DE CYBERDÉFENSE.* Récupéré sur http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

Secrétariat Général de la Défense et de la Sécurité Nationale. (s.d.). *Assurer la cyberdéfense.* Récupéré sur http://www.sgdsn.gouv.fr/missions/assurer-la-cyberdefense/

Thales & Verint. (2019, 10 07). *Cyberthreat handbook.* Récupéré sur https://www.thalesgroup.com/fr/group/journaliste/press-release/cyberthreat-handbook-thales-et-verint-presentent-leur-whos-who-des

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ACRONYMES

AC : *Autorité de Certification*

AES : *Advanced Encryption Standard*

AH : *Authentication Header*

ANSSI : *Agence Nationale de la Sécurité des Systèmes d'Information*

APT : *Advanced Persistent Threat*

CERT : *Computer Emergency Response Team*

DMZ : *DeMilitarized Zone*

ESP : *Encapsulation Security Payload*

GCSC : *Global Commission on the Stability of Cyberspace*

GGE : *Group of Governmental Experts*

HTTP : *HyperText Transfer Protocol*

HTTPS : *HyperText Transfer Protocol Secure*

ICV : *Integrity Check Value*

IDS : *Intrusion detection System*

IGC : *Infrastructure de Gestion de Clés*

IKE : *Internet Key Exchange*

IoT : *Internet of Things*

IPSEC : *Internet Protocol Security*

NAT : *Network Address translation*

NIDS : *Network Intrusion Detection System*

NIS : *Network and Information System Security*

LID : *Lutte Informatique Défensive*

LIO : *Lutte Informatique Offensive*

OIV : *Opérateur d'Importance Vitale*

ONU : *Organisation des Nations Unies*

OTAN : *Organisation du Traité de l'Atlantique Nord*

PIN : *Personal Identification Number*

PRNG : *PseudoRandom Number Generator*

PSK : *Pre-Shared Key*

SA : *Security Association*

SCADA : *Supervisory Control And Data Acquisition*

SI : *Système d'Information*

SIEM : *Security Information and Event Management*

SFTP : *Secure File Transfer Protocol*

SGDSN : *Secrétariat Général de la Défense et de la Sécurité nationale*

SMTP : *Simple Mail Transfer Protocol*

SP : *Security Policy*

SPD : *Security Policy Database*

SSL : *Secure Sockets Layer*

TAP : *Terminal Access Point*

TCP : *Transmission Control Protocol*

TLS : *Transport Layer Security*

TTP : *Tactics, Techniques, and Procedures*

UDP : *User Datagram Protocol*

USB : *Universal Serial Bus*

VPN : *Virtual Private Network*

GLOSSAIRE DES TERMES TECHNIQUES

AIRGAP *: En sécurité informatique, un air gap1, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique.*

Darkweb : *Ensemble des sites Internet qui fonctionnent sur des réseaux uniquement accessibles via des logiciels, des configurations ou des autorisations spécifiques, permettant généralement une forme d'anonymat.*

LOG : *En anglais et en argot franglais, le terme « log file » est la traduction de « journal » ou de « main-courante », tandis que le terme « inscription » est traduit en anglais par « log ».*

Man in the middle : *est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.*

One Day : *vulnérabilité dans un produit informatique ayant fait l'objet d'une publication et dont la communauté de la sécurité informatique a connaissance.*

Zero Day : *vulnérabilité dans un produit informatique n'ayant fait l'objet d'aucune publication et dont la communauté de la sécurité informatique n'a pas connaissance.*

TABLE DES MATIERES EXHAUSTIVE