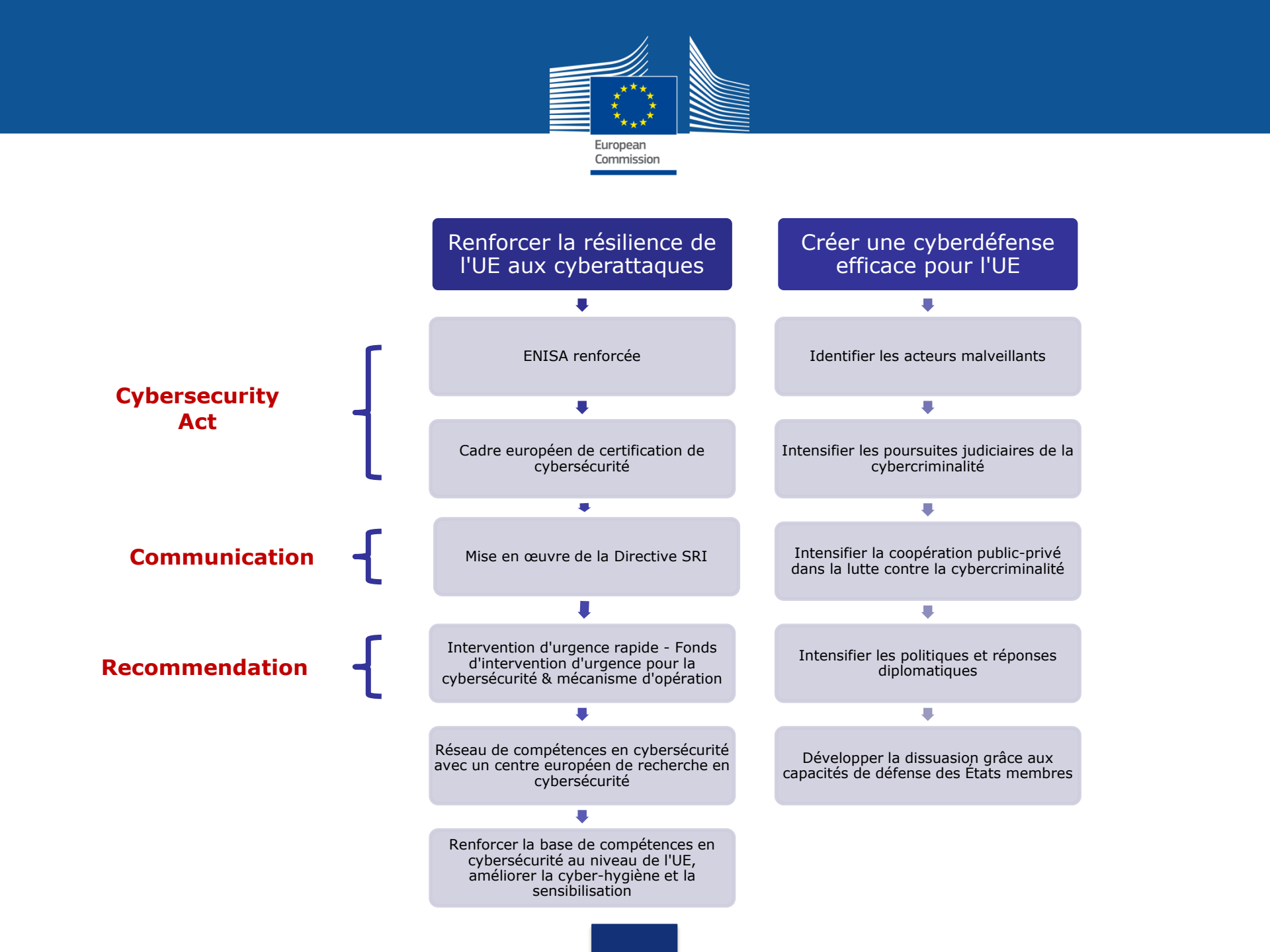
Le paquet «Résilience, Dissuasion et Défense: Construire une UE résiliente en matière de cyber sécurité»

Le paquet «Résilience, Dissuasion et Défense: Construire une UE résiliente en matière de cyber sécurité»

Mesures politiques importantes *énoncées dans le paquet pour protéger les citoyens européens, les entreprises et institutions publiques contre les cyber-attaques et les menaces hybrides:*

- *Un règlement qui renouvelle le mandat de l'**Agence de l'Union européenne pour la sécurité des réseaux et de l'information** (ENISA)*
- *Un cadre pour la **certification en matière de sécurité des Technologies de l'Information et de Communication (TIC)***
- *Une recommandation **pour une intervention coordonnée** en cas de cyber incident majeur affectant plusieurs États membres*
- *Une communication orientant les États membres sur la manière la plus efficace de **mettre en œuvre la Directive SRI** adoptée en 2016*
- *La création future **d'un réseau européen de compétences et de recherche dans le domaine de la cyber sécurité** "*


Renforcer la résilience de l'UE aux cyberattaques
Créer une cyberdéfense efficace pour l'UE
Cybersecurity Act
Communication
Recommendation
ENISA renforcée
Cadre européen de certification de cybersécurité
Mise en œuvre de la Directive SRI
Intervention d'urgence rapide - Fonds d'intervention d'urgence pour la cybersécurité & mécanisme d'opération
Réseau de compétences en cybersécurité avec un centre européen de recherche en cybersécurité
Renforcer la base de compétences en cybersécurité au niveau de l'UE, améliorer la cyber-hygiène et la sensibilisation
Identifier les acteurs malveillants
Intensifier les poursuites judiciaires de la cybercriminalité
Intensifier la coopération public-privé dans la lutte contre la cybercriminalité
Intensifier les politiques et réponses diplomatiques
Développer la dissuasion grâce aux capacités de défense des États membres

Promouvoir la cyber-hygiène la sensibilisation à la cybersécurité

Une coopération stratégique et un échange d'information permanent

Directive sur la Sécurité des Réseaux et de l'Information (SRI) 2016	Paquet «cybersécurité» (Blueprint)
– **Un «groupe de coopération» volontaire** • *Représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)* – **Le réseau CSIRT** • *Computer Security Information Response Team* – **Stratégie nationales adoptées par les Etats Membres** • *Opérateurs de Services Essentiels* • *Fournisseurs de Services Numériques*	– **Un mécanisme de réponse opérationnelle** • *Fixant les objectifs et les modalités de la coopération entre les États membres et les institutions de l'Union européenne pour répondre efficacement* • *Cyber incident majeur affectant plusieurs États membres* • *Intégration de la cybersécurité dans les mécanismes actuels de gestion des crises*

Des campagnes de sensibilisation à la cybersécurité

- **Campagnes de sensibilisation** lancées par les Etats Membres et soutenus par les entreprises avec **des formations** pour leurs employés

- **Le mois de la cybersécurité** organisé par l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information (**ENISA**)

  - **300 activités** axées sur la cybersécurité partout en Europe qui seront amplifiées
  - *Un défis européen réunissant des jeunes talents*
  - *Un projet de CyberEurope 2018 testant notre coopération inter-gouvernementale*

Les habitudes de cyber-hygiène

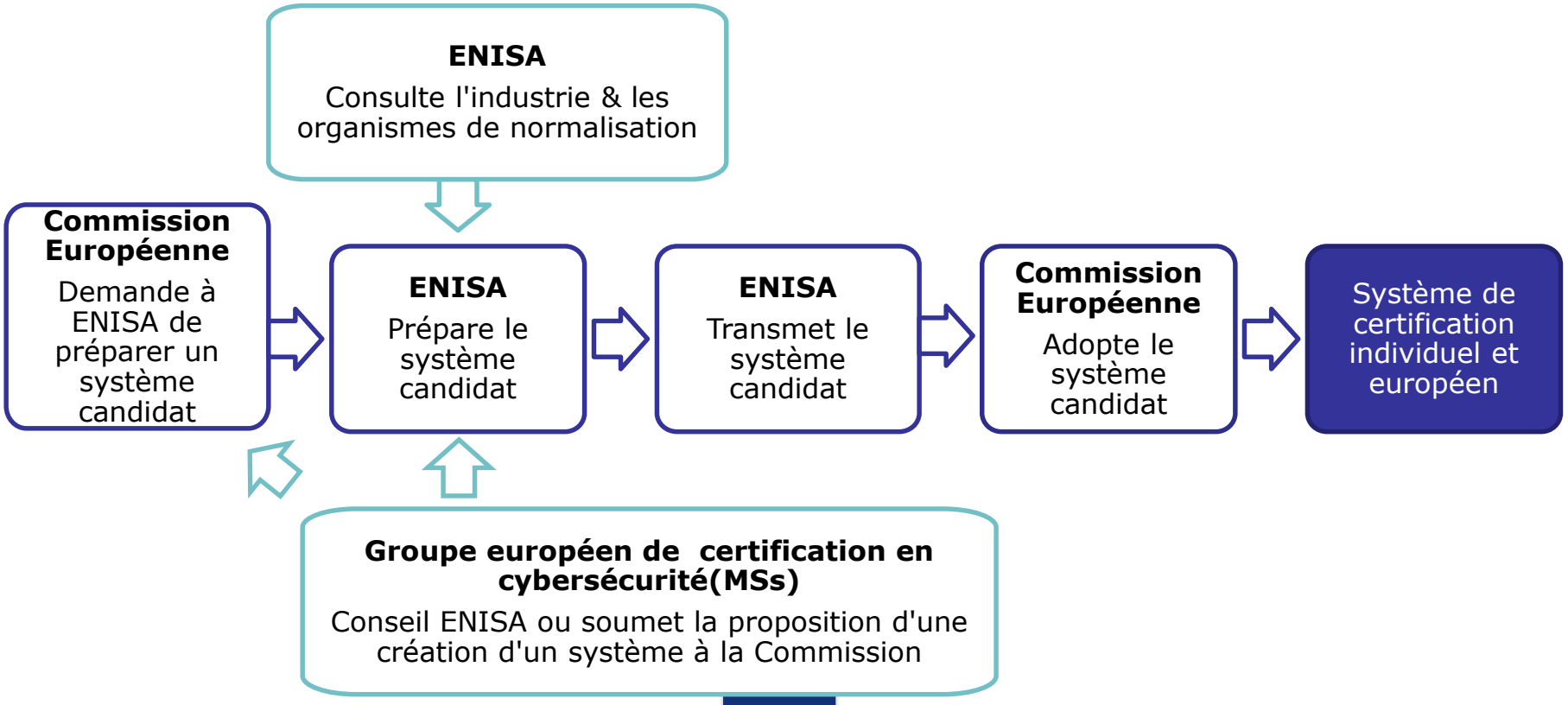
- Un soutien aux **utilisateurs** (particuliers, entreprises et administrations publiques)
- Des outils permettant d'**agir en ligne de manière responsable**
- **Une coopération avec l'industrie**

Le cadre européen de certification

Et l’approche de «sécurité dès la conception»

Notre proposition

*La création d'**un cadre européen de certification de cybersécurité** pour permettre la création de systèmes de certification individuels pour les produits et services ICT,*
valable partout dans l'UE et sur une base volontaire



Conclusion

*La réussite d'**une cybersécurité solide et robuste** demande la coopération de toutes les parties prenantes*

***Un gain de temps et d'argent pour les entreprises** grâce à **un cadre unique de certification européenne**, valide dans tous les Etats Membres*

*Des décisions d'achat éclairées pour les utilisateurs qui pourront compter sur **des produits des Technologies de l'Information et des Communications plus sûrs***

***Une situation "gagnant-gagnant"** pour tous les agents du marché, les citoyens et les gouvernements*