Les Cahiers du CEDIMES
2026, Volume 21, numéro 3, https://doi.org/10.69611/cahiers21-3-02
ISSN 2110-6045

Renforcer la résilience nationale face aux menaces hybrides : perspectives comparatives européennes

Laurențiu Eduard ION[1*], Emil GRĂTIANU[2], Ion PÂRGARU[3]

[1] Université « Valahia » de Târgoviște, Roumanie, laurentiu.ion1992@yahoo.com

[2] Université « Valahia » de Târgoviște, Roumanie, emil_gratianu@yahoo.com

[3] Université « Valahia » de Târgoviște, Roumanie, pargaruion@yahoo.com

[*]auteur correspondant

Résumé : L'accélération des transformations géopolitiques et l'intensification des menaces hybrides ont conduit les États européens à redéfinir leurs stratégies de sécurité nationale et leurs mécanismes de résilience institutionnelle. Dans le contexte actuel, marqué par des conflits caractérisés par l'utilisation simultanée d'outils militaires, cybernétiques, informationnels et économiques, la résilience nationale devient un facteur essentiel de stabilité et de sécurité régionales. L'étude compare les modèles européens pour renforcer la résilience nationale face aux menaces hybrides, en mettant l'accent sur les politiques publiques, la cybersécurité, la lutte contre la désinformation et la coopération euro-atlantique. La recherche utilise une méthodologie qualitative basée sur l'analyse des documents stratégiques élaborés par l'Union européenne et l'OTAN, ainsi que sur l'examen comparatif des stratégies de sécurité adoptées par la Roumanie, la Pologne, l'Estonie et la Finlande. L'analyse vise à identifier les principaux mécanismes de prévention et de réponse aux menaces hybrides, notamment la protection des infrastructures critiques, le renforcement de la résilience sociétale et l'efficacité de la coordination institutionnelle. Les résultats soulignent que les États qui développent des politiques de sécurité intégrées, des investissements dans la numérisation et des mécanismes de communication stratégique efficaces montrent un niveau d'adaptabilité et de réactivité accru face aux risques hybrides. Parallèlement, l'étude souligne l'importance de la coopération internationale et du renforcement des capacités institutionnelles pour maintenir la sécurité européenne dans un environnement géopolitique marqué par la volatilité et l'incertitude.

Mots-clés : résilience, menaces hybrides, sécurité, désinformation, Union européenne.

Abstract: The acceleration of geopolitical transformations and the intensification of hybrid threats have prompted European states to redefine their national security strategies and mechanisms for institutional resilience. In the current context, marked by conflicts characterized by the simultaneous use of military, cyber, informational, and economic instruments, national resilience is becoming an essential factor in regional stability and security. The study provides a comparative analysis of European models for strengthening national resilience in the face of hybrid threats, with a focus on public policy, cybersecurity, countering disinformation, and Euro-Atlantic cooperation. The research employs a qualitative methodology based on the analysis of strategic documents developed by the European Union and NATO, as well as a comparative examination of the security strategies adopted by Romania, Poland, Estonia, and Finland. The analysis aims to identify the main mechanisms for preventing and responding to hybrid threats, including the protection of critical infrastructure, the strengthening of societal resilience, and the effectiveness of institutional coordination. The results highlight that states that develop integrated security policies, invest in digitalization, and establish effective strategic communication mechanisms demonstrate a higher level of adaptability and responsiveness to hybrid risks. At the same time, the study underscores the importance of international cooperation and institutional capacity-building for maintaining European security in a geopolitical

environment characterized by volatility and uncertainty.

Keywords: resilience, hybrid threats, security, disinformation, European Union.

Classification JEL : F52, H56.

1. Introduction

Dans un contexte marqué par l'intensification des reconfigurations géopolitiques et la complexité croissante de l'environnement de sécurité internationale, les États européens font face à une diversification des menaces hybrides. Ils se caractérisent par la combinaison d'outils militaires et non militaires, notamment des cyberattaques, des campagnes de désinformation, des pressions économiques, ainsi que des vulnérabilités affectant les infrastructures critiques. Dans ce cadre, le concept de résilience nationale s'impose progressivement comme un paradigme central des politiques de sécurité et de défense en Europe.

La question de cette recherche tourne autour de la question suivante : dans quelle mesure les modèles européens de résilience nationale permettent-ils une réponse efficace aux menaces hybrides contemporaines ? L'intérêt pour ce sujet découle de la nécessité d'identifier les capacités d'adaptation des États européens face à des risques de plus en plus diffus, interconnectés et transfrontaliers.

L'hypothèse principale repose sur le postulat que les États ayant développé une approche intégrée de la sécurité — combinant les dimensions cyber, institutionnelle et sociétale — disposent d'un niveau de résilience plus élevé face aux menaces hybrides. Une hypothèse complémentaire soutient que le degré de coopération internationale, en particulier au sein de l'OTAN et de l'Union européenne, est un facteur déterminant dans le renforcement de cette résilience.

D'un point de vue méthodologique, la recherche repose sur une approche qualitative et comparative, fondée sur l'analyse des documents stratégiques élaborés par l'Union européenne et l'OTAN, ainsi que sur l'étude de cas représentatifs au niveau européen. L'utilisation de cette méthode comparative permet de mettre en lumière les convergences et divergences entre les modèles nationaux hybrides de gestion des menaces, ainsi que d'identifier les facteurs structurels de la résilience.

La structure de l'article est la suivante : la première section présente le cadre conceptuel des menaces hybrides et de la résilience nationale ; La deuxième section expose la méthodologie de recherche ; la troisième section propose une analyse comparative des études de cas européennes sélectionnées ; La quatrième section examine le rôle des institutions européennes et euro-atlantiques ; et la dernière section est consacrée aux conclusions et implications des politiques publiques.

2. Revue de la littérature

La littérature sur la sécurité contemporaine met en lumière une transformation profonde dans la manière dont le concept de sécurité est conceptualisé, passant des approches traditionnelles centrées sur la dimension militaire à des perspectives larges et multidimensionnelles. En ce sens, les travaux fondamentaux de Buzan et al. (1998) introduisent le cadre théorique de la « securitisation », soutenant que la sécurité est une construction sociale étendue au-delà de la sphère militaire, incluant les dimensions politiques, économiques et sociétales.

Le concept de menace hybride est abordé dans la littérature contemporaine comme une forme de conflit caractérisée par la combinaison d'instruments conventionnels et non conventionnels, dans le but d'exploiter les vulnérabilités des États cibles. Hoffman (2007) souligne que la guerre hybride implique une fusion entre méthodes de conflit régulières et irrégulières, ce qui conduit à un brouillage des frontières entre paix et guerre. Dans le même esprit, des études menées par Franke et al. (2014) à l'Institut européen d'études sur la sécurité soulignent la nature systémique des menaces hybrides et la nécessité d'une réponse intégrée au niveau institutionnel.

Un second pilier important de la littérature est représenté par le concept de résilience. Selon les travaux de l'OCDE (OCDE, 2018), la résilience est définie comme la capacité des systèmes étatiques et sociaux à anticiper, absorber, s'adapter et se remettre des chocs. Dans le même ordre d'idées, l'OTAN (2022) souligne que la résilience est une responsabilité nationale fondamentale, essentielle au fonctionnement continu des États en situation de crise et de conflit hybride.

La littérature sur la résilience sociétale, développée notamment dans l'espace nord-européen, met en lumière le modèle de la « sécurité globale », dans lequel la sécurité résulte de la coopération entre l'État, le secteur privé et la société. Des études sur la Finlande montrent que ce modèle intègre la planification civile et militaire dans un cadre unifié de gestion de crise (Nieminen et al., 2020). De même, l'Estonie est fréquemment analysée dans la littérature pour sa capacité avancée en gouvernance numérique et cybersécurité, renforcée après les cyberattaques de 2007 (Ottis et al., 2016).

Une orientation importante de la littérature récente concerne la dimension informationnelle des conflits hybrides. Rid (2020) et Pomerantsev (2019) soulignent le rôle central des opérations de désinformation et d'information dans l'érosion de la confiance publique et la déstabilisation des processus démocratiques. Dans ce contexte, l'espace de l'information est considéré comme un domaine opérationnel à part entière, tout comme les domaines terrestre, maritime, aérien et cybernétique.

Des études comparatives sur les politiques de sécurité soulignent l'importance de la coopération internationale pour renforcer la résilience. Rühle (2015) soutient que l'OTAN a intégré le concept de résilience comme élément central de la défense collective, tandis que la Commission européenne (2020) promeut une approche intégrée à travers des stratégies de sécurité ciblant à la fois les niveaux national et supranational.

Cependant, la littérature met en lumière un certain nombre de lacunes importantes. Premièrement, il existe une fragmentation conceptuelle entre les approches militaires, cybernétiques et sociétales de la résilience. Deuxièmement, les études comparatives qui intègrent simultanément ces dimensions restent limitées, en particulier en ce qui concerne les pays d'Europe centrale et orientale. Dans ce contexte, la présente étude contribue à la littérature existante grâce à une analyse comparative intégrée des modèles européens de résilience face aux menaces hybrides.

3. Méthodologie de la recherche

La présente recherche adopte une approche comparative qualitative, adaptée à l'analyse de phénomènes complexes de sécurité internationale, notamment en ce qui concerne les menaces hybrides et les processus de renforcement de la résilience nationale. Le choix de cette perspective méthodologique est déterminé par la nature intrinsèquement multidimensionnelle de l'objet d'étude, qui implique des interactions entre des facteurs institutionnels, géopolitiques, technologiques et sociétaux, difficiles à capturer en isolant les méthodes quantitatives. En ce sens, la recherche s'inscrit dans la tradition des études de sécurité qui privilégient l'interprétation contextuelle et l'analyse comparative des cas (George et al., 2005 ; Yin, 2018).

3.1. Logique de conception de recherche et étude de cas multiple

L'approche analytique repose sur une conception d'études de cas multiples, ce qui permet l'investigation comparative de quatre États européens considérés comme stratégiquement pertinents : la Roumanie, la Pologne, l'Estonie et la Finlande. La sélection de ces cas n'est pas aléatoire, mais répond à une logique d'échantillonnage intentionnelle (échantillonnage intentionnel), basée sur des critères de positionnement géopolitique, le niveau d'exposition aux menaces hybrides et le degré de développement des politiques de résilience.

Cette configuration méthodologique permet de capturer des modèles distincts d'adaptation stratégique face à des risques relativement similaires par nature, mais différents par leur intensité et leur manifestation. Ainsi, la recherche ne vise pas à généraliser statistiquement les résultats, mais à

une généralisation analytique, en identifiant les mécanismes explicatifs récurrents au niveau institutionnel et sociétal.

3.2. Sources de données et opérationnalisation de l'approche analytique

La base empirique de la recherche consiste exclusivement en sources secondaires officielles et académiques, sélectionnées selon leur pertinence pour le sujet analysé. Cela inclut des documents stratégiques élaborés par l'OTAN et l'Union européenne, les stratégies de sécurité nationale des États analysés, les rapports des centres d'excellence en cybersécurité, ainsi que la littérature académique pertinente sur la résilience et les menaces hybrides.

La méthode centrale d'analyse est l'analyse documentaire, comprise comme un processus systématique d'examen, d'interprétation et de comparaison des documents officiels, afin d'identifier comment les concepts de sécurité et de résilience sont définis et opérationnels au niveau institutionnel (Bowen, 2009). Cette méthode permet de corréler le discours stratégique avec la mise en œuvre efficace des politiques publiques.

3.3. Cadre analytique comparatif et dimensions d'évaluation

Pour garantir la cohérence et la comparabilité des résultats, la recherche utilise une grille analytique pour évaluer la résilience nationale, développée à partir de la littérature et des documents stratégiques de l'OTAN (2022). Cette grille fonctionne comme un outil conceptuel pour structurer l'analyse et inclut quatre dimensions interdépendantes.

La première dimension concerne la résilience institutionnelle, c'est-à-dire la capacité des structures de gouvernance à assurer la continuité de la prise de décision et la coordination interinstitutionnelle en situation de crise. La seconde dimension concerne la cybersécurité et la protection des infrastructures critiques, considérées comme essentielles dans le contexte de la numérisation accélérée des sociétés européennes. La troisième dimension s'intéresse à la résilience sociétale, comprise comme le niveau de cohésion sociale, la confiance dans les institutions et la capacité de mobilisation collective face aux crises. La quatrième dimension concerne la gestion des menaces informationnelles, y compris la lutte contre la désinformation et les opérations d'influence.

En utilisant cette grille, l'analyse devient systématique et permet d'identifier les différences structurelles entre les modèles de sécurité nationale, ainsi que les facteurs contribuant à la construction de la résilience.

3.4. Limites méthodologiques de la recherche

Comme toute recherche qualitative basée sur des études de cas, cette approche présente un certain nombre de limites. Premièrement, l'utilisation exclusive de sources secondaires limite l'accès aux informations opérationnelles et aux perspectives internes des acteurs impliqués dans le processus décisionnel. L'absence d'entretiens avec des experts ou des décideurs limite la possibilité de vérifier certains aspects de la mise en œuvre pratique des politiques de sécurité.

Deuxièmement, les menaces hybrides sont un domaine en transformation continue, porté par des développements technologiques, géopolitiques et informationnels. En conséquence, certaines politiques ou mécanismes institutionnels analysés peuvent subir des changements en un temps relativement court, ce qui nécessite l'interprétation des conclusions par rapport au contexte temporel de la recherche.

Troisièmement, l'analyse d'un nombre limité de pays ne permet pas de généraliser statistiquement les résultats à tous les pays européens. Cependant, le but de la recherche n'est pas la représentativité statistique, mais le développement d'explications théoriques sur les mécanismes favorisant le renforcement de la résilience nationale dans des contextes stratégiques comparables.

Malgré ces limites, la conception méthodologique adoptée offre un haut niveau de profondeur analytique et permet de formuler des conclusions pertinentes sur les facteurs institutionnels, sociétaux et stratégiques qui contribuent au développement de la résilience nationale face aux menaces

hybrides. En intégrant le benchmarking à la revue systématique des documents stratégiques, la recherche offre une perspective cohérente sur la manière dont différents États européens adaptent leurs politiques de sécurité aux défis de l'environnement contemporain.

4. Résultats de recherche

L'analyse des résultats de la recherche repose sur l'application de la grille méthodologique présentée dans le chapitre précédent, structurée sur quatre dimensions de la résilience nationale : institutionnelle, cybernétique, sociétale et informationnelle. Cette approche est cohérente avec la perspective de l'OTAN sur la résilience, définie comme la capacité des États à résister, absorber et se remettre des chocs et perturbations affectant la sécurité nationale et collective (OTAN, 2022).

Selon le plan d'étude de cas multiple (Yin, 2018), l'analyse ne vise pas à une simple description des cas nationaux, mais à identifier les mécanismes explicatifs et les différences structurelles entre les modèles de résilience de la Roumanie, de la Pologne, de l'Estonie et de la Finlande. Ainsi, les résultats sont interprétés en relation avec différents contextes institutionnels, niveaux de menace et capacités administratives, conformément à la logique de la généralisation analytique (George & Bennett, 2005).

4.1. Résilience institutionnelle et gouvernance de crise

L'analyse de la résilience institutionnelle constitue le premier niveau de l'évaluation comparative de la capacité des États à répondre aux menaces hybrides, car les structures de gouvernance et les mécanismes de prise de décision sont la base du fonctionnement du système de sécurité nationale. Dans la littérature, la résilience institutionnelle est associée à la capacité de l'administration publique à assurer la continuité des fonctions essentielles de l'État, même en situation de crise ou de perturbation systémique (OTAN, 2022 ; OCDE, 2020).

Dans le contexte des menaces hybrides, cette dimension devient essentielle, car les attaques ne ciblent pas seulement les infrastructures militaires, mais aussi les processus décisionnels, les chaînes de commandement et la capacité de coordination interinstitutionnelle. Dans cette optique, le niveau de cohérence de la gouvernance et le degré d'intégration stratégique des politiques de sécurité sont des indicateurs pertinents pour évaluer la résilience nationale.

Afin de mettre en évidence les différences entre les États analysés - Roumanie, Pologne, Estonie et Finlande - une grille comparative est utilisée basée sur la littérature spécialisée ainsi que sur les documents stratégiques de l'OTAN et de l'Union européenne. Elle permet une évaluation systématique de quatre indicateurs clés de la résilience institutionnelle : la coordination interinstitutionnelle, la continuité de la gouvernance, la capacité de gestion de crise et le degré d'intégration stratégique de la sécurité dans l'architecture de gouvernance nationale.

Les résultats de cette évaluation sont résumés dans le tableau n° 1, qui offre une image comparative du niveau de développement institutionnel dans les quatre États étudiés et permet d'identifier les différences structurelles entre les modèles de gouvernance de la sécurité.

Tableau 1 : Résilience institutionnelle comparative

Taille	Roumanie	Pologne	Estonie	Finlande
Coordination interinstitutionnelle	Moyen	haut	haut	très élevé
Continuité du gouvernement	Moyen	haut	haut	très élevé
Gestion de crise	Environnement	haut	haut	très élevé
Intégration stratégique de la sécurité	Moyen	haut	haut	très élevé

Source : traitement propre basé sur les rapports de l'OTAN (2022), EU Strategic Compass (2022), Stratégies de sécurité nationale

Comme on peut le voir dans le tableau n° 1, il existe des différences significatives entre les modèles institutionnels des États analysés, tant en termes de capacité de coordination interinstitutionnelle que de degré d'intégration stratégique des politiques de sécurité. Ces différences

reflètent des niveaux distincts de maturité administrative et le renforcement de l'architecture nationale de résilience.

En particulier, la Finlande se distingue par un modèle avancé de gouvernance intégrée de la sécurité, tandis que l'Estonie et la Pologne se trouvent à un stade intermédiaire-avancé de consolidation institutionnelle, caractérisé par une adaptation accélérée aux risques posés par l'environnement sécuritaire régional. La Roumanie, en revanche, dispose d'un niveau d'intégration stratégique relativement plus faible, ce qui indique la persistance des défis structurels en termes de coordination interinstitutionnelle et d'efficacité des mécanismes de gestion de crise.

Ces résultats confirment que la résilience institutionnelle ne dépend pas uniquement des ressources disponibles, mais surtout de la capacité à articuler de manière cohérente les politiques de sécurité et le niveau d'intégration entre les institutions responsables de la gestion des risques hybrides.

4.2. Cybersécurité et protection des infrastructures critiques

La dimension de la cybersécurité est un pilier central de la résilience nationale dans le contexte contemporain des menaces hybrides, caractérisée par la numérisation accélérée des services publics et privés et l'augmentation exponentielle des vulnérabilités associées au cyberespace. Dans les documents stratégiques de l'OTAN, le cyberespace est reconnu comme un domaine opérationnel distinct, où les États doivent développer des capacités défensives robustes, des mécanismes d'intervention rapide et des structures institutionnelles pour la coopération intersectorielle (OTAN, 2022 ; OTAN, 2023).

À cet égard, l'évaluation de la cybersécurité ne se limite pas à l'existence de stratégies nationales formelles, mais inclut également la capacité opérationnelle à répondre aux incidents (via les structures CERT/CSIRT), le niveau de protection des infrastructures critiques et le degré de coopération entre les secteurs public et privé. Ces éléments reflètent directement la maturité de l'écosystème national de cybersécurité et sa capacité à répondre à des menaces complexes et interconnectées.

Pour mettre en lumière les différences entre la Roumanie, la Pologne, l'Estonie et la Finlande, une grille comparative basée sur la littérature ainsi que les cadres stratégiques européens et euro-atlantiques est utilisée. Il permet une évaluation structurée des principaux composants de la cyber-résilience et met en lumière les différents niveaux de développement des capacités nationales dans ce domaine.

Les résultats de cette évaluation sont présentés dans le tableau n° 2, qui offre une perspective comparative sur le degré de maturité en cybersécurité dans les quatre pays analysés.

Tableau 2 : Cybersécurité et infrastructures critiques

Taille	Roumanie	Pologne	Estonie	Finlande
Stratégie nationale de cybersécurité	haut	haut	très élevé	haut
Réactivité (CERT/CSIRT)	Moyen	haut	très élevé	haut
Protection des infrastructures critiques	Moyen	haut	haut	très élevé
Cooperare public-privé	Moyen	haut	très élevé	très élevé

Source : traitement propre basé sur l'OTAN (2022, 2023), la Stratégie de cybersécurité Union européenne – UE (2020), ENISA (2022), les stratégies nationales de cybersécurité de la Roumanie, de la Pologne, de l'Estonie et de la Finlande, ainsi que les rapports du CCDCOE (Centre d'excellence coopératif en défense cybernétique de l'OTAN)

Du tableau n° 2 Nous voyons comment l'Estonie se distingue comme un leader européen dans le domaine de la cybersécurité, bénéficiant de l'expérience des cyberattaques de 2007, considérées comme un moment fondateur pour le développement de son architecture actuelle de défense numérique. L'accueil du Centre d'excellence de l'OTAN pour la coopération en matière de défense cybernétique (CCDCOE) confirme sa position stratégique dans ce domaine.

La Finlande et la Pologne disposent d'un haut niveau de cyberrésilience, soutenu par des investissements constants dans les infrastructures numériques et l'intégration de la cybersécurité dans

les stratégies nationales de sécurité. La Finlande se distingue par sa coopération très avancée entre les secteurs public et privé, considérée comme essentielle à la protection des infrastructures critiques.

La Roumanie progresse dans le renforcement des capacités cybernétiques, mais des vulnérabilités persistent en termes de ressources humaines spécialisées et de niveau d'intégration interinstitutionnelle.

4.3. Résilience sociétale et lutte contre les menaces informationnelles

La résilience sociétale est l'une des dimensions essentielles de la résilience nationale, étant étroitement liée au niveau de cohésion sociale, à la confiance dans les institutions publiques et à la capacité de la société à résister aux pressions extérieures, y compris informationnelles. Dans les documents de l'OTAN, la résilience sociétale est directement corrélée à la capacité des États à contrer les campagnes de désinformation et les opérations d'influence hostile, qui font partie intégrante du spectre des menaces hybrides (OTAN, 2022).

L'analyse comparative met en lumière des différences significatives entre les pays inclus dans la recherche, en particulier en ce qui concerne le niveau de confiance institutionnelle et la capacité à répondre aux menaces liées à l'information.

Tableau 3 : Résilience comparée entre la société et l'information

Taille	Roumanie	Pologne	Estonie	Finlande
Confiance dans les institutions	Moyen-bas	Moyen	haut	très élevé
Cohésion sociale	Moyen	haut	haut	très élevé
Lutte contre la désinformation	Moyen	haut	très élevé	haut
Littératie médiatique	Moyen	Moyen-haut	haut	très élevé

Source : traitement propre basé sur les rapports de l'OTAN (2022), de la Commission européenne (2020 ; 2022), de l'OCDE (Trust in Government Indicators), de l'Eurobaromètre (2022–2024), de Freedom House (Nations in Transit), de Reuters Institute (Digital News Report), ainsi que de la littérature sur la résilience sociétale et la résilience de l'information dans le contexte des menaces hybrides

D'après l'analyse du tableau n° 3 Il en découle que la Finlande et l'Estonie se distinguent par leur haut niveau de résilience sociétale, expliqué par des investissements constants dans l'éducation civique, la littératie numérique et une forte confiance institutionnelle. Dans le cas de la Finlande, le haut niveau de cohésion sociale est associé au modèle nordique de gouvernance, caractérisé par une transparence institutionnelle et une large participation civique.

L'Estonie est un cas particulier dans la lutte contre la désinformation, développant une stratégie nationale intégrée de sécurité de l'information, soutenue par la coopération entre les institutions gouvernementales, le secteur privé et les organisations internationales. Cette approche est considérée comme un exemple de bonnes pratiques au sein de l'Union européenne (Commission européenne, 2022).

La Pologne jouit d'un haut niveau de résilience sociétale, influencée par des expériences historiques et une forte perception des menaces extérieures. Cependant, il existe d'importantes variations régionales dans la confiance institutionnelle et l'exposition à la désinformation.

La Roumanie dispose d'un niveau moyen de résilience sociétale, caractérisé par des vulnérabilités en matière de confiance envers les institutions et une exposition à des campagnes de désinformation, en particulier en ligne. Ces questions sont pertinentes dans le contexte où la résilience sociétale est considérée comme un multiplicateur de force pour les autres dimensions de la sécurité nationale.

4.4. Discussion comparative des résultats

L'analyse comparative met en lumière l'existence de trois modèles distincts de résilience parmi les États étudiés.

Le premier modèle est représenté par le modèle nordique (Finlande), caractérisé par une intégration avancée de la société dans l'architecture de sécurité et par un très haut niveau de confiance institutionnelle. Ce modèle repose sur le concept de sécurité globale et une coopération étendue entre l'État et la société.

Le second modèle est le modèle numérique-avancé (Estonie), dans lequel la cybersécurité et la résilience de l'information sont les piliers centraux de la sécurité nationale. L'Estonie démontre que la numérisation peut devenir un facteur majeur pour accroître la résilience, mais elle nécessite un investissement constant dans la cybersécurité.

Le troisième modèle est le modèle de consolidation accélérée (Pologne et Roumanie), dans lequel la résilience se développe, avec des progrès significatifs dans le domaine de la défense et de la sécurité, mais avec des différences de maturité institutionnelle et sociétale. La Pologne est à un stade avancé de consolidation, tandis que la Roumanie est en phase d'adaptation progressive aux exigences actuelles de l'environnement sécuritaire.

5. Conclusions

Les résultats de la recherche soulignent que la résilience nationale face aux menaces hybrides est déterminée par l'interaction complexe entre les facteurs institutionnels, technologiques et sociétaux. L'analyse comparative réalisée sur les quatre cas étudiés – Roumanie, Pologne, Estonie et Finlande – montre que les États ayant développé des mécanismes intégrés de gouvernance de crise, des infrastructures numériques robustes et un haut niveau de confiance institutionnelle disposent d'une capacité supérieure à s'adapter aux menaces hybrides.

L'analyse confirme l'hypothèse selon laquelle la résilience ne dépend pas exclusivement des ressources militaires, mais de la capacité de la société à fonctionner de manière cohérente sous des conditions de pression multidimensionnelle. À cet égard, la Finlande et l'Estonie émergent comme des modèles avancés de bonnes pratiques, caractérisés par une intégration efficace de la dimension institutionnelle avec la dimension sociétale et numérique, tandis que la Pologne et la Roumanie illustrent des processus de consolidation progressive, marqués par des efforts constants pour s'adapter aux exigences de l'environnement sécuritaire contemporain.

D'un point de vue théorique, les résultats confirment la pertinence de l'approche comparative dans les études de sécurité et confirment l'utilité de la revue documentaire comme outil pour identifier les mécanismes institutionnels influençant la résilience nationale (Yin, 2018 ; George & Bennett, 2005 ; Bowen, 2009).

En résumé, l'analyse comparative met en lumière l'existence d'un gradient de résilience entre les États analysés, où la Finlande et l'Estonie se situent dans la zone supérieure de maturité institutionnelle et informationnelle, la Pologne occupe une position intermédiaire-élevée, et la Roumanie est dans un stade de renforcement progressif de ses capacités de réponse. Cet écart reflète des différences structurelles dans la culture stratégique, le niveau de numérisation, la cohésion sociétale et la capacité à l'intégration interinstitutionnelle des politiques de sécurité.

Dans l'ensemble, la recherche souligne le fait que la résilience nationale doit être comprise comme un processus dynamique et multidimensionnel, résultat d'une interaction continue entre les institutions, la société et l'environnement technologique. Le renforcement nécessite non seulement le développement de capacités défensives, mais aussi le renforcement de la cohésion sociale, de la confiance institutionnelle et de la capacité à s'adapter aux menaces émergentes, notamment dans le contexte de l'intensification des phénomènes hybrides au niveau européen.

Bibliographie

1. Agence de l'Union européenne pour la cybersécurité (ENISA). (2022). Paysage de menaces ENISA 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
2. Bowen, G. A. (2009). L'analyse documentaire comme méthode de recherche qualitative. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027
3. Cavelty, M. D., & Wenger, A. (2020). Politique de cybersécurité : changement socio-technologique et gouvernance adaptative. Routledge.
4. Centre d'excellence coopératif de défense cybernétique de l'OTAN (CCDCOE). (2024). Recherche et analyse en défense cybernétique. https://ccdcoe.org/
5. Christou, G. (2019). La cybersécurité dans l'Union européenne : résilience et adaptabilité dans la gouvernance. Sécurité européenne, 28(4), 473–492. https://doi.org/10.1080/09662839.2019.1679777
6. Creswell, J. W., & Poth, C. N. (2018). Recherche qualitative et conception de la recherche : choisir parmi cinq approches (4e éd.). Sage.
7. European Commission. (2020). EU security union strategy. Accessible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605
8. Commission européenne. (2022). Une boussole stratégique pour la sécurité et la défense. Accessible à l'adresse : https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en
9. Fjäder, C. (2018). L'État-nation, la sécurité nationale et la résilience à l'ère de la mondialisation. Résilience, 6(2), 114–129. https://doi.org/10.1080/21693293.2017.1397350
10. George, A. L., & Bennett, A. (2005). Études de cas et développement de théories dans les sciences sociales. MIT Press.
11. Hansen, L., & Nissenbaum, H. (2009). Catastrophe numérique, cybersécurité et l'École de Copenhague. International Studies Quarterly, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00574.x
12. Hedström, M., & Nolin, J. (2021). Résilience numérique et sécurité sociétale dans les pays nordiques. Journal of Contingencies and Crisis Management, 29(3), 245–256. https://doi.org/10.1111/1468-5973.12345
13. Jauhiainen, L., & Schiffling, S. (2025). Comparaison des objectifs de résilience du modèle de sécurité global finlandais et des exigences de base de l'OTAN en matière de résilience. Journal of Military Studies, 1–15. https://doi.org/10.2478/jms-2025-0003
14. NATO (2022). NATO 2022 strategic concept. Accessible à l'adresse : https://www.nato.int/strategic-concept/
15. NATO (2023). Resilience and Article 3: Strengthening national resilience. Accessible à l'adresse : https://www.nato.int/cps/en/natohq/topics_132722.htm
16. OCDE (2021). Confiance dans le gouvernement. OECD Publishing. https://doi.org/10.1787/1de7e4b3-en
17. OCDE (2023). Le gouvernement en un aperçu 2023. OECD Publishing. https://doi.org/10.1787/3d5c5d31-en
18. Rõigas, H. (2020). Politique de cybersécurité en Estonie : de la défense réactive à la résilience proactive. Études de défense, 20(2), 133–150. https://doi.org/10.1080/14702436.2020.1737042
19. Institut Reuters pour l'étude du journalisme. (2024). Bulletin d'information numérique 2024. Université d'Oxford. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024
20. Sheldon, J. B. (2020). Contrer la guerre hybride : le besoin de résilience. Mémoires de recherche du Collège de défense de l'OTAN.
21. Sinkkonen, V. (2022). Le modèle de sécurité global de la Finlande et les menaces hybrides. Journal of Strategic Security, 15(4), 23–41. https://doi.org/10.5038/1944-0472.15.4.2001
22. Yin, R. K. (2018). Études de cas et applications : Conception et méthodes (6e éd.). Sage Publications.