# « LA GUERRE HYBRIDE, UN DANGER POUR LA SÉCURITÉ ET LA DÉMOCRATIE »

**QUELS OUTILS POUR PRÉSERVER NOS DÉMOCRATIES FACE AUX ACTIONS DE LA GUERRE HYBRIDE :**

**L'EXPÉRIENCE BELGE ET EUROPÉENNE DANS LE CADRE DE LA PROTECTION DES ÉLECTIONS DE JUIN ET OCTOBRE 2024**

**PRÉSIDENCE BE UE**

Pascal PETRY
Président du Comité de coordination renseignement et sécurité (Belgique)

Pristina, 12 et 13 novembre 2024

# PLAN DE L'INTERVENTION

1. Concepts et réponses
2. Une structure plurielle
3. Un exemple concret
4. La continuité européenne

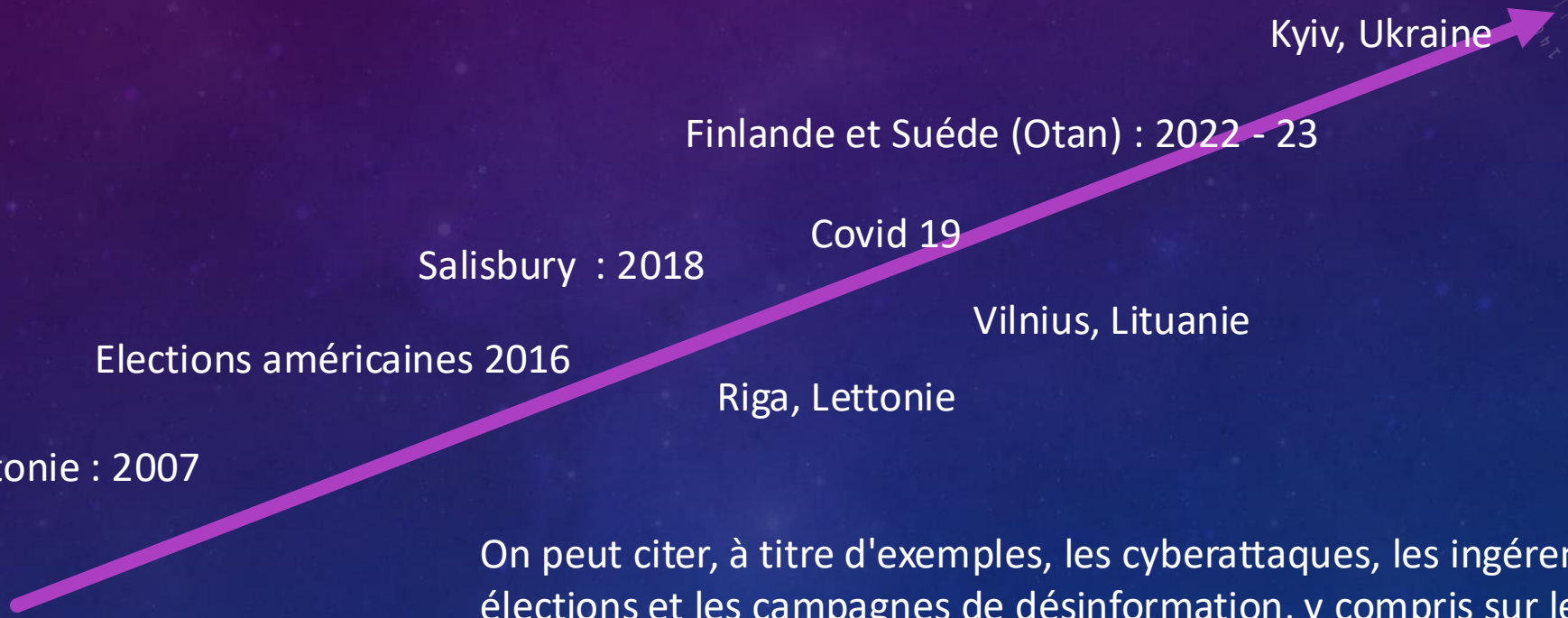
LA GUERRE HYBRIDE est une notion qui aide à définir des conflits actuels. Elle combine intimidation stratégique de la part d'Etats, opérations interarmées impliquant des unités spéciales et des mercenaires, et manœuvres de **désinformation à grande échelle.** Dans la pratique, une menace peut être considérée comme hybride dès lors qu'elle s'inscrit dans plusieurs dimensions et types de guerre différents (OTAN)


*LES CARACTÉRISTIQUES DE LA GUERRE HYBRIDE :*

*La guerre hybride repose sur la combinaison ou la fusion d'instruments de puissance conventionnels et non conventionnels et de méthodes subversives. L'objectif est d'exploiter les vulnérabilités de l'adversaire et de réaliser des synergies en employant ces outils de façon coordonnée.*

*Le recours conjoint à des moyens cinétiques et à des tactiques non cinétiques doit permettre d'infliger le plus de dommages possibles à un État belligérant. La guerre hybride présente deux autres particularités. La première est qu'elle brouille les lignes entre temps de guerre et temps de paix.*
*La deuxième particularité de la guerre hybride tient à son caractère ambigu et est liée à la question de l'attribution. En règle générale, un grand flou entoure les attaques hybrides. Les auteurs de telles attaques cultivent l'ambiguïté afin de compliquer l'attribution des actes perpétrés ainsi que la réponse à ceux-ci.*

*LES MENACES HYBRIDES désignent un large éventail de méthodes ou d'activités utilisées par des acteurs étatiques ou non étatiques hostiles de manière coordonnée afin de cibler les vulnérabilités des États et institutions démocratiques, tout en restant en dessous du seuil de la guerre officiellement déclarée (Conseil de l'Union européenne - décembre 2019)*




On peut citer, à titre d'exemples, les cyberattaques, les ingérences dans les élections et les campagnes de désinformation, y compris sur les médias sociaux.

## *Le renforcement de la confiance comme réponse démocratique aux menaces hybrides*

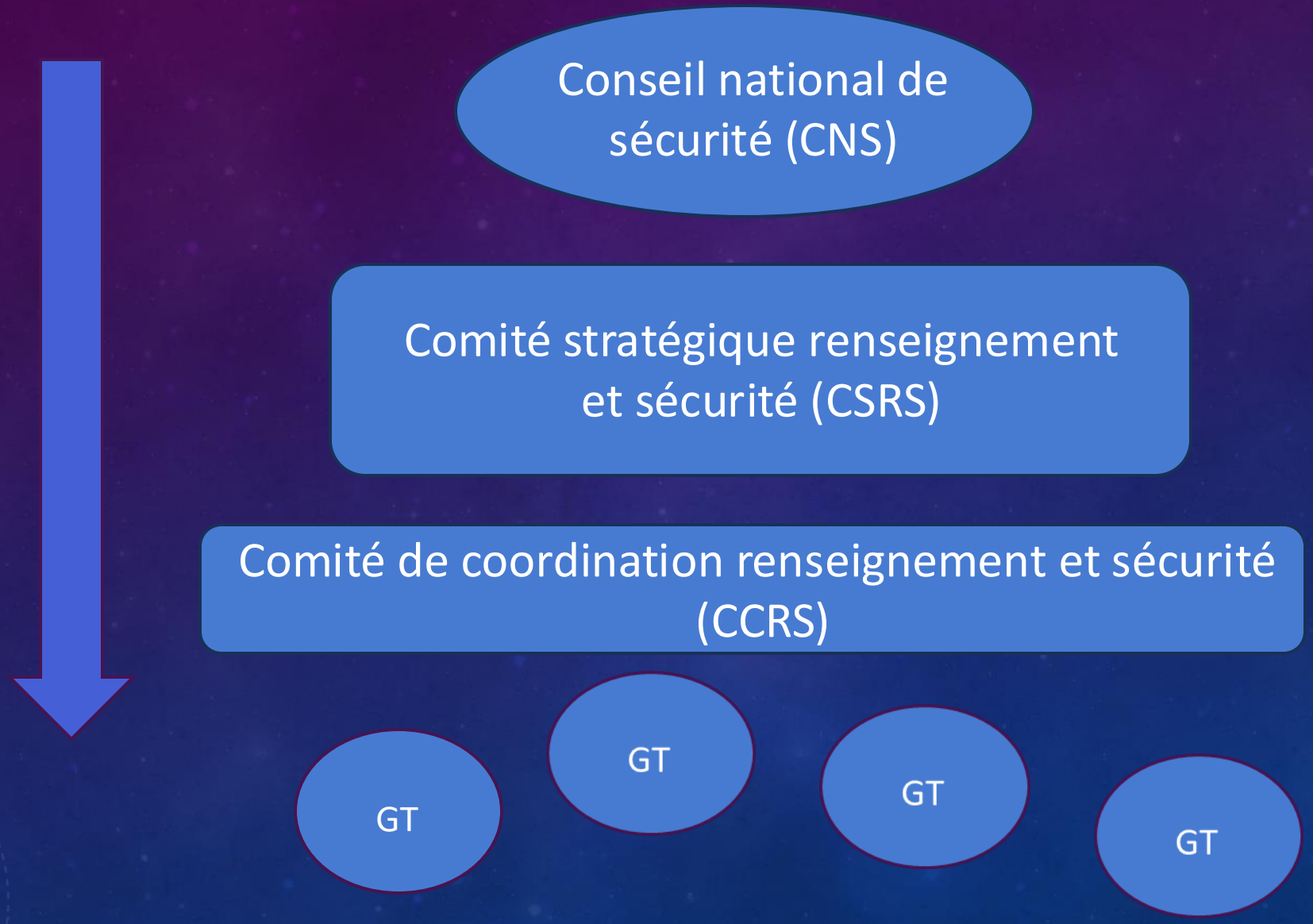
*Compte tenu de la nature complexe et des multiples visages de la guerre hybride, les experts ont défini toute une série de mécanismes de réponse, d'ordre stratégique ou autre, dont certains reposent sur un ensemble soigneusement étudié de mesures de détection, de dissuasion, de lutte et de réaction. Cependant, comme les domaines informationnel, cognitif et social revêtent une importance de plus en plus fondamentale dans la guerre hybride, il est probable qu'aucune des solutions envisagées ne constituera un antidote efficace si elle ne s'accompagne pas de mesures de renforcement de la confiance, entre les services publics et entre les services et la population. (…)*

*Il demeure essentiel d'établir – ou de rétablir – la confiance et de la renforcer pour pouvoir faire preuve, dans la durée, de résilience face aux menaces hybrides, qui mettent gravement en péril la sécurité de l'État et de la société. Le développement de la confiance devrait constituer le fondement de l'action visant à neutraliser les menaces hybrides. Dans cette optique, il est nécessaire de déployer des efforts soutenus, sur le plan structurel comme politique, en vue de créer des liens solides entre État et citoyens, dans un climat de transparence, de participation et d'inclusivité.*

*OTAN - Arsalan Bilal - 30 novembre 2021*

# L'EXEMPLE BELGE

# MOBILISER TOUS LES NIVEAUX DE L'ÉTAT, UNE RÉPONSE PLURIELLE À UNE MENACE PLURIELLE

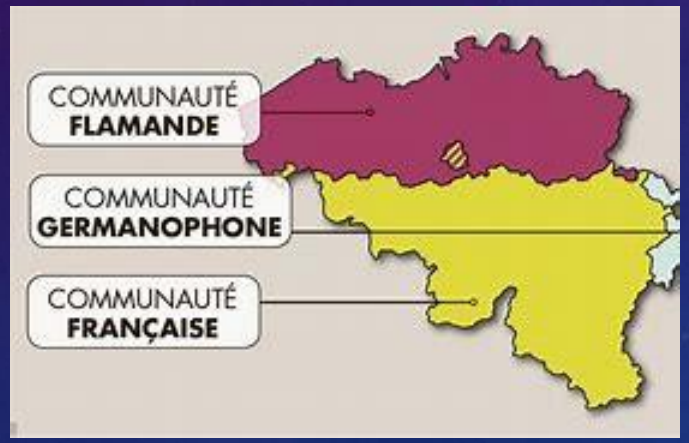


# LES SERVICES… LA PLUS-VALUE

- La sûreté de l'Etat (VSSE) : service de renseignement civil (1830)
- Le service général du renseignement et de la sécurité (SGRS)
- La police fédérale (police spécialisée et appui)
- Le centre de crise du gouvernement fédéral (NCCN)
- L'Organe de Coordination pour l'Analyse de la Menace (OCAM)
- Le SPF Affaires étrangères
- La Défense nationale
- Le Centre pour la Cybersécurité Belgique (2014)
- Le Ministère public
  - Parquet fédéral
  - Le Parquet général de Bruxelles

# ENJEUX A PROTEGER : ex. BE, FR, USA

IDENTIFIER LES RISQUES


# ENJEUX INTERNATIONAUX À PROTÉGER


Rupture de confiance

Déstabilisation


Polarisatrion

# PROTÉGER LE PROCESSUS ÉLECTORAL

IDENTIFIER LES RISQUES

PRÉVENTION

PRÉPARATION

- La campagne électorale
- Le vote
- La collecte des résultats électoraux
- La formation des gouvernements
- La mise en place des gouvernements

## Principaux Risques Identifiés :

1. Risques Hybrides :

- **Manipulation de l'opinion publique** : Très probable, avec un impact élevé, notamment par des opérations d'information visant à polariser la société.
- **Financement de partis ou candidats par des acteurs étrangers** : Probable et potentiellement déstabilisant.
- **Création d'organisations influentes** : Utilisées pour diffuser de la propagande sous couvert de recherche ou de journalisme.

2. Risques Techniques :

- **Défaillances des systèmes de vote électronique** (SMARTMATIC) : Risques de pannes techniques ou de corruption des données, avec des impacts variables selon l'étendue des défaillances

- **Défaillances des modules MARTINE** : Utilisés pour la transmission des résultats, avec des risques de retards ou de corruption des données.

## 3. Risques Cyber :

- **Cyberattaques** : Risques de perturbation des systèmes de vote électronique et de transmission des résultats, avec des impacts potentiellement élevés.

## 4. Risques Processuels :

- **Perte de bulletins de vote physiques** : Risque faible mais avec un impact potentiel élevé.
- **Erreurs de procédure** lors de la distribution des kits de vote électronique : Risque faible mais avec des conséquences importantes si elles se produisent.

## Mesures de Prévention et d’Atténuation

- **Exercices Nationaux** : Organisation d’exercices pour tester les structures et les réponses aux menaces.

- **Communication Stratégique** : Importance de la communication proactive et de la sensibilisation du public pour contrer la désinformation.

- **Sécurité des Systèmes** : Contrôles réguliers et audits des systèmes de vote électronique et des infrastructures critiques.

- **Collaboration Interdépartementale** : Coordination entre diverses agences et services pour surveiller, détecter et répondre aux menaces.

# AVANT, PENDANT ET APRÈS LA CAMPAGNE ÉLECTORALE

## Sensibilisation High Level

## Mise à disposition d'outils


CENTRE FOR CYBERSECURITY BELGIUM

## Répartition des tâches et partenariats

Presse

**Elections 2024 : la Belgique va faire la chasse aux fausses informations circulant sur internet**

Le gouvernement a décidé de faire travailler main dans la main les différents services de sécurité du pays afin de contrer la propagation de fausses informations destinée à déstabiliser l'Etat en période électorale.


« Les médias ont un rôle énorme à jouer dans la désinformation pour aider les gens à faire du **fact-checking**.

Les gens doivent vérifier les informations, recouper leurs sources »

Police et justice

**Soupçons d'ingérence russe : perquisitions au Parlement européen à Bruxelles et Strasbourg**

# TRAVAIL PARLEMENTAIRE

**SÉNAT DE BELGIQUE**

**SESSION DE 2023-2024**

22 MARS 2024

**Rapport d'information relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique**

**CONSTATATIONS ET RECOMMANDATIONS**
ADOPTÉES PAR LA COMMISSION DU RENOUVEAU DÉMOCRATIQUE, DE LA CITOYENNETÉ ET DES AFFAIRES INTERNATIONALES

## Ingérences étrangères : la Chambre se constitue partie civile à la suite de cyberattaques chinoises

La Chambre a décidé mardi de se constituer partie civile à la suite de cyberattaques dont plusieurs députés ont fait l'objet, a-t-on appris à l'issue d'une réunion du Bureau de l'assemblée.

FÉDÉRATION WALLONIE-BRUXELLES
LE PARLEMENT

Assemblée parlementaire de la Francophonie

**Commission spéciale INGE1/ING2**

## L'espionnage et l'ingérence étrangère vont être davantage punis en Belgique


disinformation
Fake
Guide de communication sur la désinformation
Une compilation d'informations utiles, de conseils et de sites web intéressants qui peuvent aider une autorité à faire face à la désinformation.

# APRÈS ? ...


Hybrid CoE

VIGINUM

EUROPOL 25

Mai 2024

*« La mise en place pratique des équipes d'intervention rapide de l'UE en cas de menaces hybrides. Cela ouvre la voie au déploiement de ces équipes sur demande, dans le cadre de la préparation et de la lutte contre les menaces et les campagnes hybrides. »*

# MERCI DE VOTRE ATTENTION…

Assemblée parlementaire de la Francophonie
Région Europe

Republika e Kosovës

Republika Kosova – Republic of Kosovo
*Kuvendi – Skupština – Assembly*

# …ET DE VOTRE ACCUEIL

# RESSOURCES

- https://view.genially.com/61b62b054f808a0d680e156e/presentation-image-manipulee
- https://www.ipnoze.com/exemples-medias-manipulent-verite/