

Séminaire de l'équipe « Linguistique Computationnelle »

Détection des comportements anormaux dans les réseaux sociaux

Présenté par :

Nour El Houda BEN CHAABENE

Docteure en Informatique de l'Institut Polytechnique de Paris

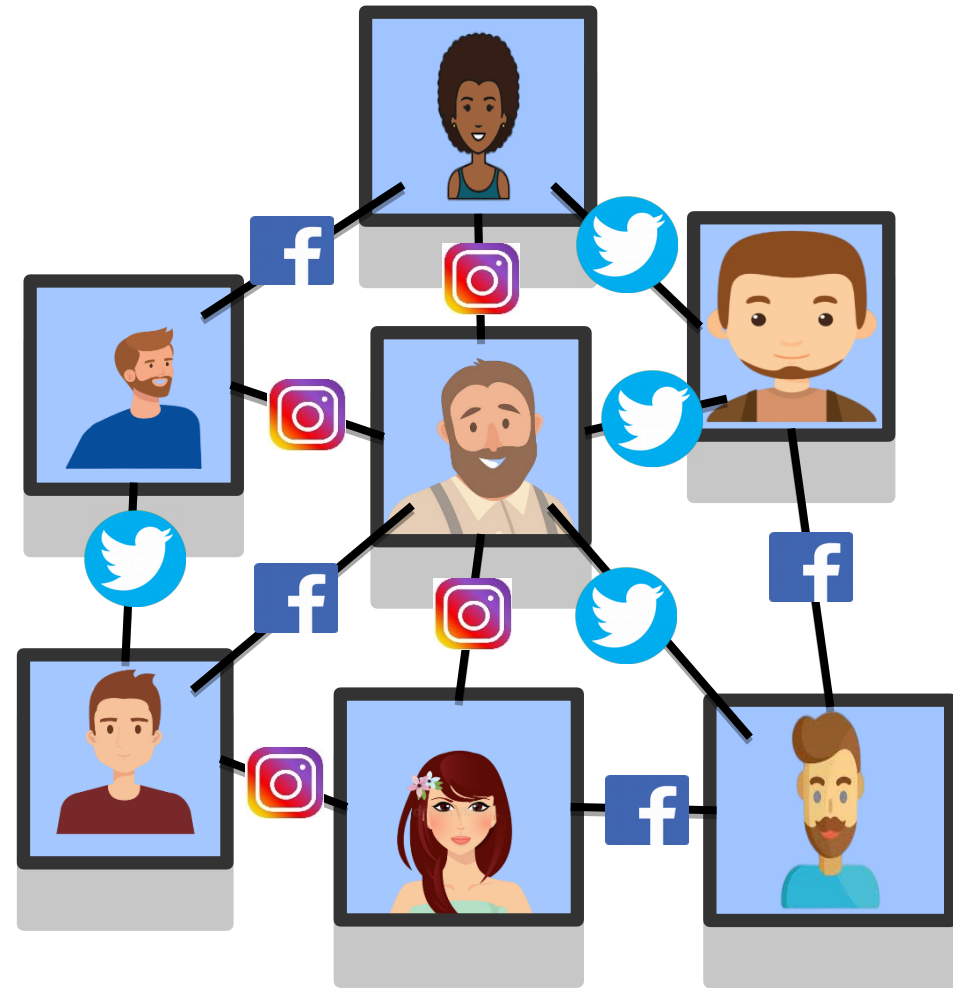
Contexte et Motivation [1/2]

❑ Réseaux sociaux :

- Systèmes complexes du monde réel
- Réseaux d'informations dynamiques
- Disponibilité croissante des données
- Modélisation sous forme de graphes

❑ Différents types d'interaction :

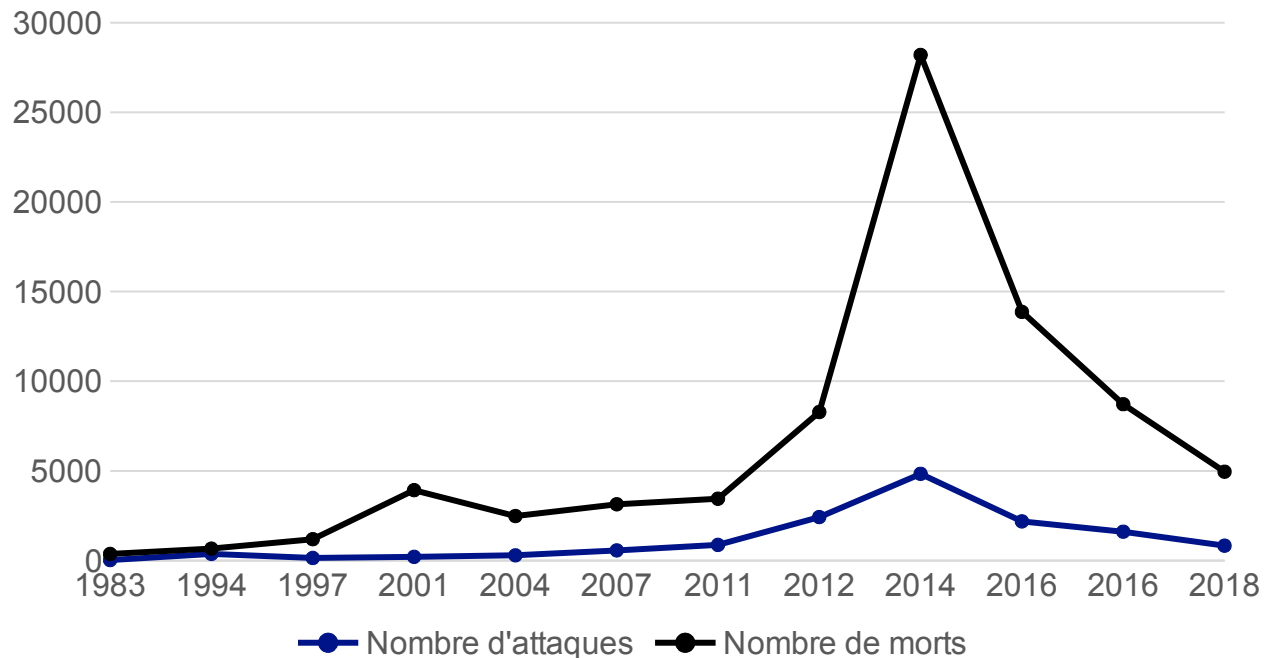
communication, échange des messages,
partage des ressources



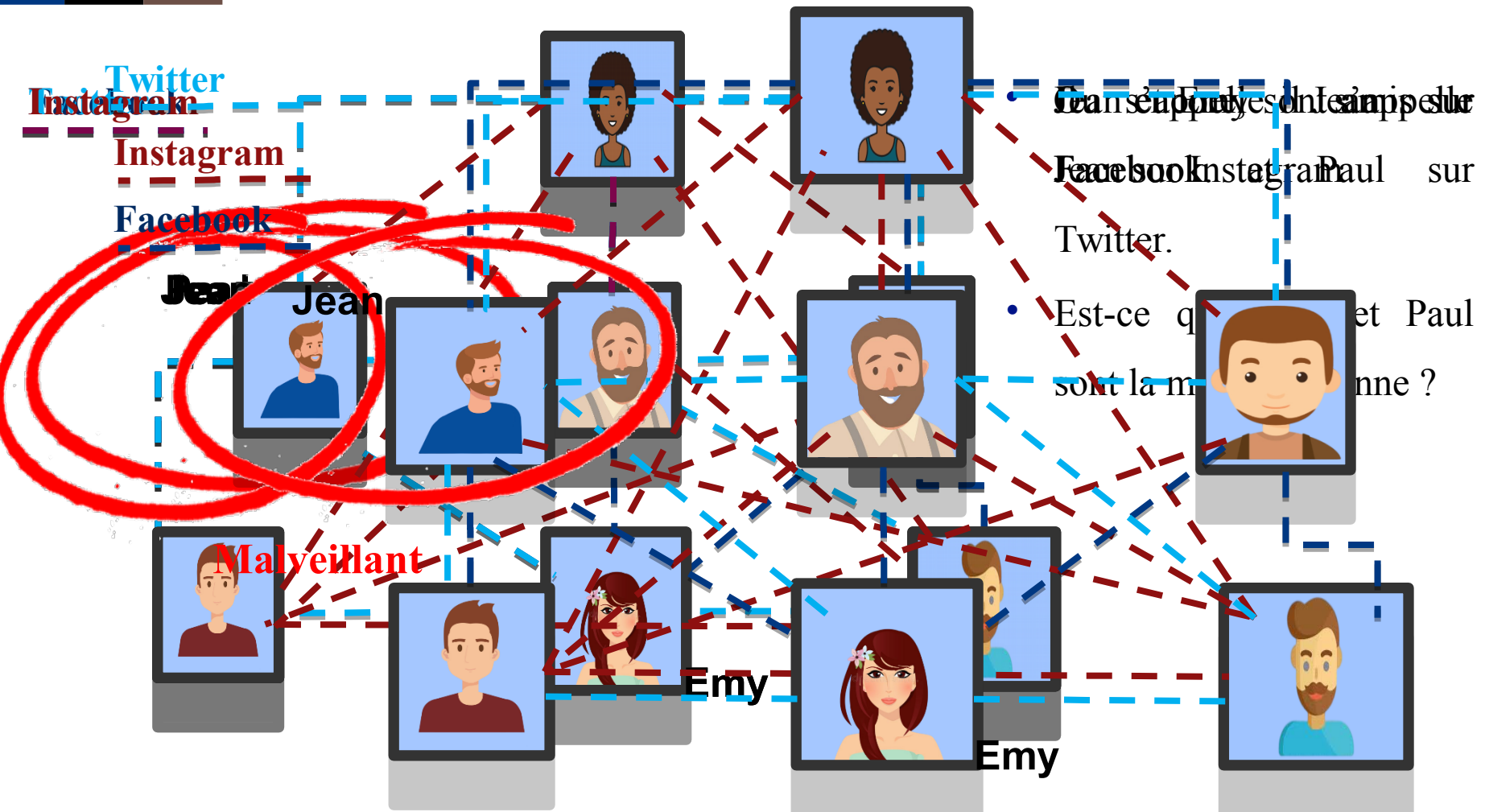
Contexte et Motivation [2/2]

- **Accroissement du nombre des fraudeurs**
- **Multiplication des actes malveillants**

Evolution des attentats terroristes dans le monde



Problématique [1/4]

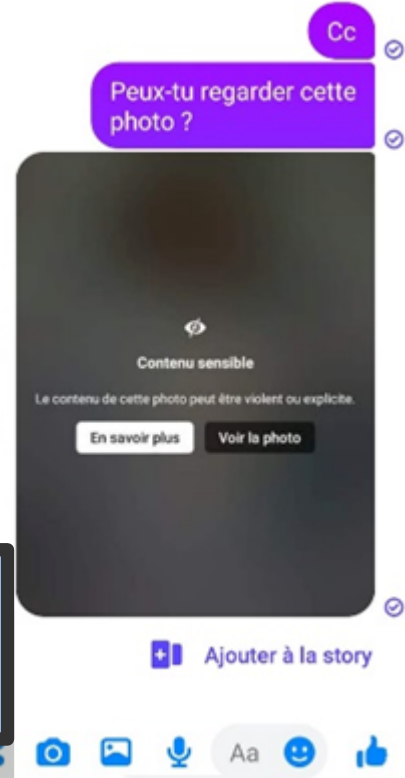
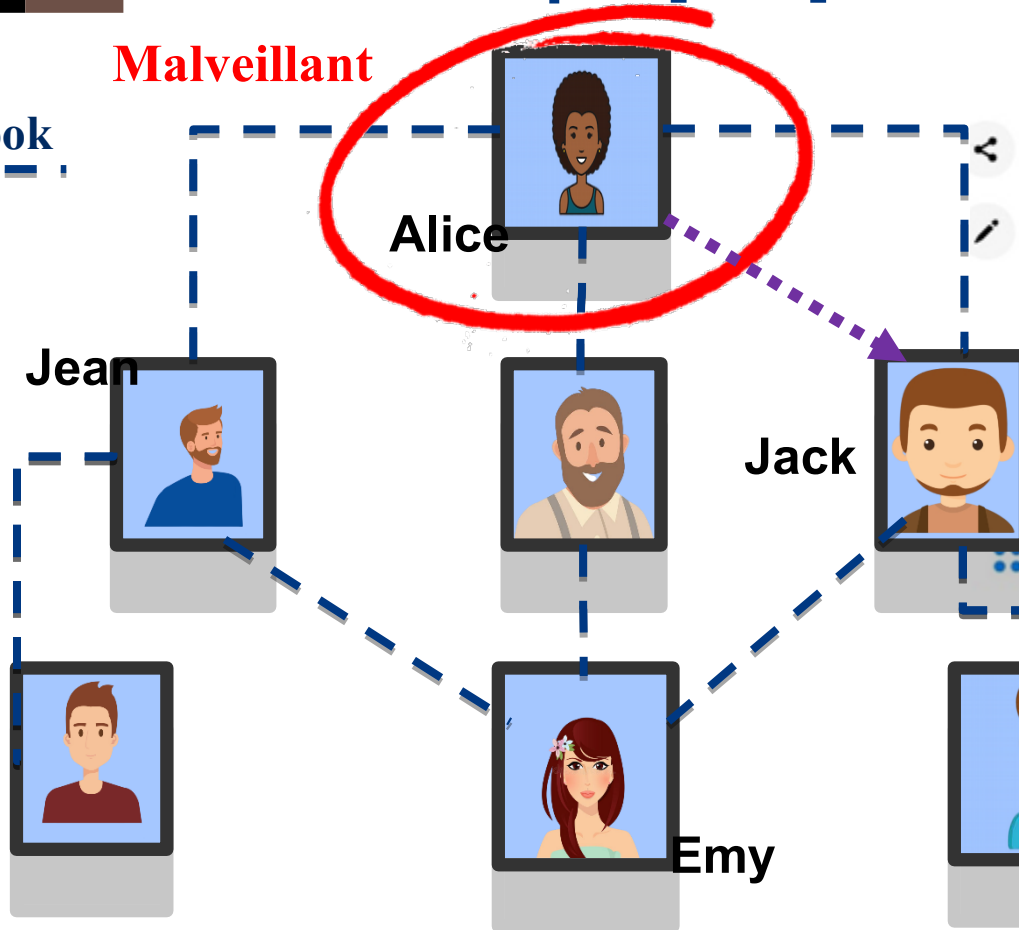


Il faut tenir compte de l'analyse de plusieurs réseaux !

Problématique [2/4]

Malveillant

Facebook

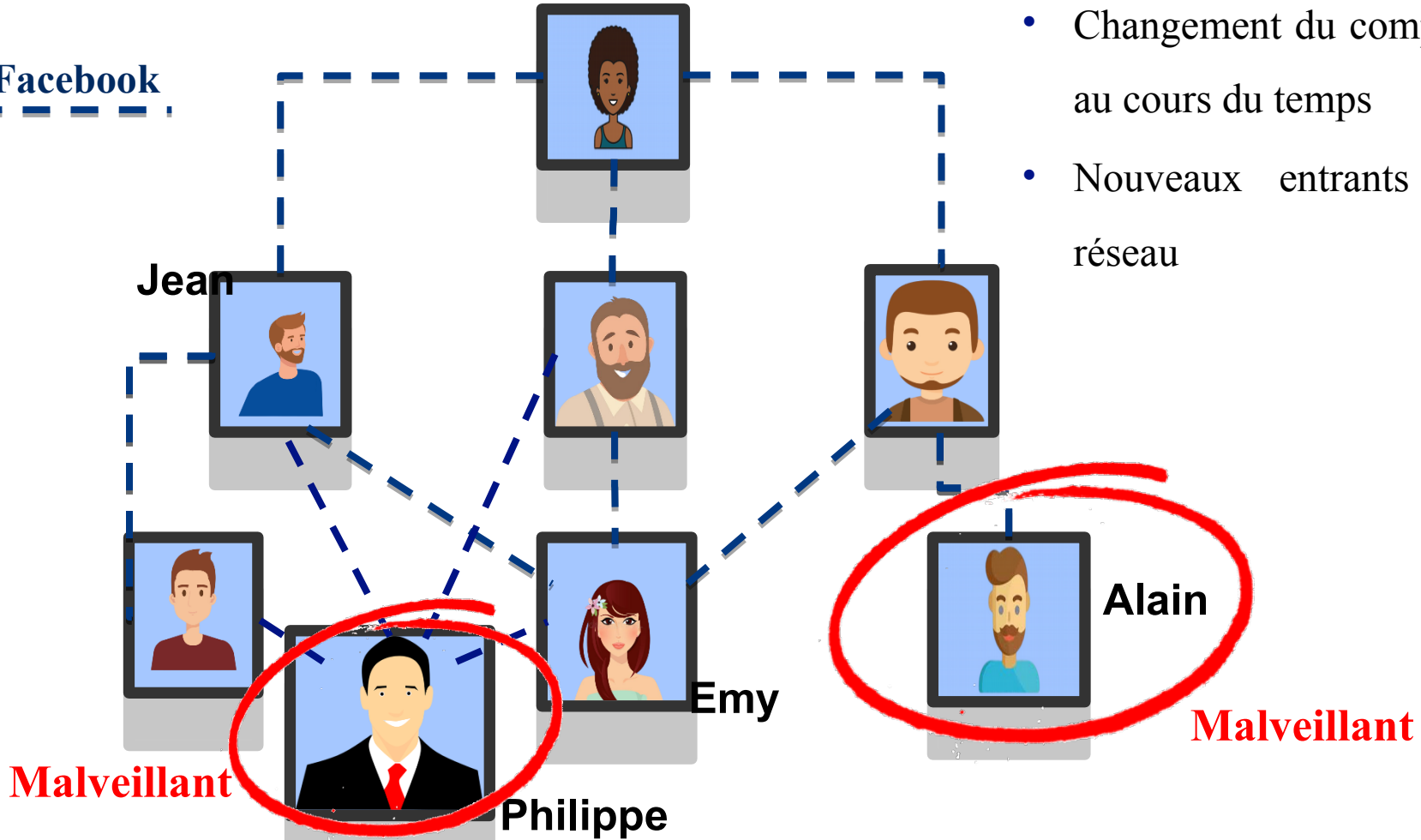


- Rien de violent dans le texte
- Mais, l'image comprend un contenu indésirable

Il faut tenir compte de l'analyse de plusieurs types de données !

Problématique [3/4]

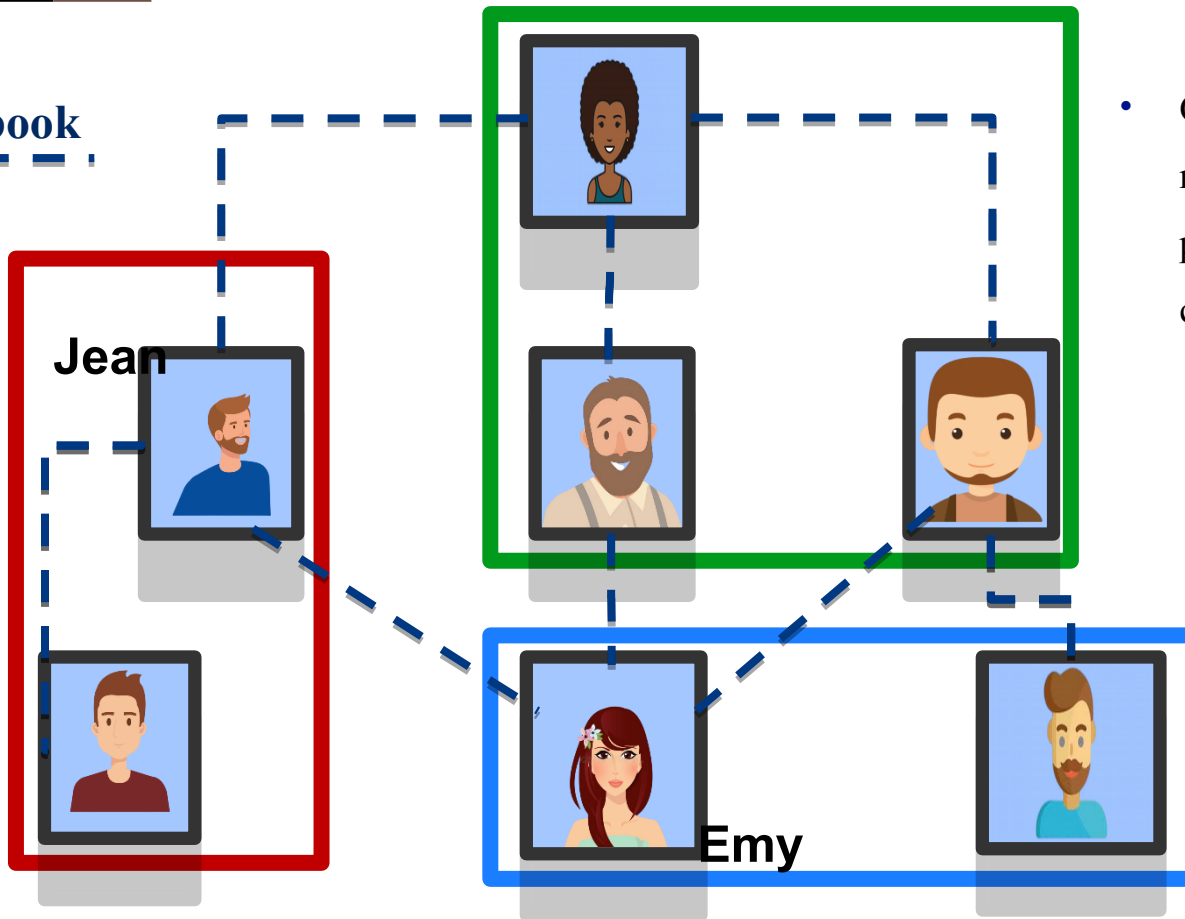
Facebook



- Changement du comportement au cours du temps
- Nouveaux entrants dans le réseau

Il faut tenir compte de l'aspect dynamique du réseau !

Problématique [4/4]



- Construction de communautés regroupant les personnes qui partagent presque les mêmes comportements

Il faut tenir compte de l'aspect communautaire du réseau !

Objectif



Il est nécessaire de trouver les moyens pour élaborer une nouvelle **solution** communautaire, **dynamique**, combinant les propriétés **structurelles complexes multidimensionnelles** pour **analyser** et **traiter** des **données multimodales** afin de détecter les comportements anormaux dans les réseaux sociaux.



Défis

Défis [1/2]

- **La détection des comportements anormaux** est souvent traitée selon l'aspect comportemental ou structurel (topographie d'un seul réseau social) sans considérer la dynamique du réseau social
 - **QR 1** : Y'a-t-il un impact sur la détection des comportements anormaux en combinant la topographie du réseau et les activités d'un individu ?
 - **QR 2** : Comment exploiter les graphes multidimensionnels et les communautés pour la modélisation des comportements anormaux ?
 - **QR 3** : Comment considérer l'évolution des comportements dans le temps ainsi que la dynamique du réseau social ?

Défis [2/2]

- **L'analyse des réseaux sociaux** manipule généralement des données homogènes (texte, image ou vidéo)
 - **QR 4** : Comment exploiter les différents types de données pour garantir l'extraction d'une information pertinente et complète ?
- **L'indisponibilité des données réelles** pour les tests est la difficulté majeure de la plupart des travaux existants en raison de la confidentialité appliquée par les réseaux sociaux.
 - **QR 5** : Comment pouvons-nous extraire des données réelles de plusieurs réseaux sociaux ? Et comment pouvons-nous les synchroniser afin de garantir une modélisation multidimensionnelle ?

1. Travaux connexes

2. Contributions

- Modèle de détection et de prédiction des comportements anormaux sur Twitter
- Méthode de détection des comportements anormaux sur la base de l'analyse des relations dans une structure multidimensionnelle
- Framework hybride de détection des comportements anormaux sur un réseau multidimensionnel utilisant des données multimodales

3. Conclusion et Perspectives

1. Travaux connexes

2. Contributions

- Modèle de détection et de prédiction des comportements anormaux sur Twitter
- Méthode de détection des comportements anormaux sur la base de l'analyse des relations dans une structure multidimensionnelle
- Framework hybride de détection des comportements anormaux sur un réseau multidimensionnel utilisant des données multimodales

3. Conclusion et Perspectives



Travaux connexes

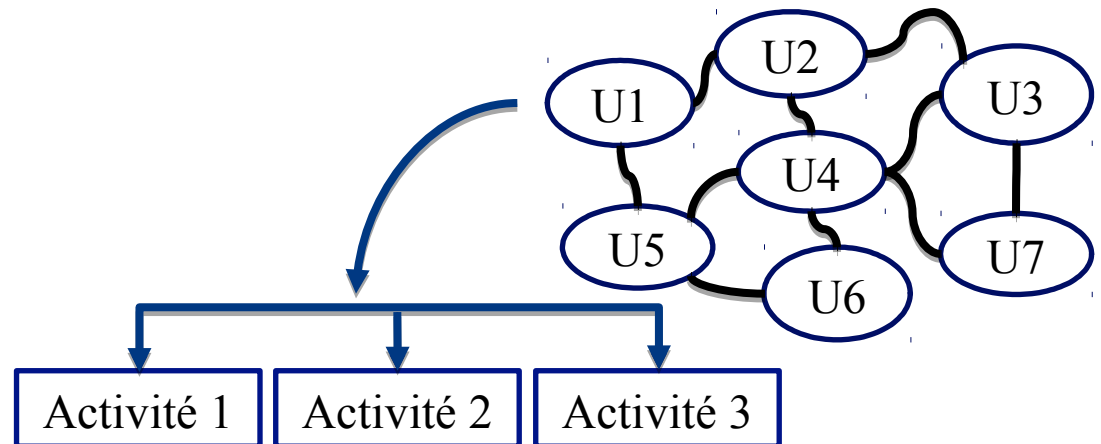
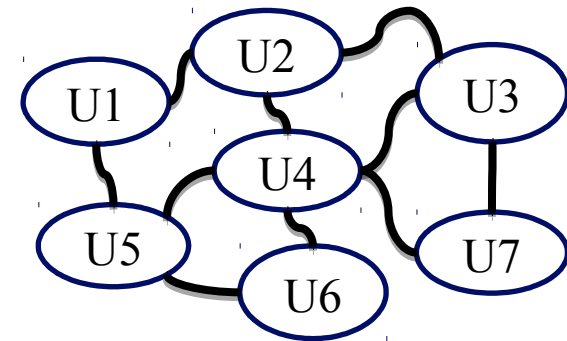
Détection des comportements anormaux

- **Définition :**

« La détection des comportements anormaux est l'identification des anomalies, d'événements ou d'observations rares qui soulèvent des suspicions compte tenu de leurs différences significatives par rapport à la majorité des autres composants du réseau. » [Grubbs, [1969](#)]

Détection des comportements anormaux

- Analyse comportementale
- Analyse structurelle
- Analyse hybride



Détection des comportements anormaux : Analyse comportementale

Méthode	Analyse multidimensionnelle	Structure communautaire	Structure dynamique	Données multimodales
[Anil et al., 2015]	✗	✗	✗	✗
[Chitrakar et al., 2016]	✗	✗	✗	✗
[Shu et al., 2017]	✗	✗	✗	✗
[Yang et al., 2018]	✗	✗	✓	✗
[Lashkari et al., 2019]	✗	✗	✓	✗
[Zamanian et al., 2019]	✗	✗	✗	✓
[Alvari et al., 2019]	✗	✗	✓	✓
	✗	✗	✗	✓

Détection des comportements anormaux : Analyse structurelle

Méthode	Analyse multidimensionnelle	Structure communautaire	Structure dynamique	Données multimodales
[Akoglu et al., 2010]	✗	✗	✗	✗
[Hassanzadeh et al., 2012]	✗	✓	✗	✗
[Fire et al., 2012]	✗	✓	✗	✗
[Rezaiei et al., 2013]	✗	✓	✗	✗
[Li et al., 2017]	✗	✓	✗	✗
[Tutun et al., 2017]	✗	✓	✓	✗
[Chouchane et al., 2017]	✗	✓	✓	✗
[Kalpakis et al., 2019]	✓	✗	✗	✗
[Mahmood et al., 2021]	✓	✗	✓	✗
	✗	✓	✗	✗



Détection des comportements anormaux : Comparaison

- Analyse comportementale
 - Problème binaire : manque de nuances, de résultats intermédiaires
 - Aucune analyse de la structure du réseau : perte de l'information
 - Analyse que des données textuelles
 - Volume des données réduit

- Analyse structurelle
 - Aucune analyse approfondie comportementale des activités

+ Une analyse hybride est plus appropriée !

Détection des comportements anormaux : Analyse hybride

Méthode	Analyse multidimensionnelle	Structure communautaire	Structure dynamique	Données multimodales
[Bhattacharjee et al., 2017]				
[Chen et al., 2018]	✗	✗	✓	✗
	✗	✗	✗	✓

 *Deep learning methods for anomalies detection in social networks using multidimensional networks and multimodal data: a survey, Multimedia System, Springer, 2021.*

1. Travaux connexes

2. Contributions

- Modèle de détection et de prédiction des comportements anormaux sur Twitter
- Méthode de détection des comportements anormaux sur la base de l'analyse des relations dans une structure multidimensionnelle
- Framework hybride de détection des comportements anormaux sur un réseau multidimensionnel utilisant des données multimodales

3. Conclusion et Perspectives



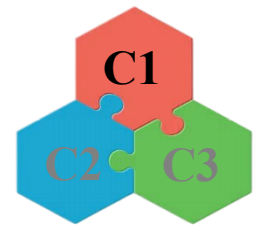
Contributions



Contribution 1

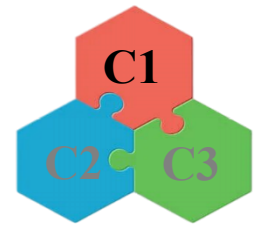


**Modèle de détection et de prédiction
des comportements anormaux sur
Twitter**

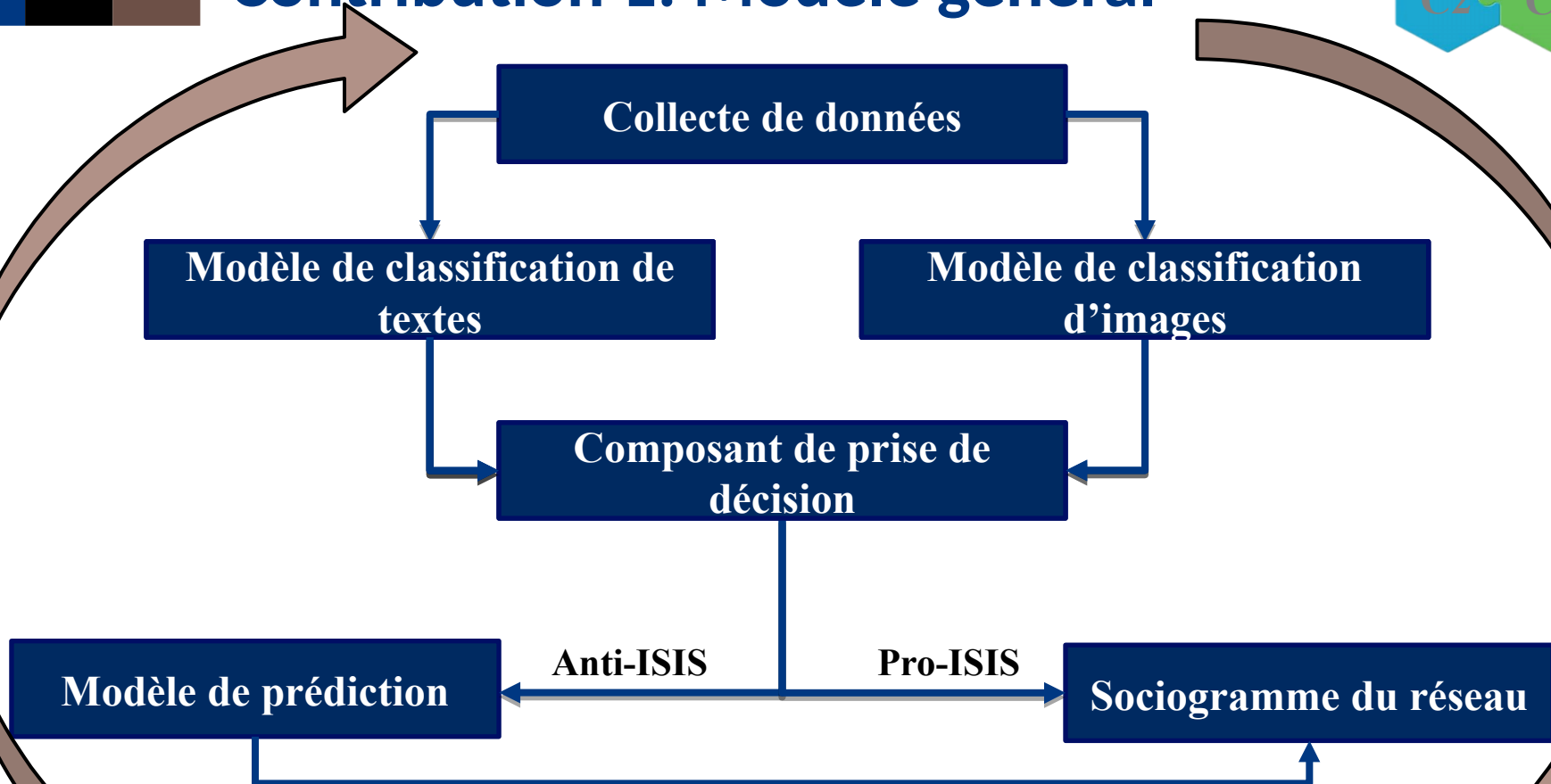


Contribution 1

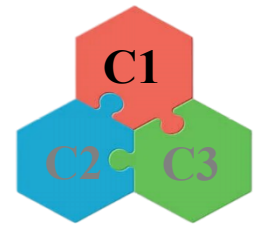
- **QR 1** : Y'a-t-il un impact sur la détection des comportements anormaux en combinant la topographie du réseau et les activités d'un individu ?
 - Analyse comportementale
 - ➔ Analyse structurelle
- **QR 4** : Comment exploiter les différents types de données pour garantir l'extraction d'une information pertinente et complète ?



Contribution 1: Modèle général



ISIS: Islamic State of Iraq and Syria



Contribution 1

Modèle de classification de textes

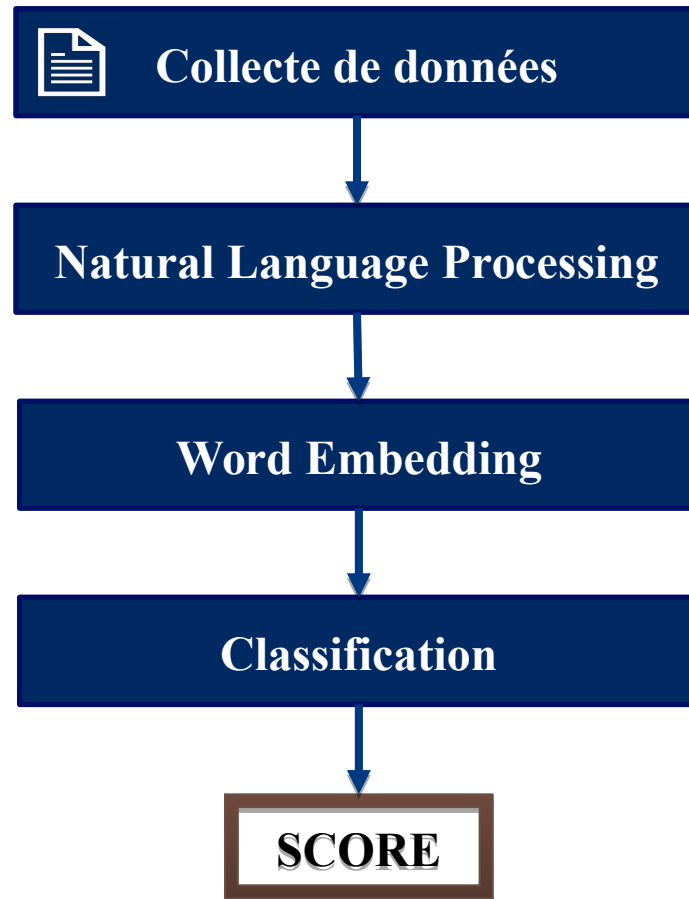
“ISIS is a terrorist organization”

Bi-Gram

ISIS	is	a	terrorist	organization
is	a	terroris	organization	

Tri-Gram

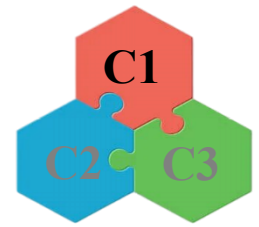
ISIS is	is a	a terrorist	organization
a	terrorist	organization	



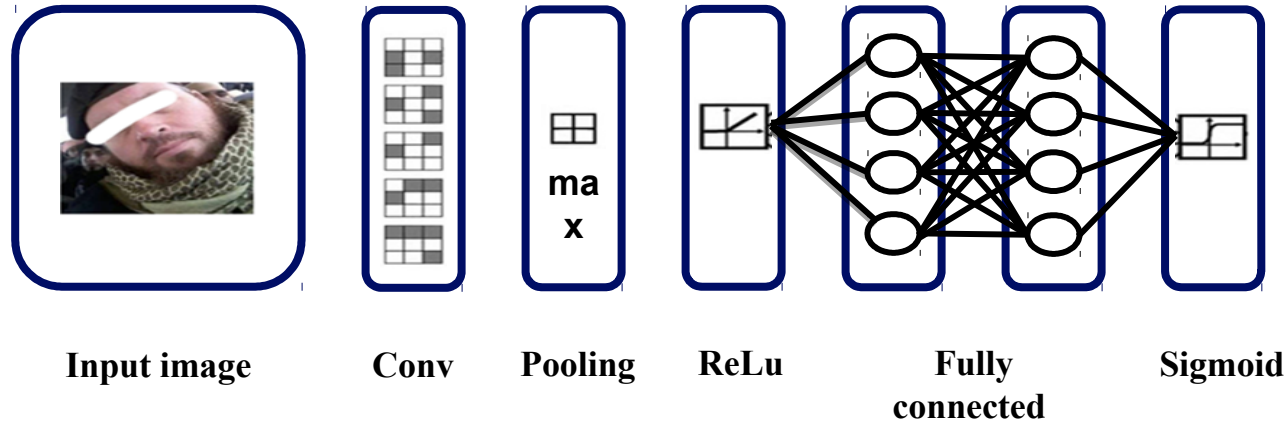
- Analyse morphologique
- Analyse syntaxique
- Analyse sémantique

- Support Vector Machines
- Logistic Regression
- Naïve Bayes

Contribution 1



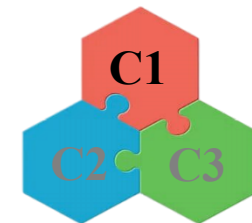
Modèle de classification d'images



Convolutional Neural Network : performance dans la classification des images !!

- Précision
- Temps d'exécution
- Structure spatiale
- Entrée multidimensionnelle

Contribution 1



Composant de décision

- Métriques de classificateurs de texte et d'image
- Taille des ensembles de données collectées



XGBoost

$$S_u = \sum_{i=1}^n \alpha_i \cdot S_{u_i}$$

Modèle de classification de
textes

Modèle de classification
d'images

S1

S2

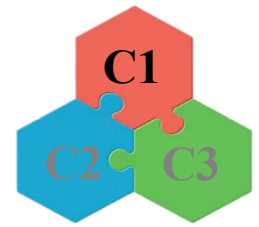
Composant de prise de
décision

$$\begin{cases} S_u \geq \gamma & (Pro - ISIS) \\ S_u < \gamma & (Anti - ISIS) \end{cases}$$



Courbe rappel-précision

Contribution 1



Modèle de prédiction

User/ Ngram	Ngram1	Ngram2	Ngram3	Ngram4
U1	4	3	?	3
U2	2	2	4	2
U3	3	4	5	4
U4	5	2	4	4

Collaborative Filtering

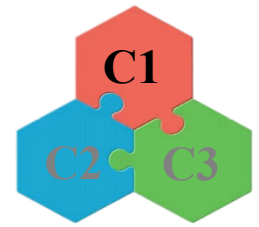
- La similarité entre U1 et tous les autres utilisateurs

Cos	U2	U3	U4
U1	0.65	0.76	0.83

Sum=2.24

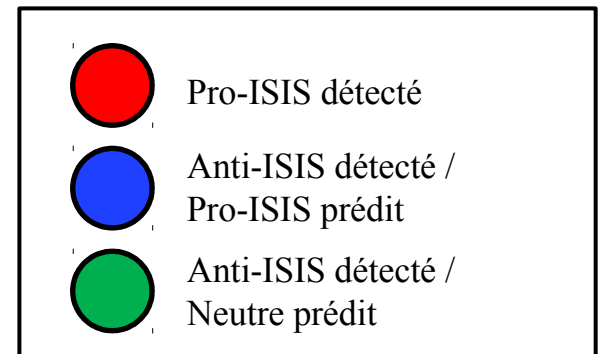
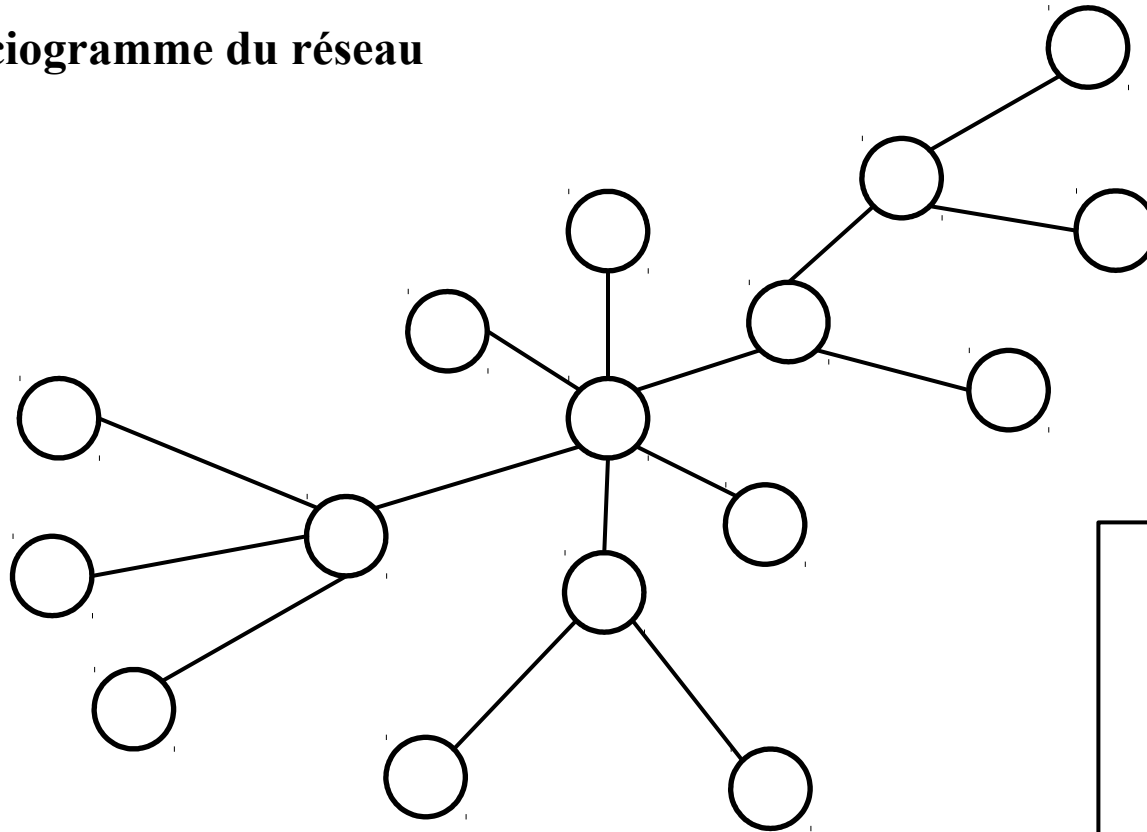
- La moyenne pondérée des notes Ngram3

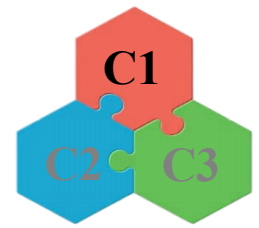
$$? = (0.65*4 + 0.76*5 + 0.83*4) / 2.24 =$$



Contribution 1

■ Sociogramme du réseau

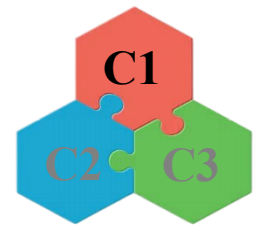




Contribution 1

- **Collecte de données**
 - Données hors ligne : Apprentissage du modèle
 - Données textuelles : Tweets de comptes Twitter bannis
 - Données d'image : Avatars des comptes Twitter bannis et image Google
 - Données en ligne : Test du modèle
 - API Twitter

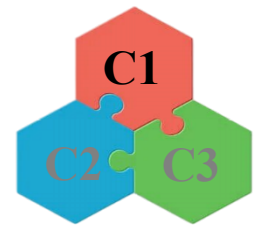
Données	#positives	#négatives
Textuelles	17350	26894
Images	341	308



Contribution 1

- **Résultats expérimentaux**
 - Résultats du modèle de classification de textes

Classifieur	Précision	Rappel	F-score	Temps d'exécution
Support Vector Machine	0,907	0,902	0,904	6h 48min 33secs
Logistic Regression	0,899	0,854	0,875	39secs
Naive Bayes	0,904	0,899	0,900	1min 11secs



Contribution 1

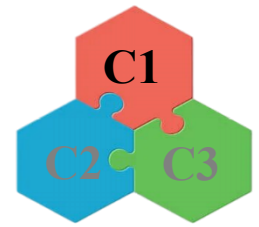
- **Résultats expérimentaux**
 - Résultats du modèle de classification d'images

Classifieur	Précision	Rappel	F-score	Temps d'exécution
CNN ¹	0,761	0,713	0,735	4min 20secs
CNN + DA ²	0,861	0,849	0,853	4min 46secs
CNN + TL ³	0,874	0,867	0,869	8min 34secs
CNN + DA + TL	0,929	0,913	0,920	9min 36secs

1. *Convolutional Neural Network*

2. *Data Augmentation*

3. *Transfer Learning*



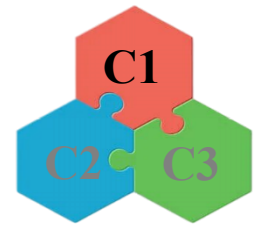
- **Résultats expérimentaux**
 - Résultats du modèle de prédiction

	NMF ⁴			Item KNN ⁵		
	Précision	Rappel	F-score	Précision	Rappel	F-score
Pro-ISIS⁶	0,742	0,613	0,670	0,792	0,655	0,702
Neutre	0,810	0,610	0,695	0,860	0,660	0,746

4. *Non-negative matrix factorization*

5. *Item-Based K Nearest Neighbor*


6. *Islamic State of Iraq and Syria*



Contribution 1

Evaluation

Méthode	Structure dynamique	Données multimodales	F-score
[Anil et al., 2015]	✗	✗	0.6400
Notre modèle	✓	✓	0.7545

 *Applying Machine Learning Models for Detecting and Predicting Militant Terrorists Behaviour in Twitter, IEEE SMC 2021.*

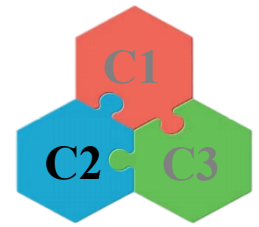


Contribution 2

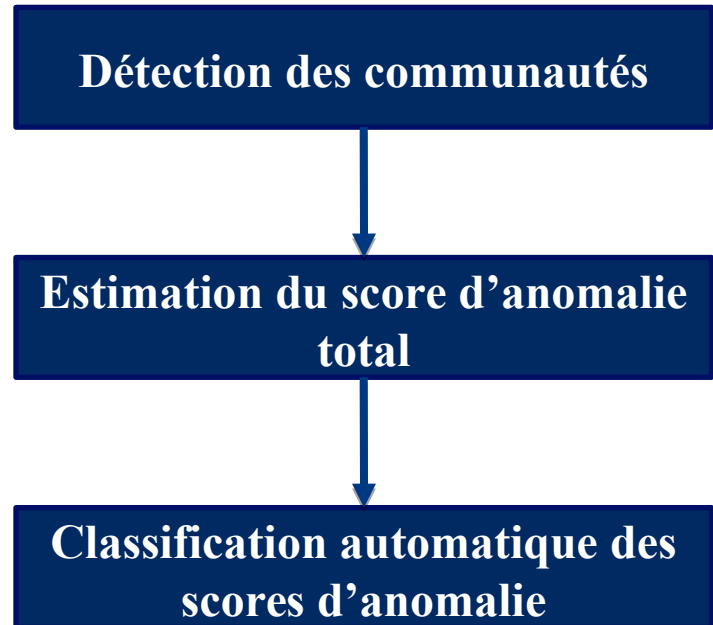


Méthode de détection des comportements anormaux sur la base de l'analyse des relations dans une structure multidimensionnelle

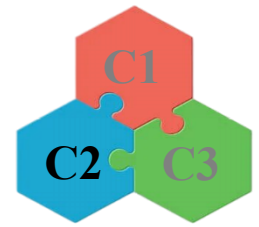
Contribution 2



- **QR 2** : Comment exploiter les graphes multidimensionnels et les communautés pour la modélisation des comportements anormaux ?



Contribution 2

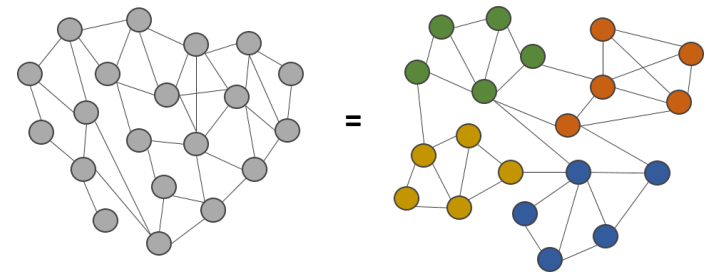


- **Détection des communautés**

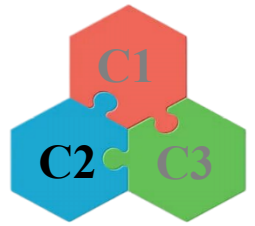
[Hassanzadeh et al., 2012]

- Calcul des communautés d'un graphe

$$C_{Com}(u, v) = \begin{cases} 1, & \text{si } degree(u, v)_{norm} \geq (|u|, |v|)/2 \\ 0, & \text{sinon} \end{cases}$$



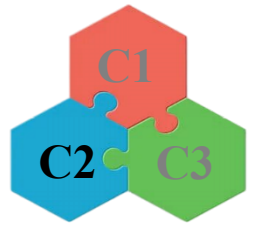
Contribution 2



- Estimation du score d'anomalie total
 - Calcul du score d'anomalie dans une dimension

$$AS(u)_{d_i} = \begin{cases} 1, \text{ si } (u \in Com) \text{ et } (u \text{ influence fortement la construction de la communauté}) \\ 0.5, \text{ si } (u \in Com) \text{ et } (u \text{ n'influence pas la construction de la communauté}) \\ 0, \text{ si } (u \notin Com) \text{ et } (u \in d_i) \end{cases}$$

Contribution 2



- **Estimation du score d'anomalie total**

- Calcul du distance entre ego(u) et ego(v)

$DE(u)_{d_i}$ = nombre de liens sortants possibles de ego(u) vers tous les noeuds du Com(u)

—

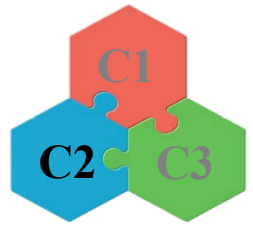
nombre de liens sortants du ego(u) vers ses voisins directs

- Calcul du nombre total de liens directs à partir de ego(u) à ego(v)

$nbc(u)_{d_i}$ = nombre de liens directs entre l'egonet(u) et l'egonet(v)

$nbct(u)_{d_i} = \frac{\sum nbc(u)_{d_i}}{\text{nombre de noeuds formants Com(u)}}$

Contribution 2

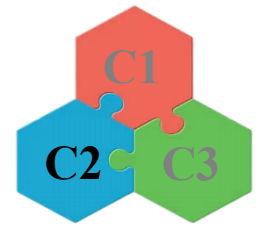


- Estimation du score d'anomalie total
 - Calcul du score d'anomalie dans une dimension

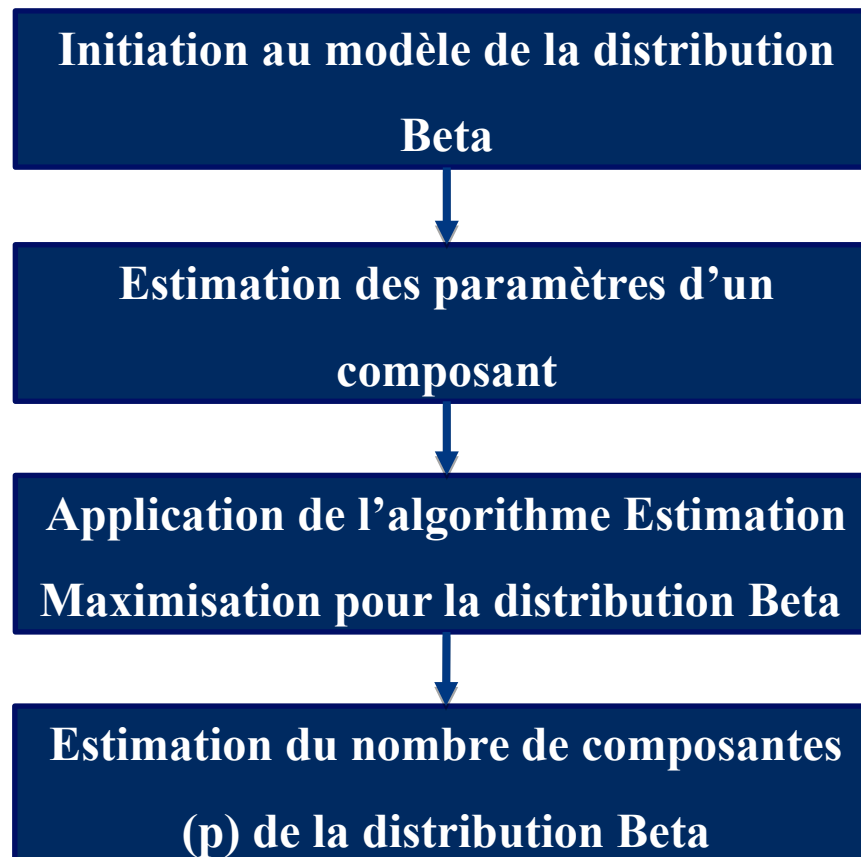
$$A$$
$$AS(u)_{d_i} = \begin{cases} \text{si } (u \in Com) \text{ alors} \\ 1, DE(u) < nbct(u) \\ 0.5, DE(u) \geq nbct(u) \\ 0, \text{sinon} \end{cases}$$

- Calcul du score d'anomalie total

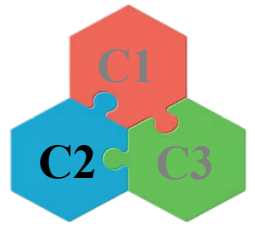
$$AST$$
$$AST(u) = \frac{\sum AS(u)_{d_i}}{\text{nombre de dimensions où } (u) \text{ existe}}$$



- Classification automatique des scores d'anomalie



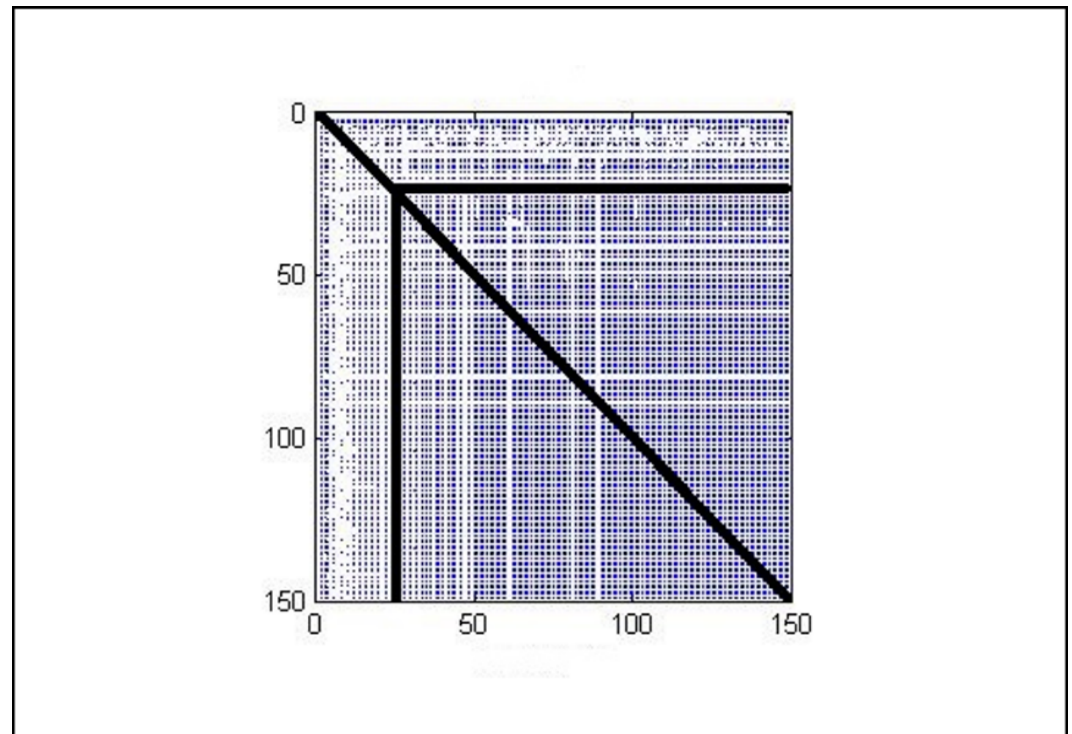
Contribution 2



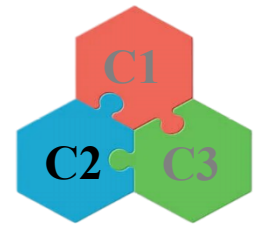
- **Résultats expérimentaux**

- Données de test : 397K de nœuds dont 10K ayant des connexions atypiques

- Matrice d'adjacence du réseau



Contribution 2



Evaluation

Méthode	Structure multidimensionnelle	Structure dynamique	Structure communautaire
[Chouchane et al., 2017]	✓	✗	✗
Notre méthode	✓	✓	✓



Detection of Users' Abnormal Behavior on Social Networks, AINA 2020.

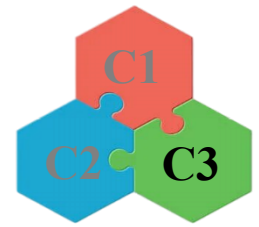


Contribution 3

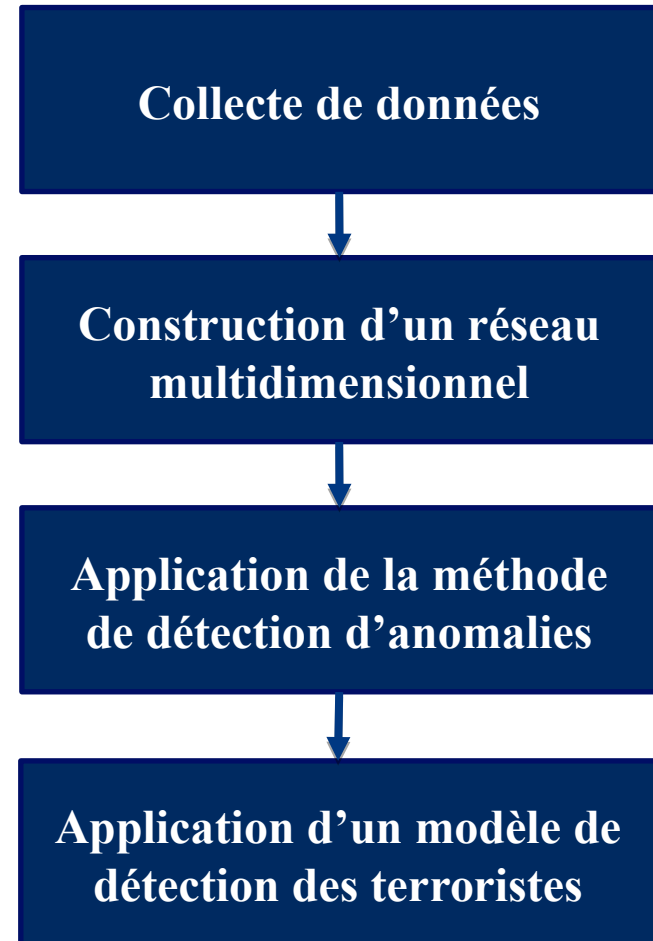


Framework hybride de détection des comportements anormaux sur un réseau multidimensionnel utilisant des données multimodales

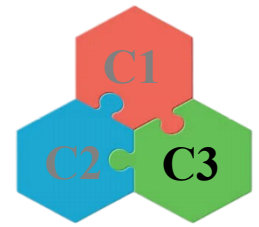
Contribution 3



- **QR 3** : Comment considérer l'évolution des comportements dans le temps ainsi que la dynamité du réseau social ?
- **QR 5** : Comment pouvons-nous extraire des données réelles de plusieurs réseaux sociaux ? Et comment pouvons-nous les synchroniser afin de garantir une modélisation multidimensionnelle ?



Contribution 3



■ Collecte de données: Données d'apprentissage

■ Données hors ligne

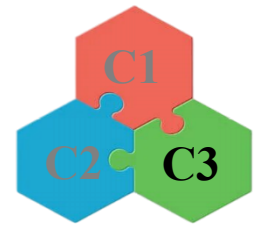
- Données textuelles : Tweets de comptes Twitter bannis (positifs) et Titres de nouvelles GTD (négatifs)
- Données d'image : Google-Image
- Données d'informations générales : PIRUS Dataset

■ Données en ligne

- Facebook Graph API
- Instagram REST API
- Twitter REST API

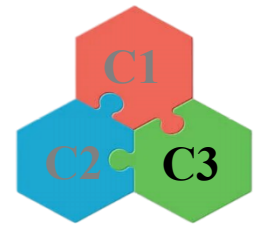
Données	#positives	#négatives
Textuelles	122619	181691
Images	219	314
Infos.Générales	114	126

Contribution 3



- **Collecte de données: Données de test**
 - 180 personnalités publiques
 - Données Facebook : publications qui datent du 24 Février 2016
 - Données Twitter : 200 dernières publications
 - Données Instagram: 20 dernières photos

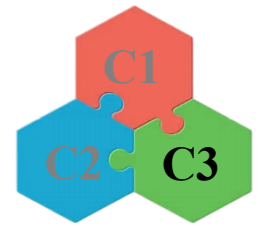
Contribution 3



- **Résultats expérimentaux**
 - Résultats du modèle de classification de textes

Classifieur	Précision	F-score	Temps d'exécution
Support Vector Machine	0,962	0,954	6h 48min 33secs
Logistic Regression	0,972	0,967	39.9secs
Neural Network	0,977	0,971	1min 11secs

Contribution 3



- **Résultats expérimentaux**
 - Résultats du modèle de classification d'images

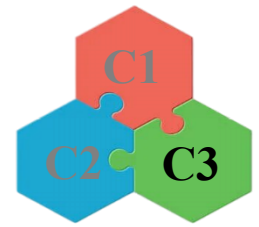
Classifieur	Précision	F-score	Temps d'exécution
CNN ¹	0.763	0.721	3min 50secs
CNN + DA ²	0.778	0.746	4min 12secs
CNN + TL ³	0.829	0.810	8min 48secs
CNN + DA + TL	0,929	0.845	9min 23secs

1. *Convolutional Neural Network*

2. *Data Augmentation*

3. *Transfer Learning*

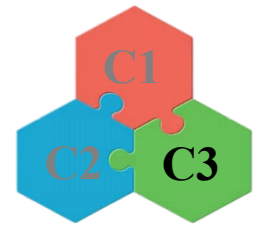
Contribution 3



- **Résultats expérimentaux**
 - Résultats du modèle de classification d'informations générales

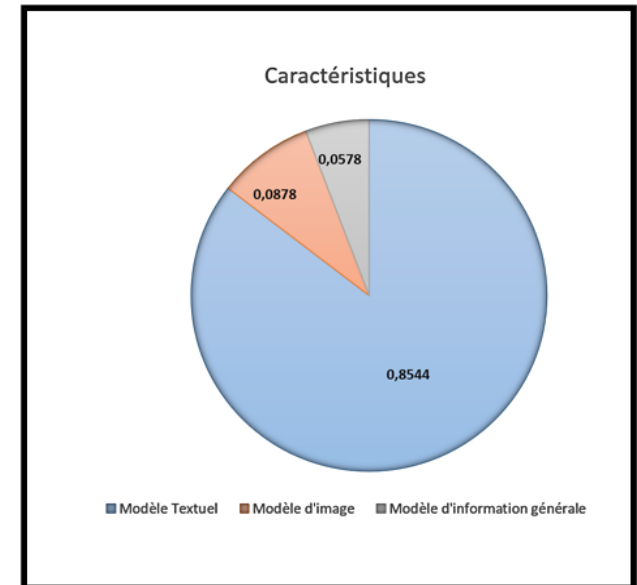
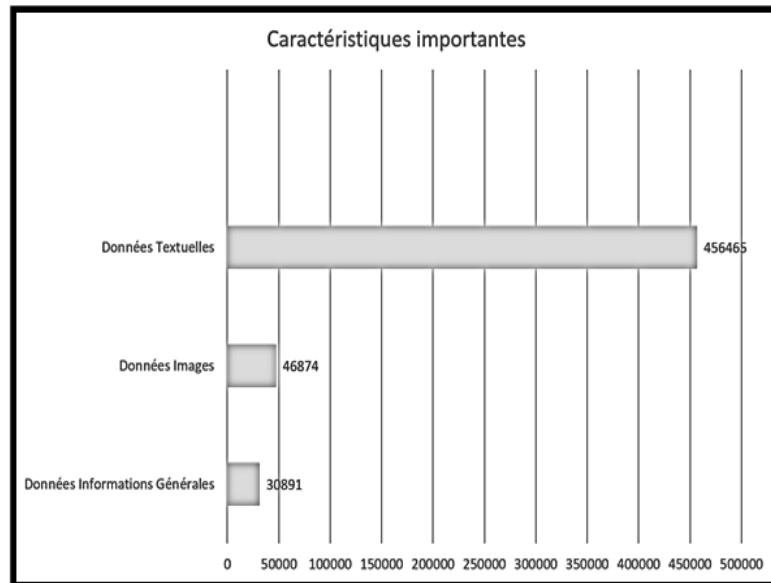
Classifieur	Précision	F-score	Temps d'exécution
Neural Network	0.817	0.832	48.6secs
Logistic Regression	0.765	0.783	5secs
Support Vector Machine	0.830	0.849	7secs

Contribution 3



■ Résultats expérimentaux

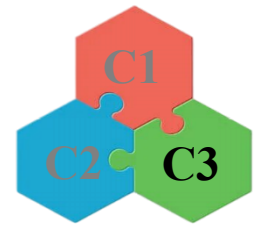
- Calcul des scores totaux de terrorisme: calcul des poids



- Classification des scores totaux de terrorisme : calcul du seuil
 - Augmenter la précision
 - Sans diminuer trop le rappel

≠ 0,0363

Contribution 3



Evaluation

Méthode	Données multimodales			Réseau multidimensionnel	Structure communautaire	Structure dynamique
	Texte	Image	Infos. Générales			
[Alvari et al., 2019]	96.018%	-	91.441%	-	-	-
[Kalpakis et al., 2019]	-	-	-	89.457%	-	84.990%
[Tutun et al., 2017]	93.562%	-	-	-	91.115%	87.714%
Notre framework	98.788%	94.665%	91.889%	95.144%	96.148%	92.322%

 *New Deep Learning Framework for Detecting the Behavior of a Terrorist Group on a Multidimensional Network Using Multimodal Data. Expert Systems With Applications 2022.*

1. Travaux connexes

2. Contributions

- Modèle de détection et de prédiction des comportements anormaux sur Twitter
- Méthode de détection des comportements anormaux sur la base de l'analyse des relations dans une structure multidimensionnelle
- Framework hybride de détection des comportements anormaux sur un réseau multidimensionnel utilisant des données multimodales

3. Conclusion et Perspectives



Conclusion et Perspectives

Synthèse

- Des personnes différentes ont diverses façons pour exprimer le même comportement violent
- La multimodalité et l'ultra-haute dimensionnalité des données structurées et non structurées rendent difficile le développement des méthodes d'exploration de données
- La nature variable des réseaux dans le temps, pour traiter à la fois les nouveaux utilisateurs et les liens entre eux, et ce pour mettre automatiquement à jour les modèles construits



Perspectives [1/2]

- Appliquer les fonctionnalités et les critères abordés dans d'autres domaines liés à l'évaluation des sources tels que la fraude, le spam et les rumeurs.
 - ➔ Génération des réseaux synthétiques avec des caractéristiques du monde réel afin d'étudier leur évolution et leur influence

Perspectives [2/2]

- Etudier le comportement des groupes plutôt que les individus en détectant des changements dans l'évolution de l'activité d'un groupe et en déterminant si cette évolution est relativement conforme ou elle s'écarte de l'évolution normale.
 - ➔ Définition des concepts de base de l'évolution de l'activité des communautés en appliquant des caractéristiques historiques



Merci de votre attention !





- **N.E.H Ben Chaabene**, A. Bouzeghoub, R. Guetari, S. Balti, and H. Hajjami Ben Ghezala. *Detection of users' abnormal behavior on social networks*. In International Conference on Advanced Information Networking and Applications (AINA), Advanced Information Networking and Applications, volume 1151, pages 617–629, **2020**.
- **N.E.H Ben Chaabene**, A. Bouzeghoub, R. Guetari, and H. Hajjami Ben Ghezala. *Deep learning methods for anomalies detection in social networks using multidimensional networks and multimodal data: a survey*. Multimedia Systems, pages 1–11, **2021**.
- **N.E.H Ben Chaabene**, A. Bouzeghoub, R. Guetari, and H. Hajjami Ben Ghezala. *Applying Machine Learning Models for Detecting and Predicting Militant Terrorists Behaviour in Twitter*. In IEEE International Conference on Systems, Man, and Cybernetics (SMC), pages 309–314, **2021**.
- **N.E.H Ben Chaabene**, A. Bouzeghoub, R. Guetari, and H. Hajjami Ben Ghezala. *New Deep Learning Framework for Detecting the Behavior of a Terrorist Group on a Multidimensional Network Using Multimodal Data*. Expert Systems With Applications, **2022**.

Références

- **A. H. Lashkari, M. Chen, and A. A. Ghorbani.** A survey on user profiling model for anomaly detection in cyberspace. *Journal of Cyber Security and Mobility*, 8 :75–112, **2019**.
- **Z. Zamanian, A. Feizollah, N. B. Anuar, L. B. M. Kiah, K. Srikanth, and S. Kumar.** User profiling in anomaly detection of authorization logs. In *Computational Science and Technology*, volume 481, pages 59–65, **2019**.
- **H. Alviri, S. Sarkar, and P. Shakarian.** Detection of violent extremists in social media. In *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, pages 43–47, **2019**.
- **B. Yang, J. Cao, R. Ni, and L. Zou.** Anomaly detection in moving crowds through spatiotemporal autoencoding and additional attention. *Advances in Multimedia*, 2018 :1–8, **2018**.
- **L. Shu, H. Xu, and B. Liu.** Doc : Deep open classification of text documents. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 2901–2906, **2017**.
- **Y. Zhang, W. Chen, C. K. Yeo, C.T Lau, and B. S. Lee.** Detecting rumors on online social networks using multi-layer autoencoder. In *Proceedings of the 2017 IEEE Technology Engineering Management Conference (TEMSCON)*, pages 437—441, **2017**.
- **P. Chitrakar, C. Zhang, G. Warner, and X. Liao.** Social media image retrieval using distilled convolutional neural network for suspicious e-crime and terrorist account detection. In *2016 IEEE International Symposium on Multimedia (ISM)*, pages 493–498, **2016**.

Références

- **B. Mahmood and M. Alanezi.** Structural-spectral-based approach for anomaly detection in facebook network : Iraqi demonstrations case study. *International Journal of Computing and Digital Systems*, 10(1) : 343–351, **2021**.
- **G. Kalpakis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris.** Identifying terrorism-related key actors in multidimensional social networks. In *International Conference on Multimedia Modeling (MMM), MultiMedia Modeling*, pages 93–105, **2019**.
- **A. Chouchane and M. Bouguessa.** Identifying anomalous nodes in multidimensional networks. In *2017 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, pages 601–610, **2017**.
- **Z. Li, D. Sun, R. Zhu, and Z. Lin.** Detecting event-related changes in organizational networks using optimized neural network models. *PloS one*, 12 (11) :1–21, **2017**.
- **A. Rezaei, Z. M. Kasirun, V. A. Rohani, and T. Khodadadi.** Anomaly detection in online social networks using structure based technique. In *Eighth International Conference on Internet Technology and Secured Transactions (ICITST)*, pages 619–622, **2013**.
- **M. Fire, G. Katz, and Y. Elovici.** Strangers intrusion detection - detecting spammers and fake profiles in social networks based on topology anomalies. *ASE Human Journal*, 1(1) :26–39, **2012**.
- **R. Hassanzadeh, R. Nayak, and D. Stebila.** Analyzing the effectiveness of graph metrics for anomaly detection in online social networks. In *Web Information Systems Engineering - WISE 2012*, pages 624–630, **2012**.

Références

- **L. Akoglu, M. McGlohon, and C. Faloutsos.** Oddball : spotting anomalies in weighted graphs. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), Advances in Knowledge Discovery and Data Mining, volume 13, pages 410–421, **2010**.
- **D. Chen, Q. Zhang, G. Chen, C. Fan, and Q. Gao.** Forum user profiling by incorporating user behavior and social network connections. In International Conference on Cognitive Computing (ICCC), pages 30–42, **2018**.
- **S. D. Bhattacharjee, J. Yuan, Z. Jiaqi, and Y. Tan.** Context-aware graphbased analysis for detecting anomalous activities. In 2017 IEEE International Conference on Multimedia and Expo (ICME), pages 1021–1026, **2017**.
- **S. Tutun, M. T. Khasawneh, and J. Zhuang.** New framework that uses patterns and relations to understand terrorist behaviors. Expert Systems with Applications, 78 :358–375, **2017**.
- **A. Anil, D. Kumar, S. Sharma, R. Singha, R. Sarmah, N. Bhattacharya, and R. Sanasam.** Link prediction using social network analysis over heterogeneous terrorist network, volume 12, pages 267–272, **2015**.
- **F. E. Grubbs.** Procedures for detecting outlying observations in samples. Technometrics, 11(1) :1–21, **1969**.