27.11.2025

PARIS

FRANCE-IX TOUR

15 ANS

ÉDITION SPÉCIALE

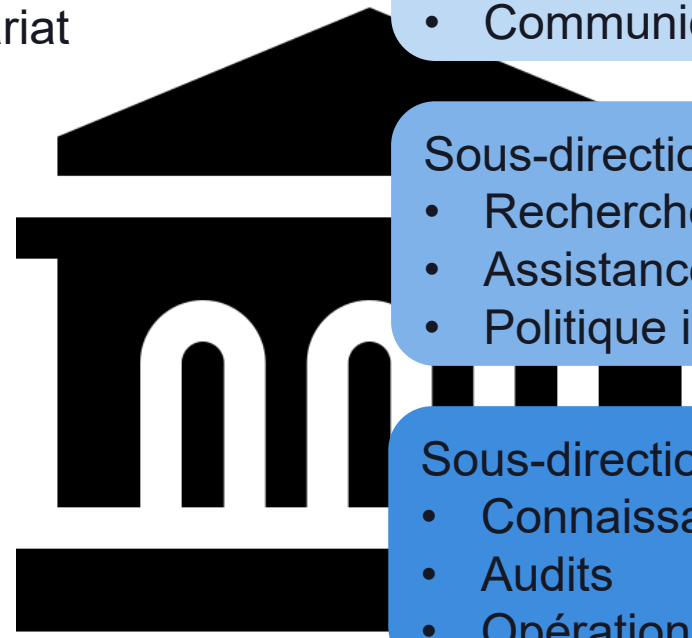
La directive NIS2 : comprendre l’essentiel en moins de 15 minutes

Ionathan Noblins - Coordinateur français pour la cybersécurité des télécommunications et des infrastructures du numérique

ANSSI

Un mot sur l'ANSSI

- Agence nationale de la sécurité des systèmes d'information
- **Autorité nationale** en matière de cybersécurité et de cyberdéfense
- **Service du Premier ministre** rattaché au Secrétariat général de la défense et de la sécurité nationale (**SGDSN**)
- Mission purement **défensive** (et non offensive)
- Trois piliers d'action :
  - Sécurité de L'État
  - Protection de la Nation
  - Réponse aux cyberattaques
- ~650 agents



Sous-direction **stratégie**
- Supervision
- Coordination(s)
- Communication

Sous-direction **expertise**
- Recherche et bonnes pratiques
- Assistance technique
- Politique industrielle

Sous-direction **opérations**
- Connaissance de la menace
- Audits
- Opérations de cyberdéfense

La menace cyber aujourd'hui

Une menace protéiforme qui touche l'ensemble du tissu économique et poursuit 3 grands objectifs

S'enrichir
Chantage / Pillage

- Augmentation de 30% des attaques par **rançongiciel** (ex. Black Cat)

- Vol de **données** puis revente (ex. DCP)
- **Fraude** (ex. appels vers numéros surtaxés, services d'appels à bas prix)

Déstabiliser
Sabotage

- **DDoS** par des groupes hacktivistes pro-russes (ex. NoName057)
- Augmentation des capacités de saturation des attaquants

- Le secteur est considéré comme particulièrement exposé à la menace, a fortiori en temps de guerre
- Ex. **destruction de cœurs** de réseaux mobiles

Dominer
Espionnage

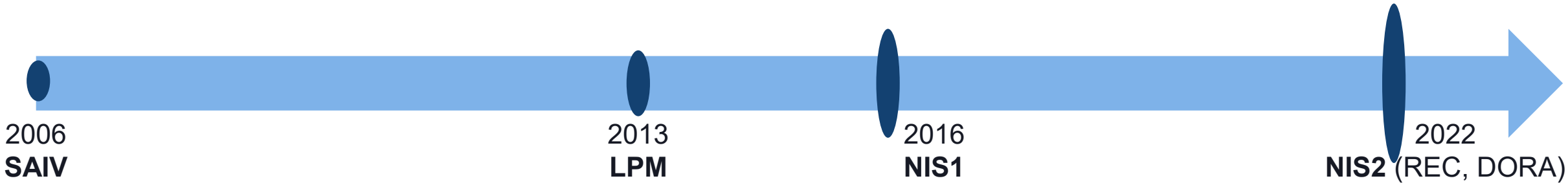
- **Ciblage direct** des opérateurs
- **Ciblage indirect** des clients des opérateurs (ex. instituts de recherche et de la BITD)

- Attaquants réputés liés aux intérêts **chinois** (ex. Gallium, Salt Typhoon, Liminal Panda)
- Activités relevant de MOA associés publiquement à l'état **russe** (ex. Sandworm, Turla)

Face aux menaces : les réponses FR et UE

Protéger la Nation et garantir le bon fonctionnement des sociétés de l'Union

- 1958 : dispositif de protection des points et réseaux **sensibles** (PPRS)
- 2006 : dispositif de sécurité des activités d'**importance vitale** (SAIV), pour protéger les opérateurs indispensables à l'exercice de l'autorité de l'Etat et au fonctionnement de l'économie, en particulier face à la montée du terrorisme
- 2013 : la loi de programmation militaire (LPM) introduit une capacité de fixer des **règles de cybersécurité** pour un ensemble particulier d'opérateurs qualifiés d'importance vitale (dits OIV, cf. ci-dessus)
- 2016 : assujettissement de grands acteurs économiques du marché intérieur et de leurs SI (OSE, SIE), renforcement du cadre de coopération en matière de cybersécurité entre états membres (ex. GC NIS)



NIS2 : premières généralités

Une hygiène informatique de base pour faire face à la cybercriminalité de masse

Objectifs & grands principes

- Élever le **niveau de cybersécurité** dans l'UE face à la **cybercriminalité de masse**

➢ Étendre le périmètre assujetti à de **plus petites structures**

➢ Introduire de nouvelles obligations notamment de **gestion des risques**

Quelques concepts clés

- **Champ** d'application : pour qui, sur quoi
  - Nature d'activité = 18 secteurs et ~70 types d'entités
  - Portée des exigences = tous SI et réseaux
- **Proportionnalité** EI/EE (obligations, sanctions)
  - Volume d'activité = statut important ou essentiel
- **Concertation** et consultations

Illustration : chapitres et orientation (25 p. /72)

Section	p.
Considérations	28
Chapitre I - Dispositions générales	**4**
Chapitre II - Cadres coordonnés	6
Chapitre III - Coopération UE/Int	6
Chapitre IV - Mesures de gestion des risques	**6**
Chapitre V - Compétence et enregistrement	**2**
Chapitre VI - Partage d'informations	2
Chapitre VII - Supervision et exécution	**7**
Chapitre VIII - Actes délégués et d'exécut°	**1**
Chapitre IX - Dispositions finales	1
Annexes I - Secteurs hautement critiques	**4**
…	6

Caractérisation des entités du secteur

Entités importantes et essentielles (EI/EE) : cas général, cas particuliers

Cas général

- Points d'**échange** internet
- Services d'informatique en **nuage**
- Services de **centres de données**
- Réseaux de diffusion de **contenu**

Cas télécom

- **Réseaux** de communications électroniques publics
- **Services** de communications électroniques accessibles au public

- **Offices** de NDD de premier niveau
- Services de **confiance** (ex. certificats, signatures)
- Services **DNS**

- Services gérés (i.e. « **managés** »)
- Services de sécurité gérés

-

-

ETI/GE	Seuil 2 : 250/50/43	EE	EE
ME	Seuil 1 : 50/10/10	EI	EE
TPE/PE	Non assujettis		EI

Proportionnalité : Obligations, Sanctions

Obligations

- Des **mesures de sécurité** relevant de **thématiques habituelles** de la cybersécurité, ex. cartographie, analyse des risques, MCS, sauvegardes, gestion des prestataires, des incidents, etc.

Un **référentiel national** qui se veut **souple** et **proportionné**, articulé sur la notion d'objectifs, toujours **en co-construction** (ex. avec un ensemble d'organisations professionnelles et de ministères).

Sanctions

- Notamment financières, de façon simplifiée : jusqu'à **2% du CA** mondial pour les EE ; 1,4% pour les EI.

Autres informations choisies

- Des obligations relatives à l'**enregistrement** et à la **notification des incidents**
- La **territorialité** et le **règlement d'exécution** (référentiel européen harmonisé)
- La spécificité des fournisseurs de **services d'enregistrement DNS** (ex. BE).

En (presque) conclusion

1. Prendre connaissance de **la directive** et du projet de loi

- https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555

2. Consulter les sites **MonEspaceNIS2** (en version bêta) et **MesServicesCyber**, les premières pierres du dispositif d'accompagnement mis en place par l'ANSSI

- https://monespacenis2.cyber.gouv.fr/
- https://messervices.cyber.gouv.fr/nis2/

3. Effectuez votre **pré-enregistrement** (en version bêta)

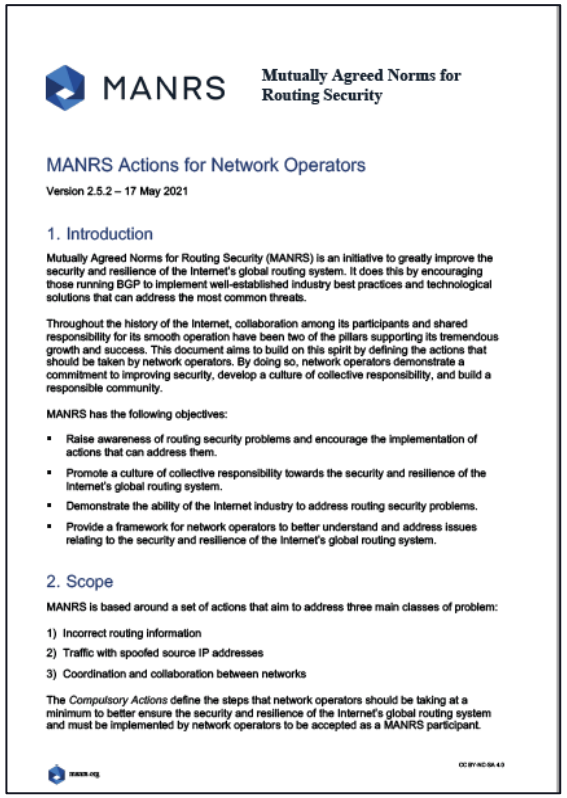
- https://club.ssi.gouv.fr/#/nis2/introduction

4. Commencer à **préparer** vos organisations à la mise en œuvre de la directive NIS2 (ex. opérationnels, juristes) en **estimant l'effort nécessaire** à la future mise en conformité sur la base des informations disponibles

- https://cyber.gouv.fr/les-fondamentaux-pour-se-securiser
- https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

Au-delà de NIS2 et des mesures d’hygiène

Risques spécifiques à l’interconnexion, autres réglementations (ex. CRA, DORA), autres menaces (ex. menace étatique, menace quantique)


MANRS Mutually Agreed Norms for Routing Security

MANRS Actions for Network Operators

Version 2.5.2 – 17 May 2021

1. Introduction

Mutually Agreed Norms for Routing Security (MANRS) is an initiative to greatly improve the security and resilience of the Internet's global routing system. It does this by encouraging those running BGP to implement well-established industry best practices and technological solutions that can address the most common threats.

Throughout the history of the Internet, collaboration among its participants and shared responsibility for its smooth operation have been two of the pillars supporting its tremendous growth and success. This document aims to build on this spirit by defining the actions that should be taken by network operators. By doing so, network operators demonstrate a commitment to improving security, develop a culture of collective responsibility, and build a responsible community.

MANRS has the following objectives:

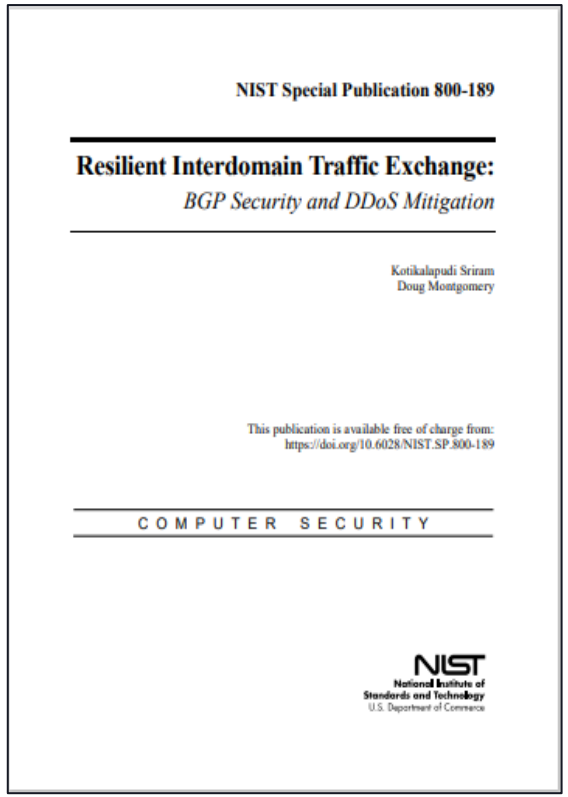
- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility towards the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

2. Scope

MANRS is based around a set of actions that aim to address three main classes of problem:

1) Incorrect routing information
2) Traffic with spoofed source IP addresses
3) Coordination and collaboration between networks

The *Compulsory Actions* define the steps that network operators should be taking at a minimum to better ensure the security and resilience of the Internet's global routing system and must be implemented by network operators to be accepted as a MANRS participant.


NIST Special Publication 800-189

Resilient Interdomain Traffic Exchange:

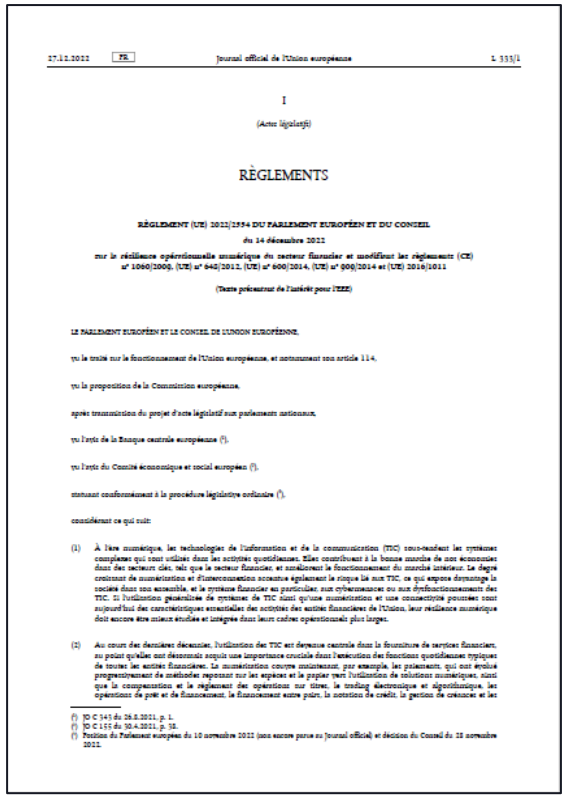
BGP Security and DDoS Mitigation

Kotikalapudi Sriram
Doug Montgomery

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-189

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


27.12.2022 FR Journal officiel de l'Union européenne L 333/1

I

(Actes législatifs)

RÈGLEMENTS

RÈGLEMENT (UE) 2022/2554 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis de la Banque centrale européenne (1),

vu l'avis du Comité économique et social européen (2),

statuant conformément à la procédure législative ordinaire (3),

considérant ce qui suit:

(1) À l'ère numérique, les technologies de l'information et de la communication (TIC) sous-tendent les systèmes complexes qui sont utilisés dans les activités quotidiennes. Elles contribuent à la bonne marche de nos économies dans des secteurs clés, tels que le secteur financier, et renforcent le fonctionnement du marché intérieur. Le degré croissant de numérisation et d'interconnexion accentue également le risque lié aux TIC, ce qui expose davantage la société dans son ensemble, et le système financier en particulier, aux cybermenaces ou aux dysfonctionnements des TIC. Si l'utilisation généralisée des systèmes de TIC ainsi qu'une numérisation et une connectivité poussées sont aujourd'hui des caractéristiques essentielles des activités des entités financières de l'Union, leur résilience numérique doit encore être mieux étudiée et intégrée dans leurs cadres opérationnels plus larges.

(2) Au cours des dernières décennies, l'utilisation des TIC est devenue centrale dans la fourniture de services financiers, au point qu'elles ont désormais acquis une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières. La numérisation couvre notamment, par exemple, les paiements, qui ont évolué progressivement de méthodes reposant sur les espèces et le papier vers l'utilisation de solutions numériques, ainsi que la compensation et le règlement des opérations sur titres, le trading électronique et algorithmique, les opérations de prêt et de financement, le financement entre pairs, la notation de crédit, la gestion de créances et les

(1) JO C 343 du 26.8.2021, p. 1.
(2) JO C 155 du 30.4.2021, p. 38.
(3) Position du Parlement européen du 10 novembre 2022 (non encore parue au Journal officiel) et décision du Conseil du 28 novembre 2022.

Des questions ?
Merci !

Ionathan Noblins - Coordinateur français pour la cybersécurité des télécommunications et des infrastructures du numérique

ANSSI

https://fr.linkedin.com/company/france-ix

https://x.com/ixpfranceix