

TABLE DES MATIÈRES (*extrait*)

PRÉAMBULE

INTRODUCTION

PREMIÈRE PARTIE – Les dangers du monde cyber

I. Des menaces en évolution rapide

L'espionnage informatique
La cybercriminalité
La déstabilisation
Le sabotage informatique

II. Les grands principes d'action et les modes opératoires des attaques informatiques

Les quatre phases d'une attaque
Les infrastructures de l'attaquant
Une structuration de la menace

III. Des systèmes toujours plus vulnérables

Un état de sécurité insuffisant
Les risques associés à la transformation numérique
L'existence d'un risque systémique
L'accroissement de la menace d'origine cyber

IV. Comment résister aux attaques ?

Intégrer à bon niveau les enjeux de cybersécurité dans les organisations
Prendre en compte la sécurité tout au long du cycle de vie des systèmes d'information
Connaître les technologies et la menace
Envisager une défense active maîtrisée

V. Une régulation internationale encore trop balbutiante

Les négociations internationales sur la régulation du cyberspace à un tournant
Des fondements théoriques en construction

VI. Les différents modèles d'organisation de cyberdéfense dans le monde

Dans le domaine cyber, les puissances sont peu nombreuses et bien identifiées
Des puissances de taille modeste capables de déployer des capacités offensives avancées

DEUXIÈME PARTIE – L'État, responsable de la cyberdéfense de la Nation

I. Le modèle français de cyberdéfense

Aux origines du modèle français de cyberdéfense
Les principes du modèle français de cyberdéfense
Le cadre juridique de la cyberdéfense française
Les six missions de la cyberdéfense française

II. Consolider l'organisation de la cyberdéfense

Créer quatre chaînes opérationnelles pour conduire les missions de cyberdéfense
Moderniser la gouvernance de la cyberdéfense

III. Améliorer la protection des activités sensibles

La sécurisation des systèmes d'information de l'État
La protection des opérateurs d'importance vitale (OIV)
La protection des activités essentielles
La protection des collectivités territoriales

IV. Renforcer la lutte contre la cybercriminalité

Évaluer plus finement l'étendue des actes de cybercriminalité
Renforcer l'efficacité de la réponse judiciaire pour améliorer la lutte contre la cybercriminalité

Développer un réseau international de collaboration entre magistrats et enquêteurs

V. L'action internationale de la France dans le domaine cyber

Renforcer le dialogue et les coopérations avec nos alliés et partenaires pour prévenir les crises cyber
Garantir la sécurité et l'autonomie stratégique européenne dans l'espace numérique
Définir une doctrine d'action
Réguler le cyberspace

TROISIÈME PARTIE – L'État, garant de la cybersécurité de la société

I. La souveraineté numérique, composante essentielle de la souveraineté nationale

Les activités souveraines
Trois technologies, parmi d'autres, dont la maîtrise est essentielle à notre souveraineté numérique
Tirer tout le potentiel des techniques d'intelligence artificielle au profit de la cybersécurité
Pour l'informatique en nuage, inventer une stratégie de régulation et de protection des données
Réguler la production et l'exportation des armements et des activités offensives cyber

II. La régulation de la cybersécurité

Le rôle normatif de l'ANSSI
Améliorer le cadre de certification pour améliorer la sécurité des produits
La responsabilité par milieu : impliquer l'ensemble des acteurs sectoriels pour élever notre niveau de cybersécurité
Les prestataires de confiance : développer une offre de services de cyberdéfense
Le développement de la qualification de prestataires de services numériques sécurisés
La mise en place d'un cadre de certification harmonisé à l'échelle européenne

III. L'économie de la cybersécurité

La base industrielle nationale
Définir une politique industrielle de cybersécurité et construire une base industrielle de cybersécurité européenne
Disposer de produits performants et certifiés
La notation « cybersécurité » et les enjeux de compliance
La mise en place d'un cercle vertueux de sécurisation des systèmes par le biais d'un mécanisme assurantiel pertinent

IV. Les enjeux humains

Éduquer dès le plus jeune âge aux enjeux de la cybersécurité
Sensibiliser le grand public par des actions pédagogiques
Diffuser la culture de la sécurité numérique au sein des entreprises et des administrations publiques
Développer l'offre de formation professionnelle aux enjeux de la cybersécurité
Perfectionner la gestion des compétences dans les services chargés de la cyberdéfense de l'État : conserver nos talents et en attirer

CONCLUSION

RECOMMANDATIONS PRIORITAIRES

ANNEXES