UQAC
Université du Québec
à Chicoutimi

UNE ONTOLOGIE INTÉGRÉE POUR LA GESTION DES INCIDENTS, L'INVESTIGATION NUMÉRIQUE, LA GESTION DES RISQUES ET LA GOUVERNANCE EN CYBERSÉCURITÉ ORGANISATIONNELLE

PAR CHEIKHOU OUMAR DIOP

MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À CHICOUTIMI EN VUE DE L'OBTENTION DU GRADE DE MAÎTRISE ÈS SCIENCES (M. SC.) EN INFORMATIQUE

QUÉBEC, CANADA

RÉSUMÉ

Les organisations dépendent fortement des systèmes d'information pour soutenir leurs activités, mais cette dépendance les expose à des cybermenaces susceptibles d'entraîner des perturbations importantes sur les plans opérationnel, financier et stratégique. Pour faire face à ces menaces, plusieurs cadres normatifs existent en matière de gestion des incidents, d'investigation numérique, d'évaluation des risques et de gouvernance, mais ces cadres sont généralement conçus de façon indépendante, avec leur propre terminologie et leurs propres structures conceptuelles. Cette fragmentation complique l'intégration des connaissances entre ces domaines et limite la capacité à soutenir un raisonnement unifié, et peut engendrer des angles morts lors de la prise de décision.

Les ontologies constituent une approche reconnue pour répondre à ce type de problème, en permettant de formaliser explicitement les concepts d'un domaine ainsi que les relations qui les unissent, et en facilitant ainsi l'interopérabilité sémantique entre cadres hétérogènes. Plusieurs travaux ont déjà proposé des ontologies en cybersécurité, notamment orientées vers le renseignement sur les menaces (par exemple STIX) ou vers les artefacts d'investigation numérique (par exemple UCO), mais ces approches couvrent généralement un domaine spécifique sans intégrer explicitement la gestion des risques ou la gouvernance dans un même cadre sémantique.

Ce mémoire présente comme contribution principale une ontologie intégrée de cybersécurité visant à relier ces différents domaines au sein d'un cadre commun de représentation des connaissances. L'ontologie s'appuie sur un référentiel d'ancrage construit à partir de la norme ISO/IEC 27035, retenue pour son rôle central dans la gestion des incidents et ses liens explicites avec ISO/IEC 27001, et étendu par des correspondances ontologiques vers des concepts issus de la sécurité de l'information, de la gestion des risques, des investigations numériques et de la gouvernance. Elle formalise les relations entre les menaces, les vulnérabilités, les incidents, les preuves numériques, les risques, les contrôles de sécurité et les décisions de gouvernance. Afin de valider l'ontologie proposée, un scénario de cyberattaque a été simulé puis utilisé pour instancier ses concepts et relations. La validation a consisté à évaluer la capacité de l'ontologie à répondre à des questions de compétence mobilisant des connaissances inter-domaines, et à inférer de nouvelles connaissances au moyen d'un raisonneur.

Les résultats montrent que l'ontologie permet de répondre à l'ensemble des questions de compétence définies et que son raisonnement automatique confirme l'absence d'incohérence logique, constituant un cadre de représentation des connaissances pour soutenir une gestion plus intégrée de la cybersécurité organisationnelle.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

APT	Advanced Persistent Threat
CAPEC	Common Attack Pattern Enumeration and Classification
CIA	Confidentiality, Integrity, Availability
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations
CQ	Competency Question
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DMZ	Demilitarized Zone
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ERM	Enterprise Risk Management
GNS3	Graphical Network Simulator 3
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IODEF	Incident Object Description Exchange Format
IPS	Intrusion Prevention System
IRT	Incident Response Team
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MDA	Model-Driven Architecture
NIST	National Institute of Standards and Technology
NORIA-O	Network-Oriented Incident Response and Investigation Ontology
NVD	National Vulnerability Database
OWL	Web Ontology Language
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard

PLS-SEM	Partial Least Squares Structural Equation Modeling
PPS	Packets Per Second
RMF	Risk Management Framework
SAO	Security Attack Ontology
SAVO	Security Asset and Vulnerability Ontology
SCADA	Supervisory Control and Data Acquisition
SDO	Security Defense Ontology
SEM	Structural Equation Modeling
SIEM	Security Information and Event Management
SP	Special Publication
SPARQL	SPARQL Protocol and RDF Query Language
SPIN	SPARQL Inferencing Notation
STIX	Structured Threat Information Expression
SWRL	Semantic Web Rule Language
SYN	Synchronize Sequence Numbers
TIC	Technologies de l'Information et de la Communication
TCP	Transmission Control Protocol
WAN	Wide Area Network
XML	eXtensible Markup Language

DÉDICACE

À mon père et à ma mère,

Je vous dédie ce travail avec une profonde gratitude pour tous les sacrifices, les encouragements et le soutien inconditionnel que vous m'avez apportés tout au long de mon parcours académique. J'espère que vous serez toujours fiers de moi et que ce mémoire constituera une source de satisfaction et de bonheur pour vous.

Je dédie également ce travail à mes frères, mes amis ainsi qu'à tous les membres de ma famille pour leur affection, leur confiance, leurs prières et leur soutien constant durant toutes ces années d'études.

Je dédie également ce travail à la mémoire de mon frère, El Hadj Gora Diop, dont le souvenir demeure vivant dans mon cœur. Qu'ALLAH lui fasse miséricorde, l'accueille dans Son vaste Paradis et lui accorde le repos éternel.

Au Professeur Jonathan Roy, pour son encadrement, sa patience, ses conseils précieux ainsi que la confiance qu'il m'a accordée durant l'ensemble de mes recherches.

À toutes les personnes qui, de près ou de loin, ont contribué d'une manière ou d'une autre à la réalisation de ce document.

Qu'ALLAH leur accorde la santé, la prospérité et les gratifie de Sa miséricorde.

REMERCIEMENTS

Je remercie, en premier lieu, ALLAH pour le courage, la patience, la santé et la force qu'Il m'a accordés afin de poursuivre mes études et de mener à bien ce travail de recherche.

Je tiens à exprimer ma profonde gratitude à mon directeur de recherche, le Professeur Jonathan Roy, pour son encadrement, sa disponibilité, ses précieux conseils ainsi que la confiance qu'il m'a accordée tout au long de cette recherche. Son soutien et ses orientations ont grandement contribué à la réalisation de ce mémoire.

J'adresse également mes sincères remerciements au Professeur Idy Diop et au Professeur Abdou Diop de l'École Supérieure Polytechnique pour leurs enseignements, leurs conseils et leur accompagnement durant mon parcours académique et mes travaux de recherche.

Je tiens aussi à remercier tous les professeurs qui m'ont encadré et transmis leurs connaissances tout au long de mon parcours scolaire et universitaire. Je souhaite adresser une reconnaissance particulière au Professeur Kalidou Barry du CEM de Guéoul, qui m'a profondément marqué depuis mes études dans cet établissement grâce à ses conseils, son soutien et ses encouragements.

Mes remerciements s'adressent également au personnel du Département d'informatique et de mathématique (DIM) de l'UQAC pour son accueil et son accompagnement.

J'exprime aussi ma gratitude au Professeur Souleymane Barry pour son soutien, ses conseils ainsi que pour son aide précieuse lors de mon intégration à la ville de Chicoutimi.

Enfin, je remercie sincèrement ma famille, mes amis et mes proches pour leur soutien constant, leurs prières et leurs encouragements, qui m'ont permis de maintenir un équilibre entre les études et la vie personnelle.

Que Dieu les récompense et leur accorde santé, bonheur et prospérité.

AVANT-PROPOS

Ce mémoire de maîtrise représente l'aboutissement d'un cheminement académique riche en apprentissages, au terme duquel j'ai pu approfondir des domaines qui me passionnent, en particulier la cybersécurité, la gestion des risques et la gouvernance des organisations. Les cours suivis ainsi que les lectures et recherches menées tout au long de ce parcours m'ont permis de développer une expertise solide touchant à la gestion des incidents de sécurité, à l'investigation forensic numérique et, surtout, à l'ingénierie des ontologies appliquée au domaine de la cybersécurité.

Au fil de mes travaux, j'ai pu observer que les différentes disciplines composant la cybersécurité organisationnelle évoluent encore trop souvent en vase clos, chacune s'appuyant sur ses propres normes et son propre langage. Cette observation a été le point de départ de ma volonté d'explorer comment les technologies sémantiques pourraient permettre de rapprocher ces différents domaines et de les faire dialoguer entre eux.

Ce travail cherche ainsi à montrer comment une ontologie intégrée peut servir de pont conceptuel entre plusieurs référentiels normatifs reconnus, en vue de favoriser une vision plus unifiée des processus liés à la gestion des incidents, à l'investigation numérique, à la gestion des risques et à la gouvernance au sein des organisations.

Ce parcours de recherche n'a pas été sans embûches : il a été ponctué de doutes, de remises en question et d'ajustements constants, mais tout autant de moments de satisfaction et d'avancées significatives. Les pages qui suivent reflètent les nombreuses heures investies dans la réflexion, l'analyse et la recherche, portées par une volonté soutenue de bien comprendre et de bien traiter le sujet abordé.

L'ensemble des propos exprimés dans ce document relève de mon entière responsabilité. Sachant toutefois que tout travail humain est perfectible, j'accueillerai avec gratitude toute remarque, critique ou suggestion susceptible d'en enrichir le contenu.

CHAPITRE I

INTRODUCTION

1.1 CONTEXTE DE LA RECHERCHE

La transformation numérique occupe aujourd'hui une place centrale dans le fonctionnement des organisations modernes. Les systèmes d'information, les infrastructures numériques et les données représentent désormais des actifs stratégiques essentiels au soutien des activités opérationnelles, financières et décisionnelles des entreprises. Cette dépendance croissante aux technologies numériques expose cependant les organisations à des cybermenaces de plus en plus sophistiquées capables de provoquer des impacts économiques, opérationnels et stratégiques considérables (Allahrakha, 2024). Les pertes mondiales liées à la cybercriminalité dépassent désormais plusieurs milliards de dollars chaque année, incluant les vols financiers, les attaques par rançongiciel, les violations de propriété intellectuelle ainsi que les coûts associés à la restauration des systèmes compromis et aux activités de reprise après incident (Allahrakha, 2024).

L'émergence rapide de l'intelligence artificielle accentue davantage cette évolution en rendant les cyberattaques plus automatisées, plus ciblées et plus difficiles à détecter. Les cybercriminels exploitent désormais des mécanismes avancés capables de générer des campagnes de phishing sophistiquées, d'automatiser l'exploitation de vulnérabilités critiques et d'accélérer les attaques contre les infrastructures numériques (Felahi & El Yousfi, 2025). Ces développements technologiques augmentent non seulement les coûts directs associés à la gestion des incidents de sécurité, mais aussi les conséquences indirectes telles que la perte de confiance des utilisateurs, la détérioration de la réputation organisationnelle et la diminution de la compétitivité des entreprises affectées (Felahi & El Yousfi, 2025).

Par ailleurs, l'accélération de la numérisation, particulièrement dans les économies émergentes, met en évidence d'importantes lacunes réglementaires ainsi qu'une fragmentation des cadres juridiques liés à la cybersécurité. Cette situation limite l'efficacité des réponses face aux cybermenaces et affaiblit la protection des entreprises, des institutions et des consommateurs (Hasbullah, 2022). Dans un environnement numérique caractérisé par une forte interconnexion des systèmes, les conséquences d'une cyberattaque dépassent souvent le cadre purement technique pour affecter directement les processus organisationnels, les opérations critiques et la continuité des activités.

Plusieurs normes, guides et cadres de référence internationaux proposent aujourd'hui des approches structurées visant à renforcer la cybersécurité organisationnelle. Parmi les référentiels largement acceptés figurent la norme International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, qui définit les exigences relatives à la mise en place, au maintien et à l'amélioration continue d'un système de gestion de la sécurité de l'information fondé sur une approche systématique de la sécurité (Milicevic & Goeken, 2010), la norme ISO/IEC 27035, qui formalise les processus de gestion des incidents de sécurité de l'information (ISO/IEC, 2023), ainsi que le guide National Institute of Standards and Technology (NIST) Special Publication (SP) 800-86, qui propose un cadre méthodologique pour l'intégration des techniques d'investigation numérique dans les processus de réponse aux incidents (Kent *et al.*, 2006). D'autres référentiels, tels que la norme ISO/IEC 27005 et le cadre Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM), fournissent respectivement des mécanismes pour la gestion des risques liés à la sécurité de l'information (ISO/IEC, 2022) et pour l'intégration des risques dans les processus stratégiques et décisionnels de l'organisation (COSO, 2017).

1.2 PROBLÉMATIQUE DE LA RECHERCHE

Malgré l'existence de plusieurs standards et cadres de référence en cybersécurité, les approches actuelles demeurent fortement fragmentées et sont généralement déployées dans des silos organisationnels (Olaniyi *et al.*, 2024). Shawe & Mengnjo (2026) qualifient cette situation de *fragmentation structurelle de la responsabilité*, dans laquelle les fonctions de cybersécurité sont réparties entre plusieurs domaines organisationnels tels que les technologies de l'information, les technologies opérationnelles, la conformité, les services juridiques et la gestion des risques d'entreprise. Cette fragmentation affaiblit la visibilité globale sur les cyberrisques et limite la cohérence des mécanismes de gouvernance et de prise de décision.

Dans plusieurs organisations, les programmes de gestion des risques d'entreprise (ERM) permettent d'identifier les cyberrisques sans toujours établir de lien structuré avec les mécanismes techniques de détection et de réponse aux incidents, ni avec les processus organisationnels d'évaluation des risques et de gouvernance (Olaniyi *et al.*, 2024). Cette fragmentation est renforcée par les incohérences terminologiques persistantes au sein du domaine de la cybersécurité, où des concepts équivalents sont désignés par des termes différents selon les secteurs, ce qui nuit à l'interopérabilité et à la communication entre professionnels (Hasan *et al.*, 2025). Cette déconnexion fonctionnelle limite ainsi la capacité des organisations à tirer pleinement parti des informations issues des incidents de sécurité pour orienter leurs décisions, alors qu'une approche intégrée permettrait au contraire de mieux cerner l'ensemble du paysage de risques numériques et de prioriser les menaces les plus critiques (Olaniyi *et al.*, 2024).

Face à la fragmentation des approches de cybersécurité, certains travaux montrent qu'une approche intégrée de la gestion des risques d'entreprise, des référentiels normatifs tels qu'ISO/IEC 27001 et des capacités d'investigation numérique permet d'améliorer significativement la gestion stratégique des risques de sécurité au sein des organisations (Olaniyi

et al., 2024). Dans cette perspective, plusieurs travaux ont eu recours aux ontologies pour améliorer l'intégration des connaissances et l'interopérabilité entre les différents domaines de la sécurité de l'information. Fenz *et al.* (2009), Massacci *et al.* (2011), Ramanauskaitė *et al.* (2013) ainsi que Vorobiev *et al.* (2008) proposent notamment des mécanismes de mapping et d'extension ontologique permettant d'établir des correspondances entre des référentiels de sécurité distincts. Toutefois, à notre connaissance, aucun de ces travaux n'intègre conjointement la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle au sein d'une ontologie intégrée. Ce constat soulève des questions relatives aux connaissances à intégrer, aux mécanismes de représentation ontologique favorisant leur interopérabilité ainsi qu'à la capacité d'une ontologie intégrée à répondre à des questions de compétence transversales liées à la gouvernance des cyberrisques.

1.3 QUESTIONS DE RECHERCHE

Dans ce contexte, cette recherche vise à répondre aux questions de recherche suivantes :

- **RQ1 :** Quels référentiels normatifs couvrant la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle peuvent être intégrés au sein d'une représentation commune des connaissances en cybersécurité ?
- **RQ2 :** Dans quelle mesure une approche ontologique formelle permet-elle d'assurer l'interopérabilité entre des référentiels de cybersécurité conçus de façon indépendante ?
- **RQ3 :** Dans quelle mesure une ontologie intégrée permet-elle de répondre à des questions transversales couvrant la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle ?

1.4 OBJECTIF DE LA RECHERCHE

Cette étude vise à concevoir et valider une ontologie intégrée de cybersécurité permettant de relier, au sein d'une représentation commune des connaissances, la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle. Pour atteindre cet objectif, cette étude s'articule autour des sous-objectifs (SO) suivants :

— **SO1 :** Identifier les référentiels normatifs pertinents et formaliser leurs concepts et relations au sein d'une ontologie intégrée ;

— **SO2 :** Évaluer la cohérence logique de l'ontologie intégrée au moyen d'un raisonnement automatique ;

— **SO3 :** Valider la capacité de l'ontologie intégrée à répondre à des questions de compétence mobilisant des connaissances issues de plusieurs domaines, notamment la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle.

1.5 APERÇU DE L'APPROCHE PROPOSÉE

L'approche proposée repose sur un référentiel d'ancrage construit à partir de la norme ISO/IEC 27035, retenue pour son rôle central dans la gestion des incidents et ses liens explicites avec ISO/IEC 27001. Ce référentiel d'ancrage fournit la structure conceptuelle initiale à partir de laquelle les différents domaines de la cybersécurité sont progressivement intégrés. L'ontologie est ensuite étendue par l'intégration des concepts issus de la norme ISO/IEC 27005, du guide NIST SP 800-86 et du cadre COSO ERM.

L'ontologie intégrée est validée à travers un scénario de cyberattaque dans un environnement simulé. Ce scénario permet d'instancier les différents concepts de l'ontologie à partir des observations collectées durant l'attaque et d'évaluer les relations établies entre les différents

domaines de la cybersécurité au moyen de questions de compétence. La cohérence logique de l'ontologie est vérifiée au moyen d'un raisonnement automatique.

1.6 STRUCTURE DU DOCUMENT

Le reste du mémoire est structuré comme suit. Le deuxième chapitre présente les fondements théoriques de la recherche, notamment les impacts économiques des cyberattaques, les approches de gestion des incidents, la forensic numérique, la gestion des risques ainsi que les principaux standards et cadres de gouvernance utilisés en cybersécurité. Le troisième chapitre est consacré à la revue de littérature et analyse les travaux de recherche portant sur la fragmentation des approches de cybersécurité organisationnelle et les solutions proposées. Il met également en évidence les lacunes identifiées dans la littérature et justifie l'approche retenue dans cette recherche.

Le quatrième chapitre décrit la méthodologie de recherche ainsi que les étapes de construction du cadre intégré. Une attention particulière est portée aux méthodes de développement et d'intégration ontologique utilisées pour concevoir le modèle proposé. Le cinquième chapitre présente la validation du cadre intégré à travers le scénario expérimental, l'évaluation du modèle, ainsi que la discussion des résultats, les contributions, les limites de la recherche et les perspectives futures. Enfin, le mémoire se termine par une conclusion générale.

CHAPITRE II

FONDEMENTS THÉORIQUES

2.1 CONTEXTE GÉNÉRAL

La transformation numérique a profondément modifié les structures économiques contemporaines en créant un environnement fortement dépendant des technologies numériques et des systèmes d'information. Les organisations modernes utilisent désormais des infrastructures numériques interconnectées pour assurer leurs activités opérationnelles, financières et stratégiques. Toutefois, cette évolution s'accompagne également d'un élargissement important de la surface d'attaque exploitable par des acteurs malveillants aux motivations variées (Allahrakha, 2024; Hasbullah, 2022).

L'essor des technologies numériques ainsi que l'intégration croissante de l'intelligence artificielle dans les systèmes d'information ont considérablement augmenté la complexité des cybermenaces. Les cyberattaques deviennent aujourd'hui plus automatisées, plus ciblées et plus difficiles à détecter (Felahi & El Yousfi, 2025). Les cybercriminels exploitent notamment des mécanismes avancés permettant d'automatiser l'exploitation de vulnérabilités critiques, de générer des campagnes de phishing sophistiquées et d'accélérer les attaques contre les infrastructures numériques. Dans ce contexte, la cybercriminalité s'impose désormais comme un phénomène macroéconomique majeur, les pertes mondiales liées aux cyberattaques étant estimées à plus d'un billion de dollars par année (Allahrakha, 2024).

Les impacts économiques des cyberattaques se manifestent à travers des coûts directs et indirects. Les coûts directs regroupent principalement les dépenses associées à la gestion des incidents de sécurité, notamment les investigations forensic, la restauration des systèmes compromis, les paiements de rançons, les pénalités réglementaires ainsi que les frais juri-

diques (Felahi & El Yousfi, 2025). Les interruptions de service provoquées par les attaques par rançongiciel ou les attaques par déni de service entraînent également des pertes financières liées à l'arrêt des activités organisationnelles et à l'indisponibilité des services numériques.

Au-delà de ces impacts directs, les organisations subissent également des conséquences indirectes souvent plus durables et plus difficiles à quantifier. Ces conséquences incluent la détérioration de la réputation organisationnelle, la perte de confiance des clients et des partenaires, la diminution de la valeur marchande des entreprises ainsi que les atteintes à l'image de marque (Felahi & El Yousfi, 2025; Hasbullah, 2022). Dans certains cas, les cyberattaques peuvent également entraîner des pertes stratégiques importantes, notamment la divulgation d'informations confidentielles, le vol de propriété intellectuelle ou la perturbation des chaînes d'approvisionnement.

Par ailleurs, les cyberattaques exercent une pression croissante sur les cadres juridiques et réglementaires existants. Les lacunes réglementaires ainsi que la fragmentation des systèmes juridiques aux niveaux national et international peuvent affaiblir considérablement la capacité des organisations à protéger efficacement leurs actifs numériques et à maintenir la confiance des parties prenantes (Hasbullah, 2022). Dans des environnements numériques fortement interconnectés, les conséquences des cyberattaques dépassent souvent les limites des organisations directement ciblées pour produire des effets en cascade sur l'ensemble de l'écosystème économique (Allahrakha, 2024).

L'analyse de la littérature scientifique met ainsi en évidence que la cybersécurité ne constitue pas uniquement une problématique technique, mais représente un enjeu stratégique, économique et organisationnel pour les entreprises modernes. La réduction des impacts financiers associés aux cyberattaques nécessite donc la mise en place de mécanismes intégrés capables d'assurer une détection précoce des menaces, une gestion structurée des incidents

ainsi qu'une coordination cohérente entre les dimensions techniques, organisationnelles et stratégiques de la cybersécurité.

2.2 NORMES ET CADRES DE GESTION DE LA SÉCURITÉ ET DES RISQUES

2.2.1 COSO ENTERPRISE RISK MANAGEMENT (COSO-ERM)

Le cadre COSO-ERM, publié initialement en 2004 puis révisé en profondeur en 2017, constitue l'un des principaux cadres de référence en matière de gestion intégrée des risques organisationnels (COSO, 2017; Efe, 2023). Développé par le *Committee of Sponsoring Organizations of the Treadway Commission*, ce cadre propose une approche stratégique visant à intégrer la gestion des risques dans l'ensemble des processus décisionnels et opérationnels de l'organisation.

Contrairement aux approches traditionnelles centrées sur la réduction des risques opérationnels, COSO-ERM considère la gestion des risques comme un élément de création de valeur et de soutien à la performance organisationnelle. Le cadre cherche ainsi à assurer un alignement entre les objectifs stratégiques, la gouvernance organisationnelle et les mécanismes de gestion des risques (COSO, 2017; Efe, 2023). Cette approche favorise une vision globale des risques susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs.

Le modèle COSO-ERM repose sur cinq composantes principales : la gouvernance et la culture, la stratégie et la définition des objectifs, la performance, la révision et l'amélioration continue, ainsi que l'information, la communication et le reporting (COSO, 2017; Efe, 2023; Olaniyi *et al.*, 2024). Ces composantes sont fortement interconnectées et permettent d'intégrer l'appétit au risque dans les processus de prise de décision stratégique. Le cadre met également l'accent sur la surveillance continue des risques ainsi que sur la capacité des organisations à adapter leurs mécanismes de gouvernance en fonction de l'évolution de leur environnement.

Dans le contexte actuel de transformation numérique, le cadre COSO-ERM apparaît particulièrement pertinent pour la gestion des cyberrisques et des risques associés aux technologies numériques (Oladoyinbo *et al.*, 2023). Les organisations utilisent de plus en plus des environnements infonuagiques, des infrastructures connectées et des systèmes numériques afin d'améliorer leur efficacité opérationnelle et leur flexibilité. Toutefois, cette évolution introduit également de nouvelles vulnérabilités liées à la confidentialité des données, à la disponibilité des services, à la conformité réglementaire et à la protection des actifs numériques.

En cybersécurité, COSO-ERM constitue ainsi un cadre important pour intégrer les cyberrisques dans les mécanismes globaux de gouvernance organisationnelle. Cependant, malgré son approche holistique de la gestion des risques, ce cadre ne formalise pas explicitement les relations entre les incidents de sécurité, les investigations forensic, les preuves numériques et les mécanismes opérationnels de réponse aux incidents. Cette limitation souligne l'importance de développer des modèles sémantiques capables d'assurer une meilleure intégration entre la gestion des risques, la gestion des incidents et la gouvernance en cybersécurité.

2.2.2 ISO/IEC 27001 : SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

La norme ISO/IEC 27001 constitue l'un des principaux standards internationaux en matière de gestion de la sécurité de l'information. Elle fournit un cadre structuré permettant aux organisations de mettre en place et d'améliorer continuellement un système de management de la sécurité de l'information (ISMS) afin de protéger leurs actifs informationnels contre les cybermenaces (Olaniyi *et al.*, 2024).

L'implémentation d'un ISMS conforme à ISO/IEC 27001 contribue au renforcement des mécanismes de prévention, de détection et de réponse aux incidents de sécurité, tout en

favorisant la résilience organisationnelle et la réduction des impacts associés aux cyberattaques (Olaniyi *et al.*, 2024).

D'un point de vue conceptuel, Milicevic & Goeken (2010) ont réalisé une analyse ontologique du standard ISO/IEC 27001 et ont identifié cinq concepts fondamentaux structurant son modèle de sécurité : l'actif, la menace, le contrôle, l'exigence et le rôle. Les auteurs soulignent également une limite importante du modèle, à savoir l'absence d'une formalisation explicite du concept de vulnérabilité, pourtant central dans plusieurs ontologies de cybersécurité et dans des standards complémentaires tels qu'ISO/IEC 27005.

Ainsi, bien que la norme ISO/IEC 27001 fournisse un cadre robuste pour la gouvernance de la sécurité de l'information, sa structure conceptuelle demeure partiellement implicite lorsqu'il s'agit de représenter formellement les connaissances et les relations sémantiques entre les différents concepts de cybersécurité. Cette limitation justifie l'utilisation d'approches ontologiques permettant d'assurer une meilleure cohérence sémantique et de faciliter l'intégration transversale avec d'autres standards de cybersécurité, notamment ceux liés à la gestion des incidents, à la forensic numérique, à la gestion des risques et à la gouvernance.

2.2.3 ISO/IEC 27035 : GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

La norme ISO/IEC 27035-1 :2023 propose un cadre structuré destiné à la gestion des incidents de sécurité de l'information en définissant les principes, les rôles organisationnels et les différentes phases du traitement des incidents (ISO/IEC, 2023). Elle reconnaît que, malgré l'implémentation de contrôles de sécurité dans un système de management conforme à ISO/IEC 27001, certaines vulnérabilités résiduelles peuvent toujours être exploitées par des

acteurs malveillants, entraînant des événements susceptibles d'évoluer en incidents de sécurité affectant les actifs informationnels et la continuité des activités.

La norme distingue explicitement les concepts de menace, de vulnérabilité, d'événement et d'incident de sécurité, contribuant ainsi à une meilleure compréhension des relations entre les différents éléments impliqués dans la gestion des incidents. Elle favorise également une approche structurée permettant d'améliorer la détection des incidents, la coordination des actions de réponse et la mise en œuvre de mesures correctives adaptées (ISO/IEC, 2023).

Les travaux de Poetiray & Salman (2023) démontrent l'applicabilité pratique de cette norme au sein d'une institution gouvernementale confrontée à des incidents récurrents. Leur étude montre que la mise en place d'une politique formelle de gestion des incidents, d'une équipe dédiée et de mécanismes structurés de signalement contribue significativement au renforcement de la résilience organisationnelle.

Ainsi, ISO/IEC 27035 constitue un cadre fondamental pour intégrer la détection des incidents, la réponse opérationnelle et l'amélioration continue des mécanismes de sécurité. Cette norme fournit également une base conceptuelle importante pour l'intégration des processus de gestion des risques et des investigations forensic, ce qui justifie son rôle central dans le modèle ontologique proposé dans cette recherche.

2.2.4 ISO/IEC 27005 : GESTION DES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION

La norme ISO/IEC 27005 constitue un cadre de référence important pour la gestion des risques liés à la sécurité de l'information. Elle propose une approche structurée reposant sur plusieurs étapes successives et itératives, notamment l'établissement du contexte, l'identifica-

tion des risques, l'analyse, l'évaluation, le traitement, l'acceptation ainsi que le suivi continu des risques (ISO/IEC, 2022; Agrawal, 2016, 2017).

Cette norme vise principalement à aider les organisations à identifier les menaces susceptibles d'affecter leurs actifs informationnels et à mettre en place des mesures appropriées afin de réduire les impacts potentiels des incidents de sécurité (ISO/IEC, 2022; Agrawal, 2016). L'approche proposée permet également d'améliorer la prise de décision en fournissant une vision structurée des risques et des contrôles de sécurité associés.

Agrawal (2016) souligne cependant que l'interprétation subjective de certains concepts fondamentaux liés au risque peut entraîner des ambiguïtés dans les processus de gestion de la sécurité. Afin de réduire cette problématique, l'auteur propose une formalisation ontologique des principaux concepts de la norme ISO/IEC 27005, notamment les notions d'organisation, d'actif, de menace, de vulnérabilité, d'événement, de conséquence, de vraisemblance et de contrôle. Cette approche permet de clarifier les relations sémantiques entre ces différents éléments et de renforcer la cohérence du processus d'évaluation des risques.

Dans une étude complémentaire, Agrawal (2017) met également en évidence que les processus définis par ISO/IEC 27005 génèrent un ensemble structuré d'informations comprenant les listes d'actifs, les menaces, les vulnérabilités, les plans de traitement ainsi que les évaluations des risques résiduels. Ces informations doivent être correctement identifiées, organisées et classifiées afin d'assurer la protection des systèmes d'information et le respect des exigences réglementaires.

Par ailleurs, les travaux de Ariyani & Sudarma (2016) démontrent l'applicabilité opérationnelle de la norme dans un environnement institutionnel fortement transactionnel. En appliquant les clauses liées à l'établissement du contexte et à l'évaluation des risques, les auteurs identifient les actifs critiques, évaluent les menaces associées et priorisent les risques

à l'aide d'une approche quantitative structurée. Les résultats montrent que l'application méthodique de la norme permet d'identifier les risques prioritaires et de mettre en œuvre des mesures correctives adaptées afin d'améliorer la fiabilité des systèmes d'information et de renforcer la résilience organisationnelle face aux incidents de sécurité.

Ainsi, ISO/IEC 27005 fournit une base méthodologique importante pour la gestion des risques en cybersécurité. Toutefois, comme plusieurs autres standards, la norme ne formalise pas explicitement les relations sémantiques entre les incidents, les investigations forensic et les mécanismes de gouvernance, ce qui justifie l'utilisation d'approches ontologiques pour assurer une meilleure intégration des différentes dimensions de la cybersécurité organisationnelle.

2.2.5 NIST SP 800-86 : INTÉGRATION DE LA FORENSIC NUMÉRIQUE DANS LA RÉPONSE AUX INCIDENTS

Le guide NIST SP 800-86 propose un cadre méthodologique structuré visant à intégrer les techniques de forensic numérique dans les processus de réponse aux incidents de sécurité (Kent *et al.*, 2006). Ce guide définit la forensic numérique comme l'application de méthodes scientifiques rigoureuses permettant d'identifier, de collecter, d'examiner, d'analyser et de présenter des données numériques tout en assurant l'intégrité des informations ainsi que la préservation de la chaîne de possession (*chain of custody*).

Le processus forensic décrit par le guide est organisé autour de quatre phases principales : la collecte, l'examen, l'analyse et le rapport (Kent *et al.*, 2006). La phase de collecte consiste à acquérir les données numériques pertinentes sans altérer leur intégrité. La phase d'examen permet ensuite de filtrer et d'extraire les informations utiles à l'investigation. L'analyse vise à interpréter les données collectées afin de reconstruire les événements liés à l'incident et d'identifier les causes de l'attaque. Enfin, la phase de rapport consiste à documenter les

résultats de l'investigation de manière structurée afin de soutenir les activités de réponse aux incidents et la prise de décision organisationnelle.

Le guide NIST SP 800-86 met également l'accent sur l'importance de la documentation rigoureuse, de la reproductibilité des analyses et de l'utilisation de procédures standardisées afin de garantir la fiabilité des investigations forensic. Cette approche permet aux organisations d'améliorer leur capacité à comprendre les incidents de sécurité, à préserver les preuves numériques et à renforcer leur posture globale de cybersécurité.

Les travaux de Luthfi *et al.* (2024) montrent que NIST SP 800-86 adopte une approche fortement orientée vers l'investigation et la réponse aux incidents, en accordant une attention particulière à l'intégration des activités forensic dans les opérations courantes des organisations. Les auteurs soulignent que l'utilisation d'un cadre méthodologique structuré facilite la gestion des preuves numériques et améliore la cohérence des investigations de sécurité.

Par ailleurs, la revue de littérature réalisée par Mndeep *et al.* (2016) met en évidence le rôle central de la forensic numérique dans la reconstruction des scénarios d'attaque et l'identification des causes profondes des incidents de cybersécurité. Les auteurs insistent sur l'importance des méthodologies structurées et des outils spécialisés pour garantir l'authenticité, l'intégrité et la fiabilité des analyses forensic.

Ainsi, le guide NIST SP 800-86 constitue une référence importante pour l'intégration des processus forensic dans la gestion des incidents de sécurité. Toutefois, comme les autres cadres cités, il ne formalise pas explicitement les relations sémantiques entre les incidents, les risques et les mécanismes de gouvernance organisationnelle. Cette limitation justifie l'utilisation d'approches ontologiques afin d'assurer une meilleure intégration entre les investigations forensic, la gestion des incidents, la gestion des risques et la gouvernance en cybersécurité.

CHAPITRE III
REVUE DE LITTÉRATURE

3.1 FRAGMENTATION DES APPROCHES ORGANISATIONNELLES EN CYBERSÉCURITÉ

Malgré la disponibilité croissante de standards internationaux en cybersécurité, leur implémentation au sein des organisations demeure fragmentée et insuffisamment coordonnée, une situation observée dans plusieurs secteurs d'activité, tailles d'organisations et modèles de gouvernance (Olaniyi *et al.*, 2024; Shawe & Mengnjo, 2026; Mdaki, 2025).

D'un point de vue théorique, Shawe & Mengnjo (2026) désignent cette situation sous le terme de *Structural Accountability Fragmentation*. Dans les grandes organisations complexes, particulièrement dans les secteurs d'infrastructures critiques tels que la santé et l'énergie, les responsabilités liées à la cybersécurité sont réparties entre plusieurs domaines fonctionnels, notamment les technologies de l'information, les technologies opérationnelles, la conformité, les services juridiques, les achats ainsi que la gestion des risques d'entreprise. Lorsque l'autorité de gouvernance est fragmentée entre ces différents domaines, aucune entité ne possède une visibilité globale sur l'exposition de l'organisation aux cyberrisques. Les auteurs montrent que cette fragmentation structurelle génère des angles morts prévisibles en cybersécurité à travers trois mécanismes interdépendants : la distribution de l'autorité, la séparation des rapports de risques et la faiblesse des mécanismes d'escalade. Ils soulignent également que les évaluations standardisées de cybersécurité, notamment celles basées sur le NIST Cybersecurity Framework (CSF) ou sur les outils d'évaluation de la Cybersecurity and Infrastructure Security Agency (CISA), permettent souvent d'identifier ces angles morts sans toutefois les corriger, faute de mécanismes de gouvernance capables d'assurer la coordination et l'escalade

des résultats vers les décideurs organisationnels (Shawe & Mengnjo, 2026). Ainsi, plusieurs risques importants demeurent invisibles jusqu'à la survenue d'un incident majeur.

Sur le plan empirique, Olaniyi *et al.* (2024) confirment cette problématique à travers une étude quantitative menée auprès de 372 professionnels de la cybersécurité provenant de plusieurs secteurs. Leurs résultats démontrent que les mécanismes de gestion des risques d'entreprise (ERM), les systèmes basés sur ISO/IEC 27001 ainsi que les capacités de forensic numérique sont souvent déployés de manière indépendante et en silo, créant ainsi des lacunes structurelles susceptibles d'être exploitées par des acteurs malveillants. Dans cette configuration, l'ERM fournit une vision stratégique des risques à l'échelle organisationnelle, tandis qu'ISO/IEC 27001 formalise les contrôles opérationnels de sécurité sans intégrer pleinement les mécanismes d'analyse post-incident issus de la forensic numérique.

Les auteurs utilisent notamment l'exemple de la fuite de données d'Equifax en 2017, qui illustre des défaillances simultanées dans l'identification des risques, la gestion des vulnérabilités et la réponse forensic, trois domaines fonctionnant indépendamment les uns des autres (Olaniyi *et al.*, 2024). Leurs résultats, obtenus à l'aide d'une analyse Partial Least Squares Structural Equation Modeling (PLS-SEM), montrent que l'intégration de ces trois composantes produit des améliorations sur plusieurs dimensions de la gestion de la sécurité numérique, confirmant qu'une approche intégrée est plus efficace qu'une implémentation isolée des différents mécanismes de cybersécurité (Olaniyi *et al.*, 2024).

La fragmentation des approches de cybersécurité ne concerne toutefois pas uniquement les grandes organisations. Mdaki (2025) montre que les petites entreprises sont également confrontées à cette problématique, où les ressources limitées amplifient les conséquences des lacunes organisationnelles. En s'appuyant sur le rapport *Verizon 2024 Data Breach Investigations Report*, l'auteur indique que 68 % des violations de données impliquent un facteur

humain et que 60 % des petites entreprises cessent leurs activités dans les six mois suivant une cyberattaque majeure. Ces résultats sont principalement liés à l'absence d'intégration entre les contrôles techniques, la gouvernance organisationnelle et la culture de sécurité. Lorsque la gestion des risques, les mécanismes de sécurité opérationnelle et les facteurs humains sont traités séparément, même des menaces relativement limitées peuvent produire des conséquences critiques pour l'organisation (Mdaki, 2025).

Dans l'ensemble, ces travaux convergent vers une conclusion commune : la fragmentation des approches de cybersécurité constitue un problème structurel majeur résultant de l'absence d'un cadre sémantique unifié capable de relier les incidents, les risques, les contrôles, les preuves numériques et les décisions de gouvernance au sein d'un modèle organisationnel cohérent. Le problème ne réside donc pas dans l'inefficacité des standards pris individuellement, mais dans l'absence d'interopérabilité entre ces cadres de référence.

3.2 SOLUTIONS PROPOSÉES

Face à la fragmentation des approches de cybersécurité, plusieurs travaux ont proposé des mécanismes visant à améliorer l'intégration des connaissances et la coordination entre les différents domaines de la sécurité de l'information.

Certaines recherches privilégient des approches organisationnelles intégrées. Par exemple, Olaniyi *et al.* (2024) démontrent que l'intégration de la gestion des risques d'entreprise (ERM), des pratiques fondées sur ISO/IEC 27001 et des capacités de forensic numérique améliore significativement les performances de la cybersécurité organisationnelle. Leurs résultats suggèrent qu'une approche coordonnée est plus efficace qu'un déploiement isolé des différents mécanismes de cybersécurité.

D'autres travaux s'intéressent à l'intégration des connaissances à travers des approches sémantiques. Fenz *et al.* (2009), Massacci *et al.* (2011), Ramanauskaitė *et al.* (2013) ainsi que Vorobiev *et al.* (2008) proposent des mécanismes de mapping et d'extension ontologique permettant d'établir des correspondances entre des référentiels de sécurité distincts et d'améliorer l'interopérabilité entre différentes sources de connaissances.

3.2.1 ONTOLOGIES FONDATRICES DE CYBERSÉCURITÉ ET FORMALISATION DES CONNAISSANCES

La cybersécurité constitue un domaine particulièrement complexe et multidisciplinaire, caractérisé par une forte hétérogénéité conceptuelle et terminologique. Les concepts fondamentaux tels que les menaces, les vulnérabilités, les incidents, les risques, les actifs, les politiques de sécurité et les contre-mesures sont souvent définis différemment selon les disciplines, les standards et les approches organisationnelles considérés. Cette diversité sémantique limite l'interopérabilité entre les systèmes hétérogènes, complique le partage des connaissances entre les experts et freine l'automatisation des mécanismes de raisonnement en sécurité de l'information (Arbanas & Čubrilo, 2015).

Selon Gruber, une ontologie est définie comme une « spécification formelle et explicite d'une conceptualisation d'un domaine d'intérêt commun » (Breitman *et al.*, 2007). Dans le domaine de la sécurité de l'information, les ontologies sont utilisées pour formaliser et représenter les concepts, les relations et les connaissances associés aux menaces, aux vulnérabilités, aux incidents de sécurité, aux politiques de sécurité, aux mécanismes de défense, à la gestion des risques ainsi qu'à la gouvernance de la sécurité (Arbanas & Čubrilo, 2015). Leur construction repose généralement sur l'identification des concepts clés du domaine, leur structuration hiérarchique et la définition de relations sémantiques explicites entre ces concepts (Boinski *et al.*, 2011).

La littérature met en évidence une évolution progressive des ontologies de sécurité, passant de simples modèles conceptuels vers des architectures sémantiques plus complexes intégrant plusieurs dimensions de la cybersécurité. Dans leur revue de littérature, Arbanas & Čubrilo (2015) identifient 52 travaux publiés répartis en trois grandes catégories : les ontologies générales de sécurité, les ontologies dédiées à des sous-domaines spécifiques de la cybersécurité ainsi que les travaux théoriques ou méthodologiques. Cette classification met en évidence à la fois la richesse et la fragmentation des connaissances dans le domaine.

Au-delà des travaux spécifiquement consacrés à la cybersécurité, plusieurs contributions ont établi les fondements méthodologiques de la construction ontologique. Parmi les plus influentes, Noy *et al.* (2001) proposent une méthodologie structurée de développement d'ontologies reposant sur l'identification du domaine et de la portée de l'ontologie, la réutilisation éventuelle d'ontologies existantes, la définition des concepts, des relations et des propriétés, ainsi que l'instanciation des connaissances. Cette approche demeure largement utilisée dans les travaux d'ingénierie ontologique et constitue une référence importante pour la conception de modèles sémantiques complexes.

Plusieurs travaux se sont intéressés à la construction d'ontologies générales capables de représenter le domaine de la sécurité de l'information. Herzog *et al.* (2007) proposent une ontologie Web Ontology Language (OWL) intégrant des concepts fondamentaux tels que les actifs, les menaces, les vulnérabilités, les contre-mesures, les stratégies de défense et les objectifs de sécurité. Cette ontologie intègre de nombreuses classes et relations permettant le raisonnement automatique et l'exécution de requêtes avancées.

De manière similaire, Fenz *et al.* (2009) développent une ontologie intégrant les concepts liés aux menaces, aux vulnérabilités, aux contrôles de sécurité et aux actifs organisationnels. Leur approche enrichit la base de connaissances ontologique grâce à l'intégration de concepts

issus du standard allemand IT-Grundschutz, démontrant l'importance des représentations sémantiques pour la gestion des risques et la gouvernance de la sécurité.

D'autres travaux ont exploré l'utilisation des ontologies pour soutenir la gouvernance de la sécurité de l'information. dos Santos Moreira *et al.* (2008) proposent un cadre structuré en trois niveaux (stratégique, tactique et opérationnel) permettant de représenter les connaissances de sécurité selon différents niveaux décisionnels. Leur approche montre que les ontologies peuvent faciliter l'intégration des vulnérabilités, des incidents, des risques et des politiques de sécurité tout en soutenant les activités de gestion et de gouvernance de la sécurité de l'information.

Ekelhart *et al.* (2007) développent une ontologie dédiée à l'analyse quantitative des risques intégrant les actifs, les menaces, les vulnérabilités et les contre-mesures.

Parallèlement aux ontologies générales, plusieurs travaux se sont intéressés à des domaines spécifiques de la cybersécurité. Dans le domaine de la gestion des vulnérabilités, Wang & Guo (2009) proposent une ontologie enrichie à partir des données de la National Vulnerability Database (NVD) afin de faciliter le raisonnement automatique et l'analyse des vulnérabilités. De leur côté, Gao *et al.* (2013) développent une ontologie des cyberattaques structurée autour des concepts d'attaquant, de vecteur d'attaque, de vulnérabilité, de cible et de mécanisme de défense. Leur modèle s'appuie sur plusieurs bases de connaissances, notamment Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE) et Common Vulnerability Scoring System (CVSS), afin de représenter formellement les cyberattaques et leurs impacts sur les systèmes d'information.

Le domaine de la sécurité des réseaux a également fait l'objet de nombreuses approches ontologiques. Simmonds *et al.* (2004) développent une ontologie extensible des attaques réseau capable de relier plusieurs classifications standardisées des menaces. Hung & Liu

(2008) proposent une approche permettant à des utilisateurs non experts de configurer des systèmes de détection d'intrusion à partir d'une ontologie du domaine. Xu *et al.* (2009) utilisent les ontologies afin d'améliorer l'analyse contextuelle des alertes de sécurité et de favoriser une gestion unifiée de la sécurité réseau.

La gestion des incidents de sécurité constitue un domaine largement étudié dans la littérature ontologique. Blackwell (2010) proposent une architecture en trois niveaux — social, logique et physique — destinée à analyser les incidents de sécurité selon des dimensions humaines, organisationnelles et techniques. De manière similaire, Martimiano & Moreira (2005) développent une ontologie OWL dédiée aux incidents de sécurité intégrant des concepts tels que l'attaque, l'agent, l'actif, la vulnérabilité, l'outil et les conséquences des incidents. Cette approche facilite la corrélation d'incidents provenant de sources hétérogènes et améliore la gestion des connaissances associées aux incidents de sécurité.

L'infonuagique constitue un domaine important d'application des ontologies de cybersécurité. Takahashi *et al.* (2010) identifient plusieurs facteurs liés au cloud, notamment la séparation des actifs, les dépendances entre ressources et l'utilisation de services externes. Bernsmed *et al.* (2013) proposent une ontologie dédiée aux obligations de sécurité afin de faciliter la comparaison automatisée des exigences entre fournisseurs de services, tandis que Youseff *et al.* (2008) développent une ontologie unifiée structurée autour des différentes couches de services et d'infrastructure.

D'autres contributions portent sur des aspects plus spécifiques de la cybersécurité. Parkin *et al.* (2009) développent une ontologie intégrant les facteurs comportementaux humains dérivés de la norme ISO 27002 afin d'analyser les impacts des décisions de sécurité sur les utilisateurs. Kang & Liang (2013) utilisent les ontologies dans une approche Model-Driven Architecture (MDA) afin d'intégrer les concepts de sécurité dans toutes les phases du cycle de

vie du développement logiciel. Janpitak & Sathitwiriyawong (2011) proposent notamment une ontologie de sécurité physique pour les centres de données basée sur Control Objectives for Information and Related Technologies (COBIT), ISO/IEC 27002 et Information Technology Infrastructure Library (ITIL).

Enfin, plusieurs travaux théoriques et méthodologiques ont contribué à l'évolution des approches ontologiques en cybersécurité. Tsoumas *et al.* (2005) proposent un cadre de gestion des connaissances reliant les politiques de sécurité de haut niveau aux contrôles techniques à travers un processus structuré de formalisation des exigences de sécurité. Obrst *et al.* (2012) développent une ontologie de cybersécurité inspirée du modèle du diamant, intégrant les acteurs, les victimes, les infrastructures et les capacités associées aux cyberattaques. De leur côté, Boinski *et al.* (2011) définissent des principes méthodologiques visant à assurer l'intégration et l'interopérabilité des ontologies de sécurité avec d'autres systèmes de connaissances.

Dans l'ensemble, ces travaux montrent que les ontologies jouent un rôle central dans la structuration des connaissances en cybersécurité, l'amélioration de l'interopérabilité sémantique, le partage des connaissances et le soutien aux mécanismes de raisonnement automatique dans des environnements complexes de sécurité de l'information.

3.2.2 AVANCÉES RÉCENTES DES ONTOLOGIES DE CYBERSÉCURITÉ

Les recherches récentes témoignent d'un intérêt croissant pour l'utilisation des ontologies dans les différents domaines de la cybersécurité. Alors que les premières ontologies avaient principalement pour objectif de formaliser les connaissances de sécurité et d'améliorer le partage d'informations, les travaux publiés au cours des dernières années s'orientent davantage vers des problématiques opérationnelles telles que la gestion des risques, la cyber threat intelligence, la détection d'anomalies, l'automatisation de l'évaluation des risques et la gestion

des incidents. Cette évolution reflète la nécessité de disposer de modèles sémantiques capables de soutenir l'automatisation, le raisonnement et la prise de décision dans des environnements de cybersécurité de plus en plus complexes.

Ontologies orientées gestion des risques : La gestion des risques constitue aujourd'hui l'un des principaux domaines d'application des ontologies de cybersécurité. Face à l'évolution des cybermenaces et à la complexité croissante des infrastructures numériques, plusieurs travaux récents ont exploré l'utilisation des technologies sémantiques afin d'améliorer l'identification, l'évaluation et la surveillance des risques. Ces approches exploitent les capacités de représentation des connaissances et de raisonnement automatique des ontologies pour faciliter la prise de décision et renforcer la connaissance de la situation de sécurité.

Merah & Kenaza (2021) proposent une ontologie destinée à la surveillance continue du cyber-risque à partir du Cyber Threat Intelligence (CTI). Leur approche étend l'ontologie OntoSIEM en l'alignant avec les concepts du standard Structured Threat Information Expression (STIX) 2.0 afin d'intégrer les connaissances relatives aux menaces, aux vulnérabilités, aux campagnes d'attaque et aux mesures de mitigation. L'objectif principal de leur modèle consiste à corréler les alertes de sécurité, les informations de topologie réseau et les renseignements sur les menaces dans un cadre sémantique commun. Grâce à l'utilisation du raisonnement ontologique, leur système permet d'identifier les vulnérabilités critiques, de détecter des scénarios d'attaque potentiels et d'améliorer la surveillance continue des risques. Cette contribution démontre l'intérêt du Cyber Threat Intelligence dans les mécanismes modernes de gestion des risques et met en évidence le rôle des ontologies dans l'amélioration de la cyber-situational awareness. Toutefois, leur approche demeure principalement centrée sur la cyberveille et ne traite pas explicitement les activités d'investigation forensic, les processus de gestion des incidents ou les mécanismes de gouvernance organisationnelle.

Dans le même domaine, Sánchez-Zas *et al.* (2023) développent une ontologie visant à soutenir la gestion des risques en temps réel et la *cyber-situational awareness* dans les environnements cyber-physiques. Leur modèle intègre des informations provenant de capteurs physiques et logiques, des anomalies détectées ainsi que des bases de renseignement sur les menaces afin d'évaluer continuellement le niveau de risque d'un système. L'approche proposée s'appuie sur la SPARQL Inferencing Notation (SPIN), un cadre permettant d'exprimer des règles d'inférence et des contraintes au moyen du langage SPARQL Protocol and RDF Query Language (SPARQL), plutôt que sur les règles du Semantic Web Rule Language (SWRL), fréquemment utilisées dans les systèmes ontologiques. Néanmoins, le modèle proposé demeure principalement orienté vers l'analyse des risques et ne couvre pas explicitement les processus de réponse aux incidents, les investigations numériques ou les mécanismes de gouvernance.

Par ailleurs, Maunero *et al.* (2023) proposent une approche ontologique visant à automatiser l'évaluation des risques de cybersécurité. Leur modèle, orienté actifs, représente les infrastructures informatiques, les vulnérabilités, les menaces et les risques au sein d'une base de connaissances unique. L'ontologie est enrichie à partir de référentiels reconnus tels que CVE, CWE, National Vulnerability Database (NVD) et Common Attack Pattern Enumeration and Classification (CAPEC) afin d'automatiser l'identification des risques. Les auteurs utilisent des règles d'inférence pour détecter les vulnérabilités présentes dans une infrastructure et déduire les menaces susceptibles d'affecter les actifs organisationnels. Cette approche réduit les efforts manuels tout en améliorant la cohérence et la reproductibilité des analyses. De plus, l'utilisation de référentiels largement adoptés facilite l'adaptation du modèle à l'évolution des menaces et des vulnérabilités. Toutefois, la solution demeure principalement orientée vers les aspects techniques de l'évaluation des risques et n'intègre pas la gestion des incidents, les investigations forensic ou les décisions de gouvernance.

Dans l'ensemble, ces travaux démontrent que les ontologies constituent des outils particulièrement efficaces pour améliorer la surveillance des cyber-risques, intégrer les connaissances issues du Cyber Threat Intelligence et automatiser les activités d'évaluation des risques. Ils montrent également que les technologies sémantiques permettent de corréler des informations provenant de sources hétérogènes et de soutenir les mécanismes de raisonnement nécessaires à la prise de décision. Cependant, les approches recensées demeurent largement spécialisées et se concentrent principalement sur les relations entre actifs, menaces, vulnérabilités et risques. Les dimensions relatives à la gestion des incidents, aux investigations forensic, à la collecte de preuves numériques, aux objectifs stratégiques de l'organisation et aux mécanismes de gouvernance restent généralement peu développées. Cette observation met en évidence la nécessité de développer des modèles ontologiques plus intégrés capables de relier les activités de gestion des risques aux processus de gestion des incidents, aux investigations numériques et à la gouvernance organisationnelle.

Ontologies orientées gestion des incidents : Les ontologies récentes ont également été utilisées pour améliorer la gestion des incidents de cybersécurité. Avec l'augmentation du nombre et de la complexité des cyberattaques, plusieurs chercheurs se sont intéressés au développement de modèles sémantiques capables de représenter de manière cohérente les événements de sécurité, les incidents, les preuves numériques, les actions de réponse et les activités de récupération. L'objectif principal de ces approches est d'améliorer la compréhension des incidents, de faciliter le partage d'information entre les différents acteurs et de soutenir les processus de prise de décision lors des opérations de réponse aux incidents.

Dans cette perspective, Chockalingam & Maathuis (2022) proposent une ontologie visant à fournir une représentation structurée des concepts intervenant dans les phases intermédiaires et postérieures à un incident de sécurité. Leur approche s'appuie sur plusieurs standards

reconnus dans le domaine de la cybersécurité, notamment STIX et Incident Object Description Exchange Format (IODEF), afin de modéliser les relations entre les incidents, les indicateurs de compromission, les preuves numériques, les actions de réponse et les activités de partage d'information. L'ontologie intègre également des concepts issus de la criminalistique numérique, tels que les artefacts d'investigation, les sources de preuves et les résultats d'analyse, permettant ainsi d'améliorer la traçabilité des événements observés lors d'un incident.

L'une des contributions majeures de cette recherche réside dans l'intégration des activités de retour d'expérience (*lessons learned*) au sein du modèle ontologique. Cette approche permet de conserver les connaissances acquises lors d'incidents précédents et de les réutiliser pour améliorer les futures opérations de réponse. Afin de valider leur modèle, les auteurs utilisent le cas réel de l'attaque par rançongiciel contre Colonial Pipeline. Cette étude de cas démontre que l'ontologie permet de représenter efficacement les relations entre les acteurs impliqués, les événements observés, les preuves collectées et les mesures correctives mises en œuvre. Toutefois, bien que cette approche améliore significativement la gestion opérationnelle des incidents, elle reste principalement centrée sur les activités de réponse et de récupération et n'intègre pas explicitement les mécanismes de gestion des risques ou les dimensions de gouvernance organisationnelle.

Dans une perspective complémentaire, Tailhardat *et al.* (2024) développent Network-Oriented Incident Response and Investigation Ontology (NORIA-O), une ontologie destinée à la détection d'anomalies et à la gestion des incidents dans les infrastructures Technologies de l'Information et de la Communication (TIC) à grande échelle. Contrairement aux approches orientées exclusivement vers les incidents de sécurité, NORIA-O adopte une vision plus large intégrant les activités de supervision, de maintenance et d'exploitation des infrastructures informatiques. L'ontologie permet de représenter les infrastructures réseau, les équipements,

les événements opérationnels, les anomalies détectées, les opérations de maintenance, les procédures de diagnostic et les actions de remédiation.

L'objectif principal de cette approche est de fournir un modèle sémantique unifié capable d'intégrer des données provenant de sources hétérogènes telles que les systèmes de supervision réseau, les outils de monitoring, les plateformes de gestion des événements et les bases de connaissances techniques. Cette intégration facilite la corrélation des événements observés et améliore l'analyse des causes racines lors d'incidents complexes. Les auteurs montrent qu'une représentation ontologique permet de mieux comprendre les dépendances entre les composants d'une infrastructure et de soutenir les activités de diagnostic dans des environnements distribués (Tailhardat *et al.*, 2024).

Par ailleurs, NORIA-O favorise l'interopérabilité entre différents outils de supervision et contribue à réduire la fragmentation des informations de sécurité au sein des infrastructures critiques. Cette contribution est particulièrement pertinente dans les organisations modernes où les incidents résultent souvent de l'interaction entre plusieurs systèmes et technologies. Cependant, malgré son intérêt pour la supervision et la gestion des incidents, cette ontologie demeure essentiellement orientée vers les aspects techniques et opérationnels des infrastructures TIC. Les concepts liés à l'évaluation des risques, aux objectifs stratégiques de l'organisation, aux décisions de gouvernance ou aux processus forensic approfondis restent relativement peu développés (Tailhardat *et al.*, 2024).

Ces travaux contribuent à renforcer les capacités de détection, d'analyse et de réponse aux incidents. Néanmoins, ils restent principalement orientés vers les aspects opérationnels et techniques de la cybersécurité et n'établissent que peu de liens avec les processus de gestion des risques stratégiques ou les mécanismes de gouvernance organisationnelle.

Revues systématiques récentes : Les revues systématiques récentes soulignent l'intérêt croissant des ontologies pour la représentation et l'intégration des connaissances en cybersécurité. Face à la multiplication des cybermenaces, à la diversité des référentiels de sécurité et à l'augmentation du volume de données, les technologies sémantiques apparaissent comme une solution prometteuse pour améliorer l'interopérabilité, le partage des connaissances et l'automatisation des processus de cybersécurité.

Dans cette perspective, Hasan *et al.* (2025) réalisent une revue systématique approfondie des ontologies de cybersécurité et identifient plusieurs défis persistants dans ce domaine. Leur analyse montre que les ontologies existantes sont principalement développées pour répondre à des besoins spécifiques tels que la gestion des vulnérabilités, la cyber threat intelligence, l'évaluation des risques, la détection d'intrusions ou la gestion des incidents. Cette spécialisation a conduit à la création de nombreux modèles indépendants utilisant des terminologies, des structures conceptuelles et des mécanismes de raisonnement différents.

Les auteurs soulignent notamment l'existence d'une importante hétérogénéité sémantique entre les ontologies de cybersécurité. Cette diversité terminologique limite l'interopérabilité entre les systèmes et complique l'intégration de connaissances provenant de différentes sources. La revue met également en évidence l'absence de mécanismes permettant de relier efficacement les différentes dimensions de la cybersécurité, notamment la gestion des risques, la gestion des incidents, la cyber threat intelligence, les investigations numériques et la gouvernance organisationnelle.

Par ailleurs, Hasan *et al.* (2025) soulignent que peu de travaux abordent explicitement la question de l'intégration des standards et référentiels de cybersécurité au sein d'un cadre ontologique unifié. Les organisations modernes s'appuient pourtant simultanément sur plusieurs référentiels complémentaires tels que les normes ISO/IEC, les guides NIST, les bases

de connaissances de cybermenaces et les cadres de gouvernance des risques. L'absence de mécanismes sémantiques capables d'établir des liens entre ces différents domaines limite l'exploitation des connaissances issues des activités de cybersécurité.

Dans l'ensemble, les recherches récentes confirment le potentiel des ontologies pour améliorer la gestion des risques, la détection d'anomalies, la gestion des incidents et le partage des connaissances. Cependant, les approches existantes demeurent largement spécialisées et fragmentées. Cette situation soulève la nécessité de développer des modèles sémantiques capables d'intégrer plusieurs domaines de connaissances au sein d'un cadre cohérent afin de soutenir une vision plus globale de la cybersécurité organisationnelle.

3.2.3 ANALYSE DE LA COUVERTURE DES DOMAINES

L'analyse de la littérature montre que les ontologies constituent aujourd'hui un mécanisme important pour structurer les connaissances de cybersécurité, améliorer l'interopérabilité entre systèmes hétérogènes et soutenir les mécanismes de raisonnement automatique. Les travaux existants ont permis de formaliser différents domaines de la cybersécurité, notamment la gestion des risques, la cyber threat intelligence, la détection d'anomalies et la gestion des incidents (Merah & Kenaza, 2021; Sánchez-Zas *et al.*, 2023; Maunero *et al.*, 2023; Chockalingam & Maathuis, 2022; Tailhardat *et al.*, 2024).

Malgré ces avancées, les ontologies recensées demeurent généralement spécialisées et se concentrent sur un domaine particulier de la cybersécurité. Les ontologies orientées gestion des risques modélisent principalement les relations entre actifs, menaces, vulnérabilités et niveaux de risque (Merah & Kenaza, 2021; Sánchez-Zas *et al.*, 2023; Maunero *et al.*, 2023), tandis que les ontologies orientées gestion des incidents privilégient les activités de détection, de réponse et de récupération (Chockalingam & Maathuis, 2022; Tailhardat *et al.*, 2024). Cette

spécialisation limite leur capacité à représenter de manière globale les interactions entre les différentes composantes de la cybersécurité organisationnelle.

Par ailleurs, les revues récentes soulignent la persistance d'une forte fragmentation sémantique entre les ontologies de cybersécurité (Hasan *et al.*, 2025). Les modèles existants reposent souvent sur des terminologies, des structures conceptuelles et des domaines d'application différents, ce qui complique l'intégration des connaissances provenant de multiples référentiels et réduit leur interopérabilité.

Une autre limite importante concerne l'absence de liens explicites entre les activités de gestion des incidents, les investigations forensic numériques, l'évaluation des risques et les mécanismes de gouvernance organisationnelle. Les ontologies orientées incidents intègrent parfois certaines informations issues des investigations numériques, mais elles modélisent rarement les conséquences organisationnelles, les objectifs stratégiques, les décisions de gouvernance ou les mécanismes de réduction des risques. À l'inverse, les ontologies orientées risques représentent les actifs, les menaces et les vulnérabilités, sans intégrer de manière détaillée les processus d'investigation numérique et de gestion des incidents.

Enfin, bien que plusieurs travaux aient proposé des approches de mapping et d'extension ontologique afin d'améliorer l'interopérabilité entre standards et référentiels de sécurité (Fenz *et al.*, 2009; Massacci *et al.*, 2011; Ramanauskaitė *et al.*, 2013; Vorobiev *et al.*, 2008), les applications recensées concernent principalement l'intégration de concepts techniques ou de référentiels homogènes. Aucun des travaux étudiés ne propose un cadre ontologique reliant simultanément les menaces, les événements de sécurité, les incidents, les investigations forensic, les risques, les conséquences organisationnelles, les décisions de gouvernance, les objectifs stratégiques et les contrôles de sécurité au sein d'un même modèle sémantique.Le Tableau 3.1 montre qu'aucun des travaux recensés ne couvre simultanément la gestion des

incidents, l'investigation forensic numérique, la gestion des risques et la gouvernance au sein d'un même cadre ontologique intégré. Ainsi, la principale lacune identifiée dans la littérature réside dans l'absence d'un cadre ontologique capable de relier ces différentes dimensions au sein d'un modèle sémantique unifié.

TABLEAU 3.1 : Couverture des domaines incident, forensic, risque et gouvernance dans les travaux existants

Travaux	Gestion incidents	Forensic numérique	Gestion des risques	Gouvernance
(Agrawal, 2016)	×	×	✓	×
(Milicevic & Goeken, 2010)	×	×	×	×
(Martimiano & Moreira, 2005)	✓	×	×	×
(dos Santos Moreira *et al.*, 2008)	∼	×	∼	✓
(Fenz *et al.*, 2009)	×	×	✓	∼
(Merah & Kenaza, 2021)	×	×	✓	×
(Sánchez-Zas *et al.*, 2023)	×	×	✓	×
(Maunero *et al.*, 2023)	×	×	✓	×
(Chockalingam & Maathuis, 2022)	✓	∼	×	×
(Tailhardat *et al.*, 2024)	✓	∼	×	×

Légende : ✓ = couverture complète ; ∼ = couverture partielle ; × = absence de couverture.

3.2.4 APPROCHE PROPOSÉE

Les ontologies apparaissent comme des outils particulièrement pertinents pour structurer les connaissances, réduire les ambiguïtés terminologiques et permettre le raisonnement automatique en cybersécurité (Arbanas & Čubrilo, 2015). Les travaux de Fenz *et al.* (2009) démontrent notamment que les méthodologies de mapping ontologique facilitent l'intégration de standards de sécurité hétérogènes au sein d'un modèle conceptuel cohérent. De son côté, Agrawal (2016) propose une formalisation ontologique de la norme ISO/IEC 27005

afin de structurer les concepts liés à la gestion des risques. Toutefois, ces travaux demeurent généralement limités à des référentiels spécifiques et n'abordent pas l'intégration complète de la chaîne incident ;forensic ;risque ;gouvernance.

Afin de combler cette lacune, cette recherche propose un cadre intégré de cybersécurité reposant sur une ontologie développée à partir des connaissances issues des normes ISO/IEC 27035, ISO/IEC 27001, ISO/IEC 27005, du guide NIST SP 800-86 et du cadre COSO ERM. L'approche proposée utilise l'ontologie ISO/IEC 27035 comme référentiel d'ancrage, étendu progressivement par l'intégration des concepts liés à l'investigation forensic numérique, à la gestion des risques et à la gouvernance organisationnelle. L'objectif est de fournir un modèle sémantique unifié permettant d'établir des liens explicites entre les incidents de sécurité, les preuves numériques, les risques organisationnels et les décisions de gouvernance.

CHAPITRE IV
MÉTHODOLOGIE

4.1 MÉTHODOLOGIE DE CONSTRUCTION DE L'ONTOLOGIE INTÉGRÉE

La construction de l'ontologie intégrée proposée dans cette recherche repose sur l'utilisation successive de deux méthodologies distinctes, chacune intervenant à une étape spécifique du processus de construction ontologique.

Dans un premier temps, la méthodologie de développement d'ontologies proposée par Noy *et al.* (2001) est utilisée pour développer séparément les différentes ontologies sources nécessaires à cette recherche. Elle permet ainsi de structurer et de formaliser les connaissances propres à chaque source.

Dans un second temps, l'approche de *mapping* ontologique proposée par Fenz *et al.* (2009) est utilisée pour établir les correspondances entre ces ontologies et intégrer progressivement leurs connaissances. Cette intégration s'effectue autour d'un référentiel d'ancrage basé sur la norme ISO/IEC 27035, qui constitue la structure centrale de l'ontologie intégrée.

Les deux méthodologies remplissent ainsi des fonctions distinctes dans le processus : Noy *et al.* (2001) guide le développement des ontologies sources, tandis que Fenz *et al.* (2009) guide leur mise en correspondance et leur intégration au référentiel d'ancrage. La démarche méthodologique adoptée s'articule autour de trois phases principales : **(1)** le développement ou la réutilisation des ontologies sources, **(2)** leur extension et leur intégration progressive au référentiel d'ancrage, et **(3)** l'évaluation de l'ontologie intégrée obtenue.

La Figure 4.1 présente une vue d'ensemble de la méthodologie suivie pour la construction de l'ontologie intégrée proposée.

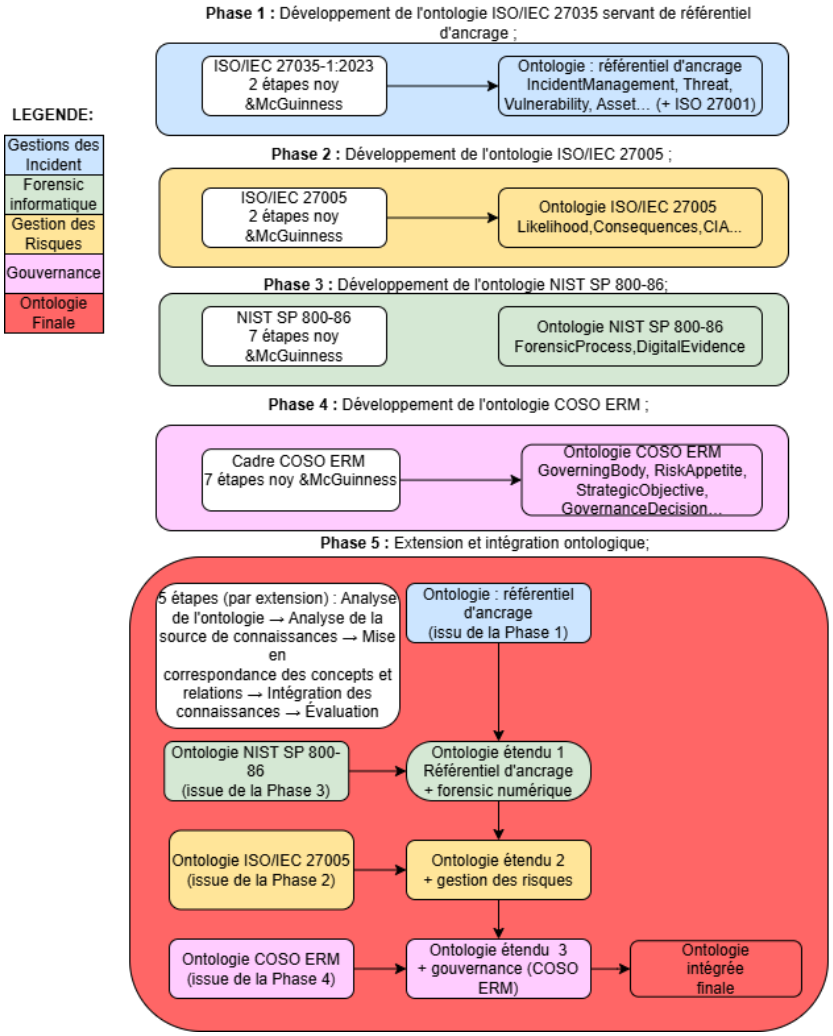

FIGURE 4.1 : Méthodologie de construction de l'ontologie intégrée.

4.2 DÉVELOPPEMENT ONTOLOGIQUE SELON NOY ET MCGUINNESS

La méthodologie proposée par Noy *et al.* (2001) constitue l'une des approches les plus largement utilisées pour le développement d'ontologies. Elle repose sur un processus itératif composé de sept étapes :

1. Déterminer le domaine et la portée de l'ontologie ;
2. Examiner la possibilité de réutiliser des ontologies existantes ;

3. Identifier les termes pertinents du domaine ;
4. Définir les classes et organiser la hiérarchie des classes ;
5. Définir les propriétés d'objet ;
6. Définir les propriétés de données ;
7. Créer les instances.

Dans cette recherche, cette méthodologie est appliquée de manière différenciée selon les référentiels étudiés. Les deux premières étapes sont utilisées pour ISO/IEC 27035 et ISO/IEC 27005 dans une logique de réutilisation de connaissances existantes. En revanche, les sept étapes complètes sont appliquées au développement des ontologies relatives au guide NIST SP 800-86 et au cadre COSO ERM.

4.2.1 DÉVELOPPEMENT DE L'ONTOLOGIE ISO/IEC 27035 COMME RÉFÉRENTIEL D'ANCRAGE

Étape 1 : Détermination du domaine et de la portée. Le domaine couvert par cette ontologie concerne la gestion des incidents de sécurité de l'information. Son objectif est de fournir une structure conceptuelle permettant de représenter les événements de sécurité, les incidents, les menaces, les vulnérabilités, les actifs, les contrôles de sécurité ainsi que les processus organisationnels associés à la gestion des incidents.

La norme ISO/IEC 27035-1 :2023 a été retenue comme référentiel d'ancrage en raison de son rôle central dans la gestion des incidents. Contrairement aux autres référentiels étudiés, la norme ISO/IEC 27035-1 :2023 occupe une position transversale au sein du cycle de cybersécurité. La gestion des incidents constitue en effet un point de convergence entre les événements de sécurité, les menaces, les vulnérabilités, les contrôles de sécurité, les investigations numériques et les processus organisationnels de réponse (ISO/IEC, 2023).

Étape 2 : Réutilisation des connaissances existantes. Cette étape consiste à réutiliser des connaissances existantes afin de servir de base à la construction de l'ontologie. Dans cette recherche, les deux modèles conceptuels proposés par la norme ISO/IEC 27035-1 :2023 ont été réutilisés pour identifier les principaux concepts et relations de la gestion des incidents de sécurité, puis regroupés dans un modèle conceptuel unique servant de référentiel d'ancrage (ISO/IEC, 2023).

L'ontologie développée à partir de la norme ISO/IEC 27035-1 :2023 joue ainsi le rôle de référentiel d'ancrage au sein de l'architecture proposée. Elle fournit la structure conceptuelle de référence à partir de laquelle les extensions liées à l'investigation forensic, à la gestion des risques et à la gouvernance organisationnelle sont progressivement intégrées.

La Figure 4.2 illustre la structure conceptuelle de l'ontologie ISO/IEC 27035 obtenue à l'issue de cette phase de développement et servant de référentiel d'ancrage pour les phases ultérieures d'intégration ontologique.

4.2.2 DÉVELOPPEMENT DE L'ONTOLOGIE ISO/IEC 27005

Étape 1 : Détermination du domaine et de la portée. Le domaine couvert par cette ontologie concerne la gestion des risques liés à la sécurité de l'information. Son objectif est d'enrichir le référentiel d'ancrage par des concepts permettant de représenter les conséquences des incidents, leur vraisemblance d'occurrence, leurs impacts sur l'organisation ainsi que les objectifs susceptibles d'être affectés.

L'intégration d'ISO/IEC 27005 vise à compléter la représentation des risques déjà présente dans l'ontologie développée à partir d'ISO/IEC 27035 en introduisant des concepts nécessaires à l'évaluation et au traitement des risques organisationnels.

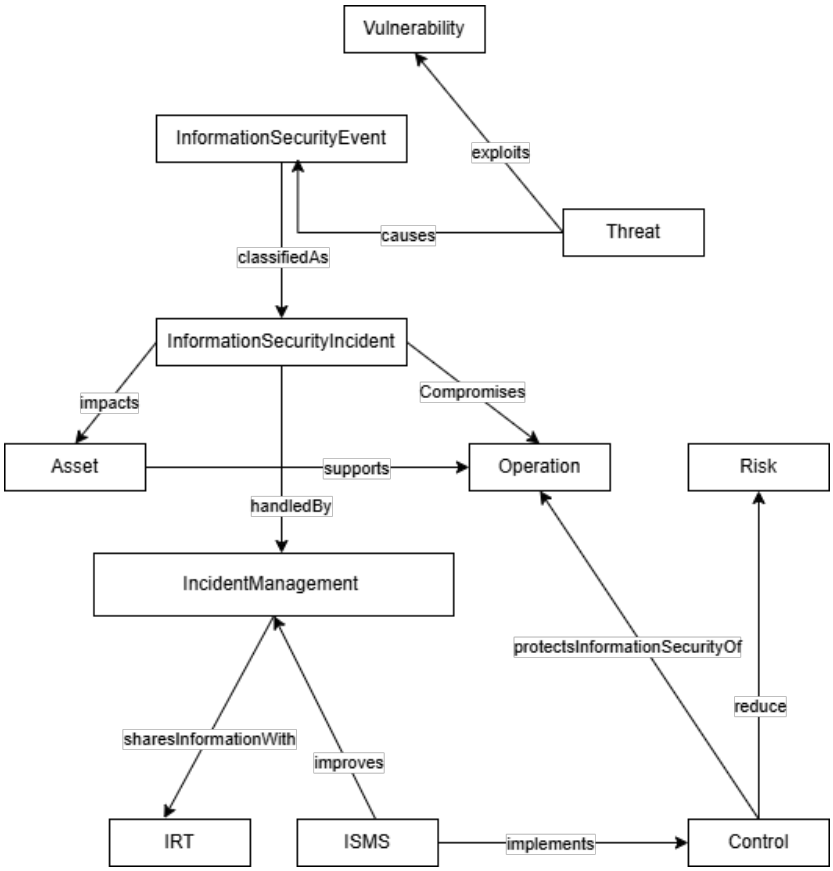

FIGURE 4.2 : Ontologie du référentiel d'ancrage ISO/IEC 27035.

Étape 2 : Réutilisation des connaissances existantes. Conformément à la deuxième étape de la méthodologie proposée par Noy *et al.* (2001), une analyse des ontologies existantes relatives à la gestion des risques a été réalisée. Cette analyse a conduit à retenir l'ontologie proposée par Agrawal (2016), qui constitue une formalisation OWL des concepts issus de la norme ISO/IEC 27005.

La Figure 4.3 présente l'ontologie ISO/IEC 27005 retenue comme source de connaissances pour représenter les concepts de gestion des risques pertinents pour cette recherche.

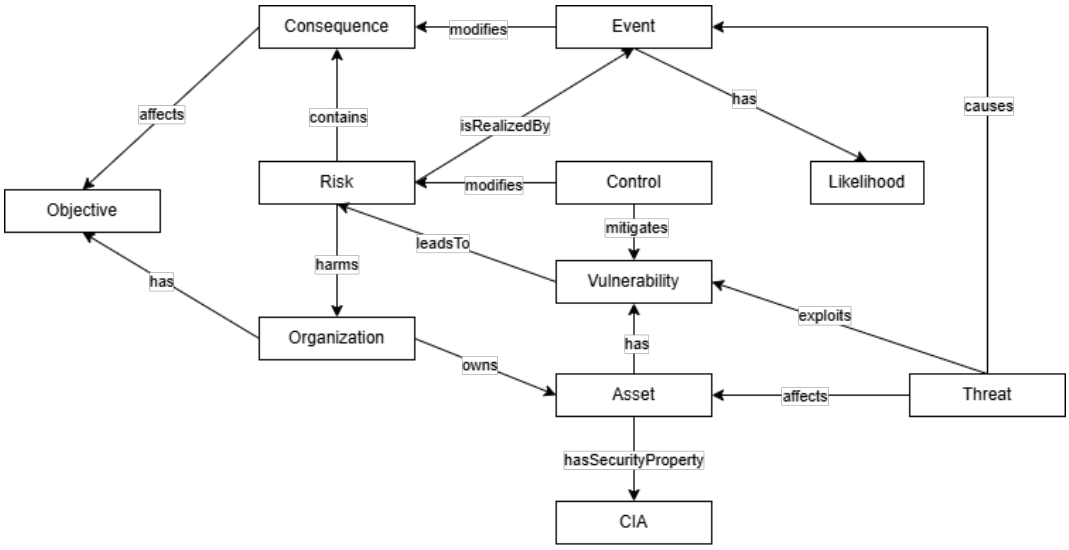

FIGURE 4.3 : Ontologie ISO/IEC 27005 extraite d' Agrawal (2016).

4.2.3 DÉVELOPPEMENT DE L'ONTOLOGIE NIST SP 800-86

Contrairement à l'ontologie développée à partir de la norme ISO/IEC 27035, qui joue le rôle de référentiel d'ancrage au sein de l'architecture proposée, l'ontologie NIST SP 800-86 a été développée en appliquant les sept étapes de la méthodologie d'ingénierie ontologique proposée par Noy *et al.* (2001). Cette démarche permet de construire une ontologie de manière progressive et cohérente tout en assurant sa compatibilité avec les autres composantes.

Étape 1 : Détermination du domaine et de la portée de l'ontologie. Le domaine retenu concerne l'investigation forensic numérique appliquée à la réponse aux incidents de sécurité de l'information. L'objectif de cette ontologie est de représenter les concepts permettant de relier un incident de sécurité aux activités d'investigation numérique et aux preuves produites, tout en tenant compte du contexte dans lequel ces activités sont réalisées.

Étape 2 : Réutilisation des connaissances existantes. Une analyse de la littérature a été réalisée afin d'identifier d'éventuelles ontologies couvrant les concepts du guide NIST SP 800-86. Cette analyse n'a pas permis d'identifier une ontologie directement exploitable et suffisamment alignée avec les objectifs de cette recherche. Le développement d'une ontologie a donc été entrepris à partir du contenu normatif du guide (Kent *et al.*, 2006).

Étape 3 : Identification des termes importants du domaine. L'analyse du guide NIST SP 800-86 a permis d'identifier les concepts nécessaires à la représentation des activités d'investigation numérique ainsi que de leur contexte opérationnel. Les termes retenus incluent les événements de sécurité, les incidents, les actifs informationnels, les opérations organisationnelles, les menaces, les vulnérabilités, l'équipe de reponse aux incidents, les contrôles de sécurité, les processus forensic et les preuves numériques produites au cours d'une investigation.

Étape 4 : Définition des classes et de la hiérarchie. Les concepts identifiés ont été transformés en classes ontologiques. Les classes sont *InformationSecurityEvent*, *Incident*, *Operation*, *Asset*, *Vulnerability*, *Control*, *Threat*, *Incident Response Team (IRT)*, *ForensicProcess* et *DigitalEvidence*. Les définitions détaillées de ces concepts sont présentées dans le Tableau 5.1.

Étape 5 : Définition des propriétés d'objet. Les relations sémantiques entre les différentes classes ont été modélisées sous forme de propriétés d'objet. Parmi les principales relations identifiées figurent *causes*, *leads*, *triggers*, *compromises*, *supports*, *produces*, *adjusts*, *qualifies*, *managedBy*, *implements*, *protects* et *exposes*.

Étape 6 : Définition des propriétés de données. Les propriétés de données nécessaires à la description des concepts forensic ont été identifiées lors de cette étape. Elles permettent notamment d'associer aux preuves numériques des informations descriptives telles que leur type, leur format, leur source ou leur empreinte cryptographique.

Étape 7 : Création des instances. Les instances de l'ontologie sont créées à partir du scénario expérimental USHOP présenté au Chapitre V. Cette approche permet de dissocier la phase de développement de l'ontologie de sa phase de validation. Les instances sont ainsi générées à partir des observations recueillies durant le scénario d'attaque afin de vérifier la capacité du modèle à représenter les relations entre les activités d'investigation numérique, les preuves produites et les autres composantes de la chaîne intégrée de cybersécurité.

La Figure 4.4 présente l'ontologie développée à partir du guide NIST SP 800-86.

4.2.4 DÉVELOPPEMENT DE L'ONTOLOGIE COSO ERM

L'ontologie COSO ERM a été développée selon la méthodologie d'ingénierie ontologique proposée par Noy *et al.* (2001). Comme pour l'ontologie NIST SP 800-86, les sept étapes de cette méthodologie ont été appliquées afin de construire une représentation formelle des concepts liés à la gouvernance organisationnelle. Les étapes mises en œuvre dans le cadre de cette recherche sont décrites ci-dessous.

Étape 1 : Détermination du domaine et du périmètre de l'ontologie. Le domaine retenu concerne la gouvernance des risques d'entreprise appliquée à la cybersécurité. L'objectif de cette ontologie est de représenter les mécanismes de gouvernance permettant de relier

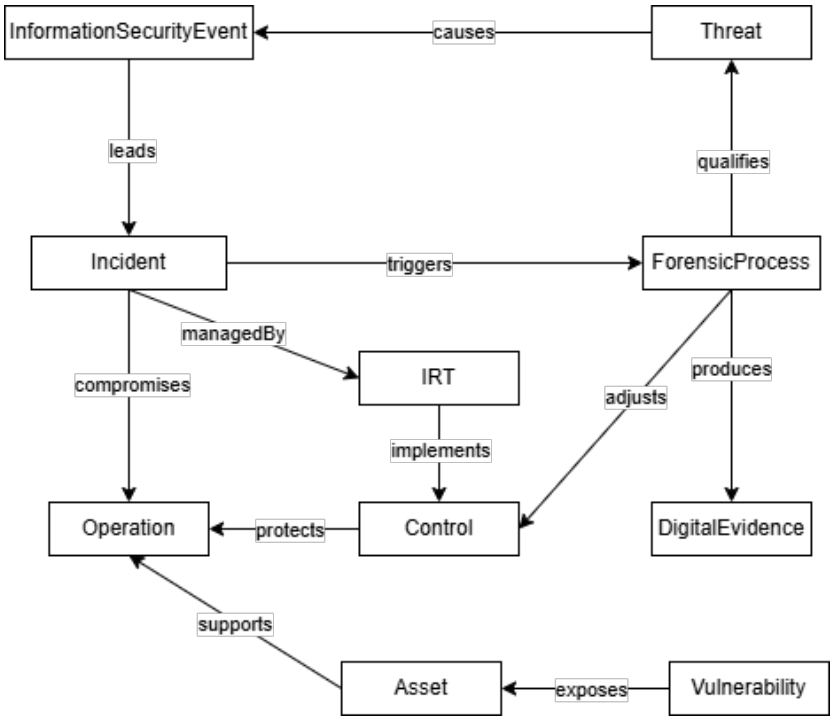

FIGURE 4.4 : Ontologie NIST SP 800-86.

les cyberrisques aux objectifs stratégiques de l'organisation et aux décisions prises par les instances dirigeantes.

Étape 2 : Réutilisation des connaissances existantes. Une analyse des principaux cadres de gouvernance et de gestion des risques a été réalisée afin d'identifier les concepts les plus pertinents pour la modélisation ontologique (COSO, 2017; Efe, 2023). Cette analyse a montré qu'aucune ontologie COSO ERM directement exploitable n'était disponible pour répondre aux besoins spécifiques de cette recherche, justifiant ainsi le développement d'une ontologie.

Étape 3 : Identification des termes pertinents du domaine. Les principaux concepts du cadre COSO ERM ont été identifiés à partir de l'analyse du référentiel COSO ERM. Cette étape a permis de sélectionner les concepts liés à la gouvernance, aux objectifs stratégiques, à

la culture du risque, à l'appétit au risque, à la tolérance au risque, à l'évaluation des risques, à la priorisation des risques, au suivi, au reporting et à la prise de décision organisationnelle.

Étape 4 : Définition des classes et de la hiérarchie. Les concepts identifiés ont été transformés en classes ontologiques. Les classes sont *Organization*, *GoverningBody*, *StrategicObjective*, *RiskCulture*, *RiskAppetite*, *RiskTolerance*, *Risk*, *RiskAssessment*, *RiskPrioritization*, *GovernanceDecision*, *Monitoring* et *Reporting*. Les définitions détaillées de ces concepts sont présentées dans le Tableau 5.1.

Étape 5 : Définition des propriétés d'objet. Les relations sémantiques entre les différentes classes ont été modélisées sous forme de propriétés d'objet. Parmi les principales relations identifiées figurent *governs*, *establishes*, *defines*, *influences*, *determines*, *threatens*, *isSubjectTo*, *providesInputTo*, *justifies*, *protects*, *detects*, *generates* et *guides*.

Étape 6 : Définition des propriétés de données. Les propriétés de données nécessaires à la description des concepts de gouvernance ont été identifiées et définies lors de cette étape. Elles permettent d'associer aux instances des valeurs littérales représentant notamment les niveaux de risque, les seuils de tolérance, les niveaux de priorité ou d'autres attributs descriptifs utilisés dans le cadre de la gouvernance des risques.

Étape 7 : Création des instances. Les concepts de gouvernance sont instanciés dans le cadre de l'instanciation globale de l'ontologie intégrée, présentée au Chapitre V. Elle permet de vérifier leur cohérence au sein du modèle ainsi que leur rôle dans la représentation des relations entre les risques organisationnels, les objectifs stratégiques et les décisions de gouvernance.

La Figure 4.5 présente l'ontologie COSO ERM

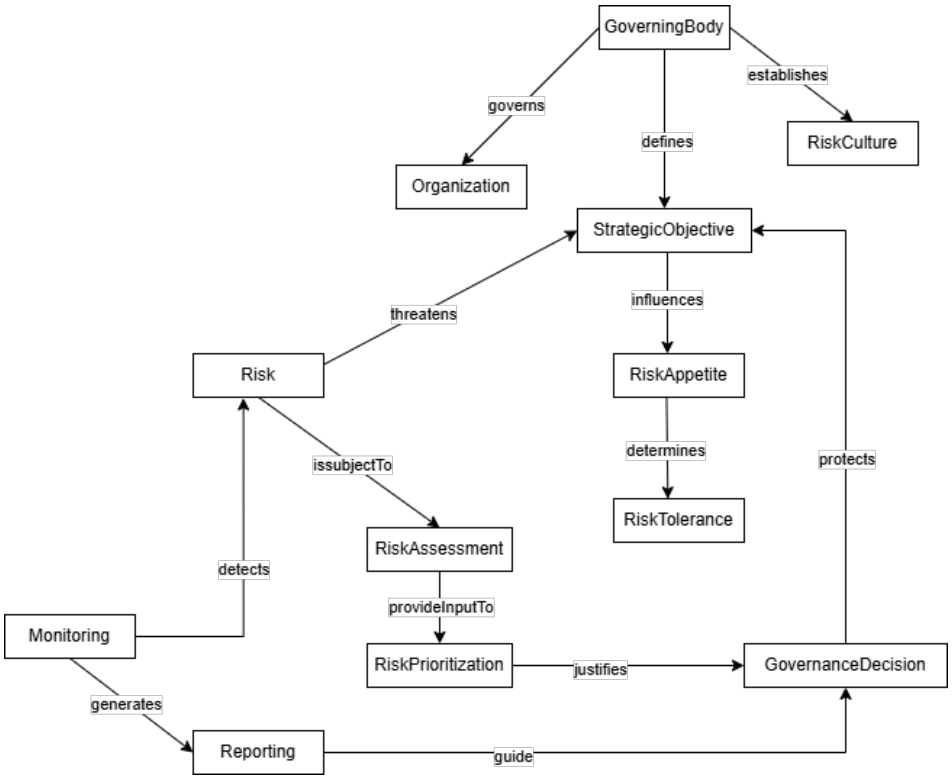

FIGURE 4.5 : Ontologie COSO ERM.

4.3 EXTENSION ET INTÉGRATION ONTOLOGIQUE

L'intégration d'ontologies issues de référentiels, de normes et de cadres de gouvernance en cybersécurité nécessite des mécanismes capables d'aligner des concepts provenant de modèles hétérogènes possédant des structures et des terminologies différentes. Dans ce contexte, le mapping ontologique constitue une approche importante permettant d'établir des correspondances formelles entre des concepts, des relations et des structures issus de différentes sources de connaissances (Fenz *et al.*, 2009).

Plusieurs travaux soulignent l'intérêt des approches d'extension et d'intégration ontologiques dans le domaine de la sécurité de l'information. Massacci *et al.* (2011) montrent que l'extension ontologique permet d'unifier différentes approches de l'ingénierie de sécurité

en intégrant des concepts liés aux acteurs, aux actifs, aux menaces, aux vulnérabilités et aux exigences de sécurité. Leur approche améliore la cohérence entre différents modèles tout en facilitant la validation des exigences de sécurité à partir de scénarios réels.

De manière similaire, Fenz *et al.* (2009) proposent une méthodologie de mapping visant à intégrer des standards et des guides de bonnes pratiques dans une ontologie de sécurité existante. Cette approche repose sur l'identification des correspondances entre concepts et relations ainsi que sur leur transformation en représentations OWL réutilisables au sein d'une ontologie commune.

Par ailleurs, Ramanauskaitė *et al.* (2013) proposent une approche de mapping adaptatif basée sur une ontologie pivot servant de couche d'abstraction commune entre plusieurs standards de sécurité hétérogènes. Organisée autour de concepts tels que les actifs, les menaces, les vulnérabilités, les organisations et les contre-mesures, cette approche réduit la complexité de l'intégration et facilite la génération automatique des correspondances entre référentiels.

D'autres travaux soulignent également l'importance de l'intégration ontologique et de l'interopérabilité dans les environnements de cybersécurité. Boinski *et al.* (2011) montrent que les exigences d'intégration doivent être prises en compte dès les premières étapes de conception des ontologies afin d'assurer leur compatibilité avec d'autres systèmes de connaissances. De même, Vorobiev *et al.* (2008) étendent les ontologies Security Asset and Vulnerability Ontology (SAVO), Security Attack Ontology (SAO) et Security Defense Ontology (SDO) afin d'établir des liens entre les politiques de sécurité, les mécanismes de défense et les cyberattaques dans les systèmes logiciels basés sur des composants.

Dans cette recherche, l'intégration progressive des connaissances issues des ontologies NIST SP 800-86, ISO/IEC 27005 et COSO ERM au sein de l'ontologie ISO/IEC 27035, utilisée comme référentiel d'ancrage, repose sur l'approche de mapping ontologique proposée

par Fenz *et al.* (2009). Cette approche a été développée pour intégrer des standards et des guides de bonnes pratiques dans une ontologie et comprend cinq étapes principales : l'analyse de l'ontologie, l'analyse de la base de connaissances, la mise en correspondance des concepts et des relations, l'intégration des connaissances et l'évaluation (Fenz *et al.*, 2009).

Conformément aux exigences de cette approche, les différentes sources de connaissances utilisées dans cette recherche sont disponibles sous une forme structurée et exploitable. L'ontologie NIST SP 800-86 ainsi que l'ontologie COSO ERM ont été développées dans cette recherche selon la méthodologie proposée par Noy *et al.* (2001). L'ontologie ISO/IEC 27005 s'appuie quant à elle sur les travaux d' Agrawal (2016). Ces trois ontologies constituent ainsi des sources de connaissances formelles compatibles avec le processus de mapping proposé par (Fenz *et al.*, 2009).

Étape 1 : Analyse de l'ontologie. Cette étape consiste à analyser l'ontologie cible avant le processus d'intégration. Une attention particulière est portée aux concepts et aux relations déjà présents afin de faciliter leur mise en correspondance avec les connaissances à intégrer. Dans cette recherche, cette étape correspond à l'analyse de l'ontologie ISO/IEC 27035 servant de référentiel d'ancrage.

Étape 2 : Analyse de la source de connaissances. Cette étape vise à analyser les ontologies NIST SP 800-86, ISO/IEC 27005 et COSO ERM afin d'identifier les concepts et relations présentant une similarité sémantique avec ceux déjà présents dans l'ontologie cible.

Étape 3 : Mise en correspondance des concepts et des relations. À partir des résultats des deux premières étapes, les concepts et relations issus des différentes ontologies sont mis en correspondance avec ceux de l'ontologie fondée sur la norme ISO/IEC 27035. Cette phase

permet d'identifier les concepts déjà existants ainsi que les nouveaux concepts nécessaires à l'enrichissement du modèle.

Cependant lorsque des entités communes sont nommées différemment dans les référentiels, leur correspondance ne repose pas uniquement sur leur nom, mais sur l'analyse de leur définition, de leurs propriétés et de leurs relations avec les autres entités. La concordance de ces éléments permet de déterminer si, malgré des appellations différentes, elles désignent une même réalité sémantique. Elles sont alors considérées comme équivalentes et représentées par une même entité dans l'ontologie intégrée.

Étape 4 : Intégration des connaissances. Cette étape consiste à intégrer les nouvelles connaissances au sein de l'ontologie cible à partir du schéma de correspondance établi précédemment. Dans cette recherche, elle permet l'intégration progressive des concepts liés à la forensic numérique, à la gestion des risques et à la gouvernance organisationnelle.

Étape 5 : Évaluation. La dernière étape vise à évaluer la cohérence et la validité de l'ontologie enrichie. Selon Fenz *et al.* (2009) cette phase peut nécessiter une validation manuelle des connaissances intégrées. Dans cette recherche, cette étape est réalisée au Chapitre V à travers les questions de compétence, les requêtes SPARQL et le raisonnement automatique.

Les quatre premières étapes sont appliquées dans les sections suivantes afin de décrire l'intégration des connaissances issues des ontologies NIST SP 800-86, ISO/IEC 27005 et COSO ERM au sein de l'ontologie ISO/IEC 27035 servant de référentiel d'ancrage.

4.3.1 EXTENSION NIST SP 800-86

La première extension du référentiel d'ancrage vise à intégrer la dimension de la criminalistique numérique à partir de l'ontologie NIST SP 800-86 développée précédemment. Bien que cette ontologie couvre un ensemble plus large de concepts liés à l'investigation numérique, seuls les concepts nécessaires aux objectifs de cette recherche ont été retenus pour enrichir le référentiel d'ancrage basé sur ISO/IEC 27035.

Analyse de l'ontologie : L'ontologie ISO/IEC 27035 a d'abord été analysée afin d'identifier les concepts déjà présents pouvant servir de points d'ancrage à l'intégration des concepts issus de l'ontologie NIST SP 800-86. Cette analyse a montré que les concepts *InformationSecurityIncident*, *InformationSecurityEvent*, *Threat*, *Vulnerability*, *IRT*, *Control*, *Operation* et *Asset* étaient déjà représentés dans le modèle.

Analyse de la source de connaissances : La deuxième étape a consisté à analyser l'ontologie NIST SP 800-86 développée précédemment afin d'identifier les concepts d'investigation numérique susceptibles d'enrichir l'ontologie intégrée. Le concept *ForensicProcess* modélise les activités d'investigation numérique menées à la suite d'un incident de sécurité, tandis que le concept *DigitalEvidence* représente les preuves numériques collectées, préservées et analysées au cours de ces investigations.

Mise en correspondance des concepts et des relations : La troisième étape a consisté à établir les correspondances entre les concepts identifiés dans l'ontologie NIST SP 800-86 et ceux déjà présents dans le référentiel d'ancrage. L'analyse a permis d'établir qu'un *InformationSecurityIncident triggers* un *ForensicProcess*, lequel *produces* des *DigitalEvidence*. Le *ForensicProcess feeds* également les activités d'*IncidentManagement*, *adjusts* les *Control*

existants et *qualifies* les *Threat*. Ces correspondances permettent de relier explicitement les activités d'investigation numérique aux mécanismes de gestion des incidents, de qualification des menaces et d'amélioration continue de la sécurité.

Intégration des connaissances : Les concepts *ForensicProcess* et *DigitalEvidence* ont été ajoutés au modèle conceptuel existant et reliés aux concepts de gestion des incidents, de menaces et de contrôles de sécurité. Cette extension introduit la dimension de l'investigation numérique au sein de l'ontologie intégrée tout en préservant la cohérence du référentiel d'ancrage basé sur ISO/IEC 27035.

Le Tableau 4.1 présente les éléments intégrés au référentiel d'ancrage à partir de l'ontologie NIST SP 800-86.

TABLEAU 4.1 : Éléments intégrés à partir du guide NIST SP 800-86

Type	**Éléments intégrés**
Concepts	ForensicProcess, DigitalEvidence
Relations	triggers, produces, feeds, adjusts, qualifies

4.3.2 EXTENSION ISO/IEC 27005

La deuxième extension vise à intégrer la dimension de gestion des risques à partir de l'ontologie ISO/IEC 27005 réutilisée dans cette recherche à partir des travaux d' Agrawal (2016). Bien que cette ontologie couvre un ensemble plus large de concepts relatifs à la gestion des risques liés à la sécurité de l'information, seuls les concepts nécessaires aux objectifs de cette recherche ont été retenus afin d'enrichir le référentiel d'ancrage.

Analyse de l'ontologie : L'ontologie ISO/IEC 27035 enrichie par l'extension forensic précédente a d'abord été analysée afin d'identifier les concepts déjà présents pouvant servir de points d'ancrage à l'intégration des concepts de gestion des risques. Cette analyse a montré que les concepts *InformationSecurityEvent*, *Risk*, *Vulnerability*, *Control*, *Threat* et *Asset* étaient déjà représentés dans le modèle.

Analyse de la source de connaissances : L'analyse de l'ontologie ISO/IEC 27005 proposée par Agrawal (2016) a permis d'identifier les concepts complémentaires nécessaires à l'enrichissement du référentiel d'ancrage. Les concepts retenus sont *Likelihood*, *Consequence*, *Objective*, *Organization* ainsi que les propriétés fondamentales de sécurité *Confidentiality*, *Integrity* et *Availability*, regroupées sous le concept *CIA*.

Mise en correspondance des concepts et des relations : Les concepts sélectionnés ont été mis en correspondance avec ceux déjà présents dans le référentiel d'ancrage afin de représenter la logique de gestion des risques. Ainsi, *InformationSecurityEvent has Likelihood* et *modifies Consequence* ; *Consequence affects Objective* ; *Organization has Objective* et *owns Asset* ; *Asset hasSecurityProperty CIA* ; *Risk contains Consequence* et *harms Organization* ; enfin, *Control mitigates Vulnerability*. Ces correspondances enrichissent la représentation des risques tout en préservant la cohérence du modèle conceptuel existant.

Intégration des connaissances : Les concepts *Likelihood*, *Consequence*, *Objective*, *Organization* et *CIA* ont ensuite été intégrés au modèle conceptuel. Cette extension complète la représentation des risques déjà présente dans le référentiel d'ancrage en ajoutant les notions de vraisemblance, de conséquence, d'objectif organisationnel, d'organisation et de propriétés fondamentales de sécurité de l'information.

Le Tableau 4.2 présente les éléments intégrés au référentiel d'ancrage à partir de l'ontologie ISO/IEC 27005.

TABLEAU 4.2 : Éléments intégrés à partir d'ISO/IEC 27005

Type	**Éléments intégrés**
Concepts	Likelihood, Consequence, Objective, Organization, CIA
Relations	has, modifies, affects, hasObjective, hasLikelihood, owns, hasSecurityProperty, contains, harms, mitigates

4.3.3 EXTENSION COSO ERM

La dernière extension vise à intégrer la dimension de gouvernance organisationnelle à travers l'ontologie COSO ERM développée précédemment. Contrairement aux extensions du cadre NIST SP 800-86 et de la norme ISO/IEC 27005, qui introduisent respectivement les dimensions de l'investigation numérique et de la gestion des risques, cette extension permet d'ajouter une couche de gouvernance à l'ontologie intégrée.

Analyse de l'ontologie : L'ontologie dérivée d'ISO/IEC 27035, enrichie par les extensions précédentes, a été analysée afin d'identifier les concepts existants pouvant servir de points d'ancrage à la gouvernance organisationnelle. Cette analyse a montré que les concepts *Risk* et *Organization* étaient déjà présents dans le modèle à la suite de l'intégration d'ISO/IEC 27005.

Analyse de la source de connaissances : La deuxième étape a consisté à analyser l'ontologie COSO ERM. Cette analyse a permis d'identifier les concepts de gouvernance nécessaires à l'enrichissement de l'ontologie intégrée, notamment *GoverningBody*, *StrategicObjective*,

RiskCulture, *RiskAppetite*, *RiskTolerance*, *RiskAssessment*, *RiskPrioritization*, *GovernanceDecision*, *Monitoring* et *Reporting*.

Mise en correspondance des concepts et des relations : La troisième étape a consisté à établir les correspondances entre les concepts de gouvernance et les concepts déjà présents dans l'ontologie enrichie. Les concepts *Risk* et *Organization* ont servi de points d'ancrage pour l'intégration des mécanismes de gouvernance. L'analyse a également permis d'établir que *ForensicProcess validates RiskAssessment* et que *Objective contributesTo StrategicObjective*. Ces correspondances permettent de relier les résultats des investigations forensic et les objectifs opérationnels aux mécanismes de gouvernance.

Intégration des connaissances : Cette étape consiste à intégrer les nouveaux concepts de gouvernance au sein de l'ontologie enrichie. Les concepts *GoverningBody*, *StrategicObjective*, *RiskCulture*, *RiskAppetite*, *RiskTolerance*, *RiskAssessment*, *RiskPrioritization*, *GovernanceDecision*, *Monitoring* et *Reporting* ont ainsi été ajoutés au modèle conceptuel. Cette extension permet de compléter l'ontologie intégrée en reliant les incidents de sécurité, les investigations numérique et les mécanismes de gestion des risques aux processus de gouvernance organisationnelle et de prise de décision stratégique.

Afin de synthétiser les résultats de cette phase d'intégration, le Tableau 4.3 présente les éléments ajoutés à l'ontologie intégrée à partir de l'ontologie COSO ERM.

TABLEAU 4.3 : Éléments intégrés à partir de l'ontologie COSO ERM

Type	**Éléments intégrés**
Concepts	GoverningBody, StrategicObjective, RiskCulture, RiskAppetite, RiskTolerance, RiskAssessment, RiskPrioritization, GovernanceDecision, Monitoring, Reporting
Relations	validates, contributesTo

CHAPITRE V

RÉSULTATS ET VALIDATION DE L'ONTOLOGIE

5.1 ONTOLOGIE INTÉGRÉE FINALE

Comme illustré à la Figure 5.1, l'ontologie intégrée finale capture les relations sémantiques établies entre les menaces, les vulnérabilités, les incidents, les preuves numériques, les processus forensic, les risques, les contrôles de sécurité, les mécanismes de gouvernance ainsi que les objectifs stratégiques organisationnels.

5.1.1 DÉFINITION DES PRINCIPAUX CONCEPTS

Les définitions présentées dans le Tableau 5.1 sont synthétisées et adaptées à partir des standards et travaux scientifiques utilisés dans cette recherche : l'ISO/IEC 27035 (ISO/IEC, 2023), l'ontologie ISO/IEC 27005 (Agrawal, 2016), le guide NIST SP 800-86 (Kent *et al.*, 2006) ainsi que le cadre COSO ERM (COSO, 2017; Efe, 2023).

5.1.2 SCÉNARIO DE CYBERATTAQUE

Afin de valider l'ontologie intégrée, un scénario réaliste de cyberattaque a été mis en œuvre dans un environnement contrôlé sous Graphical Network Simulator 3 (GNS3), un émulateur graphique permettant de concevoir, de configurer et de simuler des infrastructures réseau virtuelles (Korniyenko *et al.*, 2019), à travers une entreprise fictive de commerce électronique nommée **USHOP**. L'objectif de cette expérimentation est d'évaluer la capacité de l'ontologie intégrée à représenter les relations sémantiques entre les menaces, les incidents de sécurité, les investigations numériques, les risques et les décisions de gouvernance.

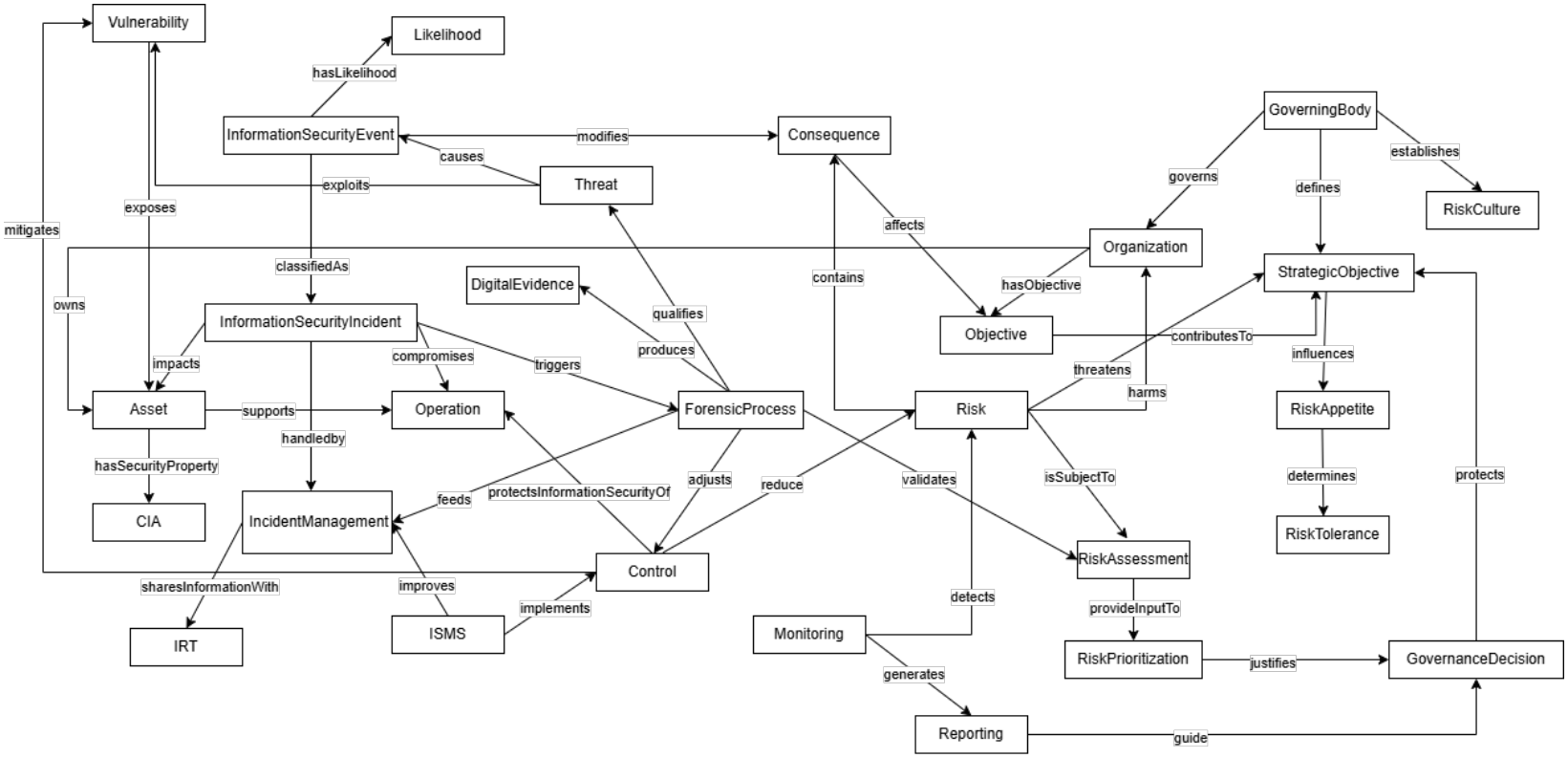

FIGURE 5.1 : Ontologie intégrée.

TABLEAU 5.1 : DÉFINITIONS DES CONCEPTS.

Concept ontologique	Définition
Asset	Ressource informationnelle ou technique ayant une valeur pour l'organisation.
CIA	Ensemble des propriétés de confidentialité, d'intégrité et de disponibilité.
Consequence	Impact négatif résultant d'un incident ou d'un risque.
Control	Mesure de sécurité permettant de réduire un risque ou protéger un actif.
DigitalEvidence	Donnée numérique utilisée dans une investigation forensic.
ForensicProcess	Processus de collecte, d'analyse et d'exploitation des preuves numériques.
GovernanceDecision	Décision stratégique liée à la gestion des risques et à la sécurité.
GoverningBody	Entité responsable de la gouvernance organisationnelle.
IncidentManagement	Processus de gestion et de traitement des incidents de sécurité.
InformationSecurityEvent	Événement observable lié à la sécurité de l'information.
InformationSecurityIncident	Événement compromettant la sécurité des actifs informationnels.
ISMS	Système de management de la sécurité de l'information.
IRT	Équipe responsable de la réponse aux incidents.
Likelihood	Probabilité d'occurrence d'un événement ou d'un risque.
Monitoring	Activité continue de surveillance des risques et événements.
Objective	Résultat ou finalité recherchée par l'organisation.
Operation	Activités nécessaires au fonctionnement de l'organisation.
Organization	Entité regroupant ressources, processus et objectifs.
Reporting	Activité de documentation et de communication des résultats.
Risk	Possibilité qu'une menace produise un impact négatif.
RiskAppetite	Niveau global de risque accepté par l'organisation.
RiskAssessment	Processus d'identification et d'évaluation des risques.
RiskCulture	Valeurs et comportements influençant la gestion des risques.
RiskPrioritization	Classement des risques selon leur importance.
StrategicObjective	Objectif stratégique à long terme de l'organisation.
RiskTolerance	Niveau acceptable de variation face aux risques.
Threat	Entité ou action capable d'exploiter une vulnérabilité.
Vulnerability	Faiblesse pouvant être exploitée par une menace.

L'architecture réseau simulée suit un modèle classique de segmentation d'entreprise composé de trois zones de sécurité interconnectées à travers un pare-feu :

— **Wide Area Network (WAN)** : (`192.168.253.0/24`) représentant le réseau externe et hébergeant la machine attaquante (`Kali Linux - 192.168.253.130`);

— **Demilitarized Zone (DMZ)** : (`192.168.187.0/24`) hébergeant le serveur Web Apache2 (`192.168.187.128`) exposé aux utilisateurs externes ;

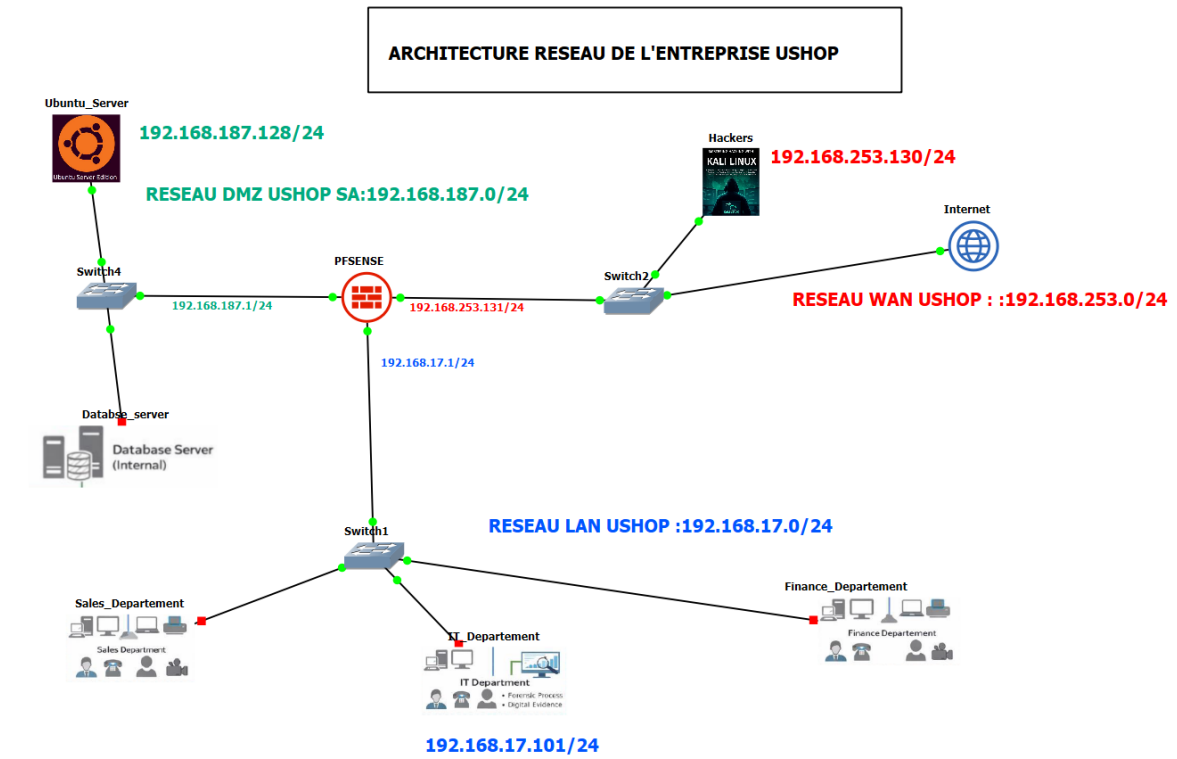

FIGURE 5.2 : Architecture réseau de l'entreprise USHOP.

— **Local Area Network (LAN)** : (`192.168.17.0/24`) contenant les systèmes internes de l'organisation ainsi que les différents départements opérationnels.

Comme illustré à la Figure 5.2, l'architecture organisationnelle simulée a été déployée sous GNS3 afin de reproduire un environnement réseau segmenté intégrant les zones WAN, DMZ et LAN interconnectées à travers un pare-feu.

Le pare-feu assure la séparation logique entre les différentes zones de sécurité et applique les règles de filtrage nécessaires. Les règles configurées sont présentées dans le Tableau 5.2.

TABLEAU 5.2 : Règles de sécurité appliquées sur le pare-feu

Interface	Action	Source	Destination	Description
WAN	Block	Réseaux Bogon	WAN	Blocage des réseaux non attribués ou considérés comme illégitimes par l'IANA.
WAN (NAT)	Pass	Any	192.168.187.128 :80	Redirection du trafic HTTP externe vers le serveur Apache hébergé dans la DMZ.
LAN	Pass	192.168.17.0/24	Any	Autorisation du trafic sortant du réseau interne vers les autres réseaux.
LAN	Pass	192.168.17.0/24	192.168.187.0/24	Autorisation d'accès des postes internes aux services hébergés dans la DMZ.
DMZ	Block	192.168.187.0/24	192.168.17.0/24	Interdiction des connexions initiées depuis la DMZ vers le réseau interne afin de limiter les mouvements latéraux.

Cette configuration permet la publication du serveur Web vers Internet tout en maintenant une séparation entre les ressources exposées dans la DMZ et les systèmes internes de l'organisation. Les tests de connectivité réalisés au cours de l'expérimentation ont confirmé l'accessibilité du serveur Web depuis l'internet ainsi que l'isolation du réseau LAN vis-à-vis des connexions initiées depuis la DMZ.

Le scénario de cyberattaque est de type Transmission Control Protocol (TCP) Synchronize Sequence Numbers (SYN) Flood ciblant le serveur Web hébergé dans la zone DMZ. L'attaquant génère un volume important de requêtes TCP SYN incomplètes afin de saturer la file d'attente des connexions du serveur Web. Cette cyberattaque vise à provoquer une indisponibilité du service Web pour les utilisateurs légitimes.

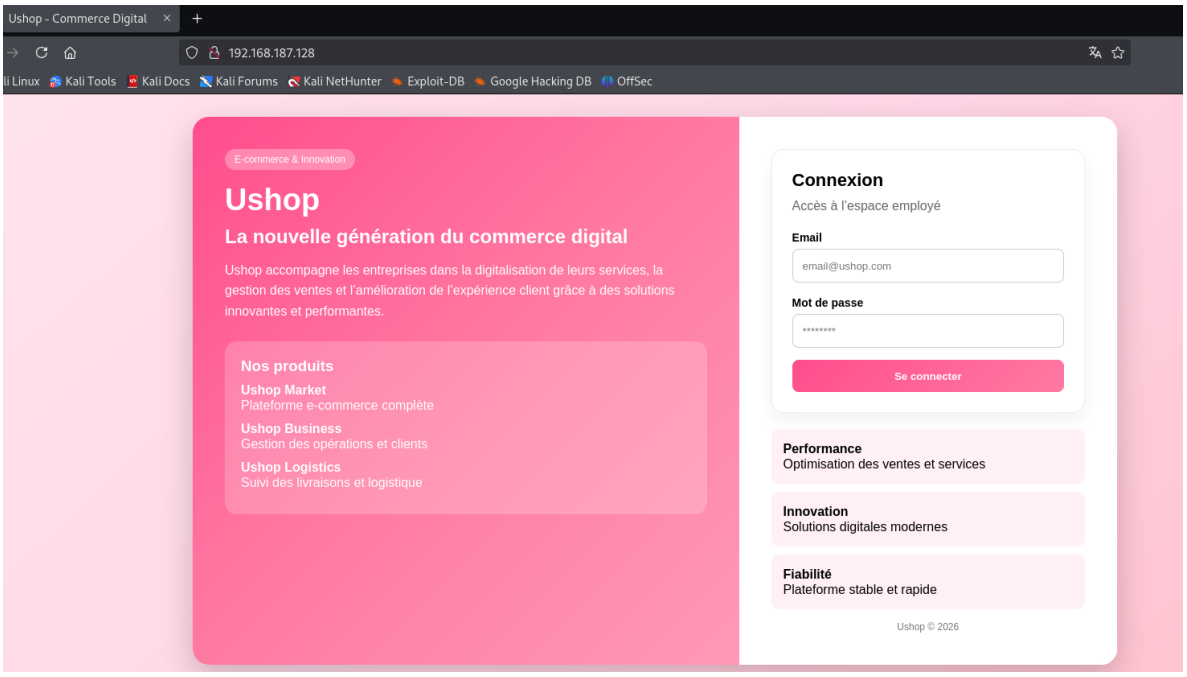

FIGURE 5.3 : Plateforme web USHOP avant l'attaque SYN Flood.

Bien que le pare-feu pfSense fournisse une segmentation réseau efficace, aucune mesure spécifique de protection contre les cyberattaques TCP SYN Flood n'était activée au moment de l'expérimentation. En particulier, les mécanismes tels que les *SYN Cookies*, les limitations de connexions (*Rate Limiting*), les systèmes de détection et de prévention d'intrusion (IDS/IPS) ou encore les protections avancées contre les cyberattaques de saturation n'étaient pas déployés.

La Figure 5.3 présente la plateforme web USHOP fonctionnant dans des conditions normales avant l'exécution de la cyberattaque TCP SYN Flood.

5.1.3 ANALYSE FORENSIC

L'intégrité des preuves numériques collectées a été vérifiée à l'aide de fonctions de hachage cryptographique. L'analyse statistique du trafic capturé à l'aide de *Wireshark*, un

analyseur de protocoles réseau permettant de capturer, d'inspecter et d'analyser le trafic réseau en temps réel (Soepeno, 2023), a permis d'obtenir les indicateurs suivants :

— **Nombre total de paquets :** 546 801 ;

— **Durée de la capture :** 26 secondes ;

— **Débit moyen :** environ 10 Mbps ;

— **Paquets par seconde :** environ 20 762 pps ;

— **Taille moyenne des paquets :** 60 octets ;

— transmission massive de paquets TCP SYN ;

— absence de réponses SYN-ACK provenant du serveur cible ;

— réutilisation répétée des ports sources TCP ;

— handshakes TCP incomplets ;

L'analyse détaillée du trafic capturé met en évidence la transmission de 546 801 segments TCP d'une taille moyenne de 60 octets vers le serveur USHOP durant une période de 26 secondes, avec un débit moyen d'environ 10 Mbps et un taux d'émission de près de 20 762 paquets par seconde.La faible taille moyenne des paquets combinée au nombre élevé de paquets observés suggère la présence d'un trafic généré artificiellement.

Les graphiques E/S (Entrées/Sorties) produits par Wireshark, montrent une augmentation du trafic compris entre environ 18 000 et 25 000 paquets par seconde, comme illustré à la Figure 5.4. Les barres rouges correspondent aux événements identifiés comme des erreurs TCP par Wireshark (`tcp.analysis.flags`), tandis que la courbe noire représente l'ensemble des paquets capturés. La concentration de ces événements est caractéristique d'un trafic anormal susceptible d'entraîner l'épuisement des ressources du serveur.

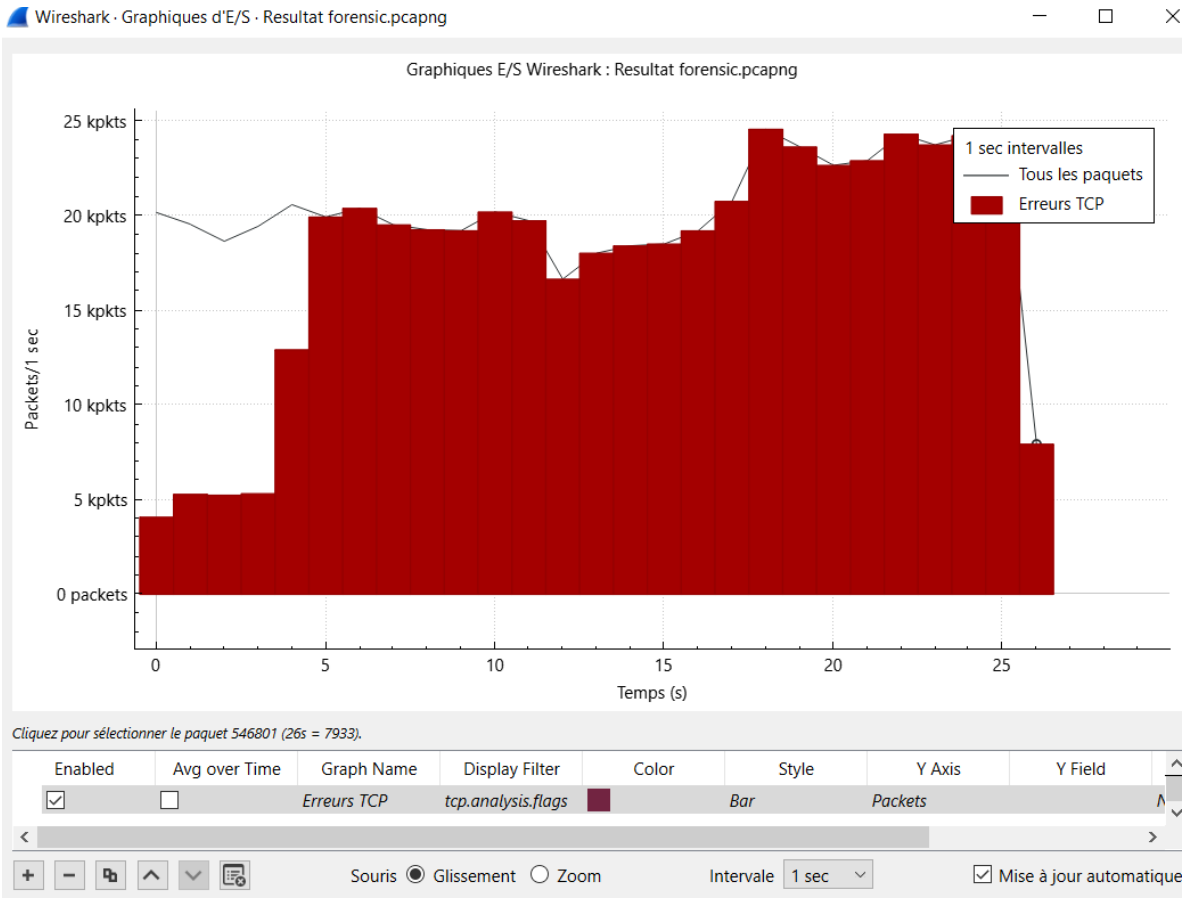

FIGURE 5.4 : Graphique E/S (Entrées/Sorties) de Wireshark illustrant l'évolution du trafic réseau et des événements TCP observés durant l'attaque.

L'analyse indique que les ressources du serveur ont été progressivement saturées par une cyberattaque TCP SYN Flood, provoquant l'indisponibilité complète de la plateforme de commerce électronique USHOP.

5.1.4 INSTANCIATION DE L'ONTOLOGIE

Le scénario de cyberattaque USHOP a été utilisé afin d'instancier les concepts et relations de l'ontologie integrée. Les observations forensic collectées durant l'expérimentation

TABLEAU 5.3 : Exemples d'instances extraites du scénario forensic USHOP.

Concept ontologique	**Instance du scénario**
Threat	`DoS_Threat`
Vulnerability	`Absence_Protection_SYN_Flood`
InformationSecurityEvent	`Web_Service_Unavailability`
InformationSecurityIncident	`SYN_Flood_Attack`
IncidentManagement	`Incident_Response_Process_USHOP`
Asset	`Web_Server_192.168.187.128`
Operation	`Ecommerce_Operations_USHOP`
ForensicProcess	`Forensic_Analysis_Wireshark`
DigitalEvidence	`PCAP_Resultat_forensic`
Risk	`Business_Continuity_Risk`
GovernanceDecision	`Approve_Cybersecurity_Improvement_-Plan`
Control	`Activate_SYN_Protection`, `Deploy_IDS_-IPS`
StrategicObjective	Maintain_Business_Continuity

ont été associées aux différentes classes dans le but de valider la cohérence sémantique du modèle intégré. La Table 5.3 présente les instances du scénario.

L'ontologie intégrée a été entièrement instanciée sous Protégé, une plateforme open source de modélisation d'ontologies permettant de créer, d'éditer et d'instancier des ontologies OWL (Knublauch *et al.*, 2004), à partir du scénario USHOP.

La Figure 5.5 illustre un exemple d'instanciation de l'ontologie sous Protégé.

5.2 VALIDATION AU MOYEN DE QUESTIONS DE COMPÉTENCE

Les questions de compétence (*Competency Questions*) correspondent à un ensemble de questions auxquelles une base de connaissances fondée sur l'ontologie doit être capable de

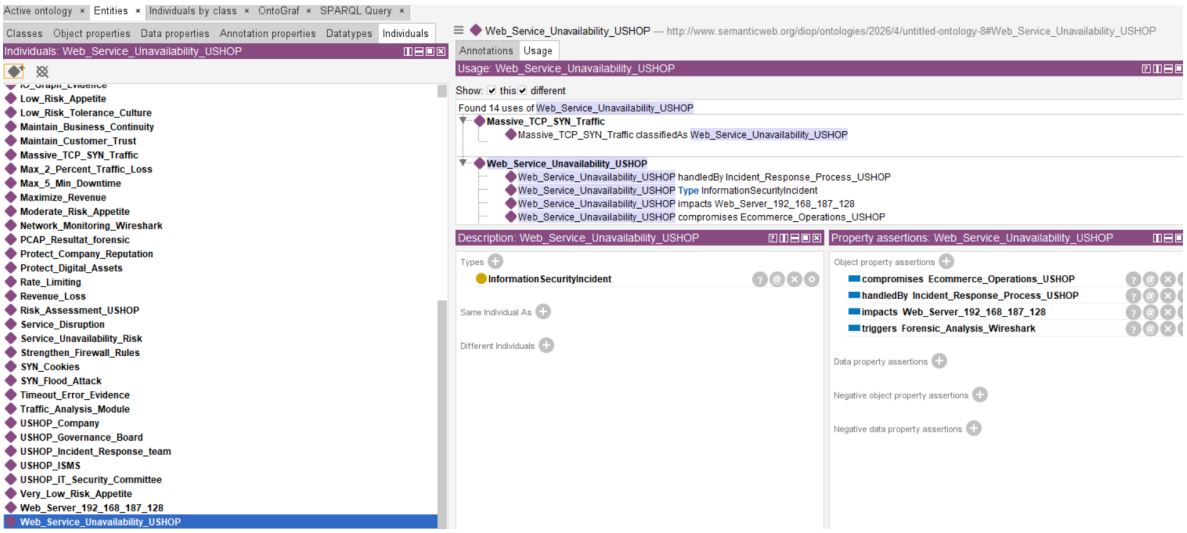

FIGURE 5.5 : Exemple d'instanciation de l'ontologie sous Protégé.

répondre. Elles servent à la fois à délimiter le périmètre de l'ontologie lors de sa conception et à constituer un critère de validation visant à vérifier que l'ontologie contient les connaissances nécessaires pour satisfaire les besoins identifiés (Noy *et al.*, 2001).

Cette section présente la validation de l'ontologie intégrée au moyen d'un ensemble de questions de compétence couvrant la gestion des incidents de sécurité, l'investigation numérique, la gestion des risques ainsi que la gouvernance organisationnelle. Les questions sont organisées de manière progressive afin d'évaluer la capacité du modèle à établir des liens sémantiques entre ces différents domaines..

5.2.1 CQ1 — MENACE, VULNÉRABILITÉ ET INCIDENT

Question de compétence : Quelle menace a exploité quelle vulnérabilité pour provoquer un incident de sécurité ?

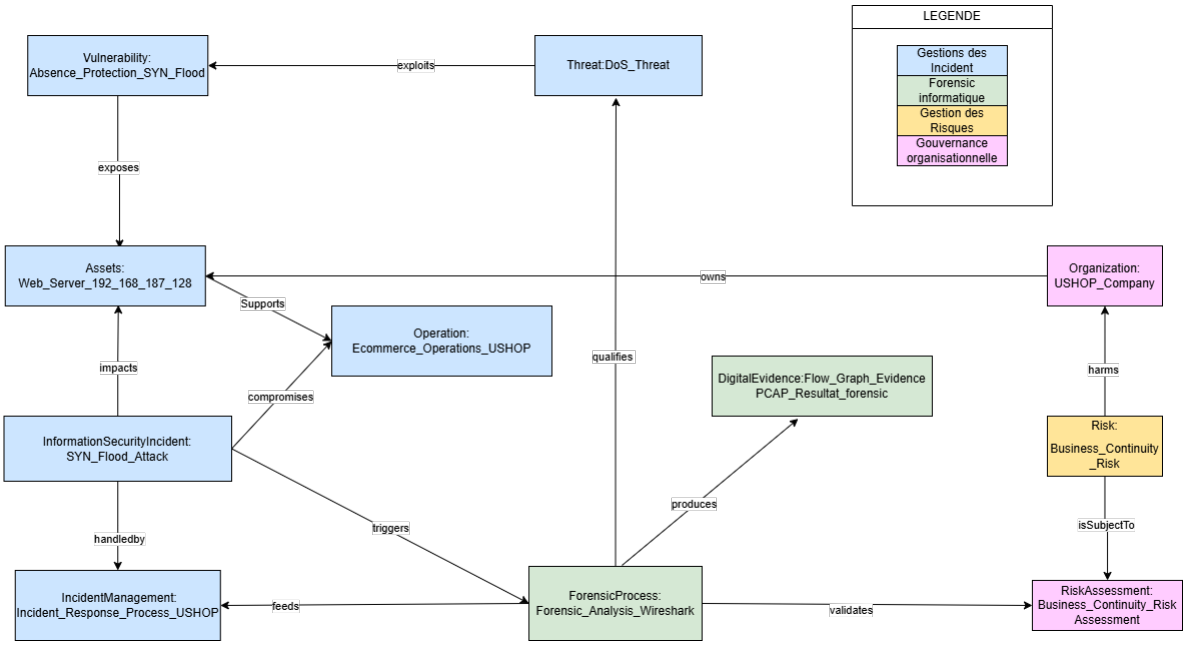

FIGURE 5.6 : Instances et relations identifiées par l'ontologie pour répondre aux questions de compétence CQ1 à CQ5.

Cette question vise à vérifier que l'ontologie intégrée permet de représenter le lien entre une menace, une vulnérabilité exploitée et l'incident de sécurité qui en résulte. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.7. Cette requête permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `Threat`, `Vulnerability`, `InformationSecurityEvent` et `InformationSecurityIncident`.

Les résultats présentés dans la Figure 5.6 montrent que la menace `DoS Threat` exploite la vulnérabilité `Absence Protection SYN Flood`. Cette exploitation provoque l'événement de sécurité `Web Service Unavailability`, lequel est classifié comme l'incident `SYN Flood Attack`. Ces résultats confirment que l'ontologie intégrée permet de représenter la chaîne causale allant d'une menace exploitant une vulnérabilité jusqu'à la classification en incident de sécurité.

```
SELECT ?Threat ?Vulnerability ?Event ?Incident
WHERE {
    ?Threat      rdf:type :Threat .
    ?Vulnerability rdf:type :Vulnerability .
    ?Event       rdf:type :InformationSecurityEvent .
    ?Incident    rdf:type :InformationSecurityIncident .

    ?Threat :exploits ?Vulnerability .
    ?Threat :causes   ?Event .
    ?Event  :classifiedAs ?Incident .
}
```

FIGURE 5.7 : Requête SPARQL utilisée pour répondre à la question de compétence CQ1.

```
SELECT ?Incident ?ForensicProcess ?DigitalEvidence
WHERE {
    ?Incident       rdf:type :InformationSecurityIncident .
    ?ForensicProcess rdf:type :ForensicProcess .
    ?DigitalEvidence rdf:type :DigitalEvidence .

    ?Incident        :triggers ?ForensicProcess .
    ?ForensicProcess :produces ?DigitalEvidence .
}
```

FIGURE 5.8 : Requête SPARQL utilisée pour répondre à la question de compétence CQ2.

5.2.2 CQ2 — INVESTIGATION FORENSIC ET PREUVES NUMÉRIQUES

Question de compétence : Quelles preuves numériques ont été collectées dans le cadre de l'investigation de cet incident ?

Cette question permet de vérifier que l'ontologie intégrée relie un incident de sécurité au processus d'investigation déclenché et aux preuves numériques produites.Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.8. Cette requête permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `InformationSecurityIncident`, `ForensicProcess` et `DigitalEvidence`.

```
SELECT ?Incident ?Asset ?Operation
WHERE {
    ?Incident  rdf:type :InformationSecurityIncident .
    ?Asset     rdf:type :Asset .
    ?Operation rdf:type :Operation .

    ?Incident :compromises ?Operation .
    ?Asset    :supports    ?Operation .
}
```

FIGURE 5.9 : Requête SPARQL utilisée pour répondre à la question de compétence CQ3.

Les résultats montrent que l'incident `SYN Flood Attack` déclenche le processus forensic `Forensic Analysis Wireshark`. Ce processus produit plusieurs preuves numériques, notamment `Flow Graph Evidence` et `PCAP Resultat forensic`. Ces résultats démontrent que l'ontologie intégrée est en mesure d'établir un lien entre l'incident investigué et les preuves numériques collectées au cours de l'investigation forensic.

5.2.3 CQ3 — ACTIFS INFORMATIONNELS ET OPÉRATIONS CRITIQUES AFFECTÉS

Question de compétence : Quels actifs informationnels et quelles opérations critiques ont été affectés par cet incident ?

Cette question vise à vérifier la capacité de l'ontologie intégrée à relier un incident aux actifs informationnels et aux opérations critiques de l'organisation. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.9. Cette requête permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `InformationSecurityIncident`, `Asset` et `Operation`.

```
SELECT ?Incident ?Organization ?Asset ?Operation ?Risk
WHERE {
    ?Incident     rdf:type :InformationSecurityIncident .
    ?Organization rdf:type :Organization .
    ?Asset        rdf:type :Asset .
    ?Operation    rdf:type :Operation .
    ?Risk         rdf:type :Risk .

    ?Incident     :compromises ?Operation .
    ?Asset        :supports    ?Operation .
    ?Organization :owns        ?Asset .
    ?Risk         :harms       ?Organization .
}
```

FIGURE 5.10 : Requête SPARQL utilisée pour répondre à la question de compétence CQ4.

Les résultats indiquent que l'incident `SYN Flood Attack` compromet l'opération critique `Ecommerce Operation USHOP`. Cette opération est supportée par l'actif informationnel `Web Server 192 168 187 128`. Cette réponse montre que l'ontologie intégrée permet de relier un incident aux ressources techniques et aux opérations critiques affectées.

5.2.4 CQ4 — RISQUES ORGANISATIONNELS ASSOCIÉS AUX ACTIFS AFFECTÉS

Question de compétence : Quels risques organisationnels sont associés aux actifs affectés par cet incident ?

Cette question permet de vérifier que l'ontologie intégrée établit un lien entre les actifs affectés, les opérations critiques, les risques et l'organisation. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.10. Cette requête permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `InformationSecurityIncident`, `Organization`, `Asset`, `Operations` et `Risk`.

```
SELECT ?ForensicProcess ?DigitalEvidence ?RiskAssessment ?Risk
WHERE {
    ?ForensicProcess rdf:type :ForensicProcess .
    ?DigitalEvidence rdf:type :DigitalEvidence .
    ?RiskAssessment  rdf:type :RiskAssessment .
    ?Risk            rdf:type :Risk .

    ?ForensicProcess :produces  ?DigitalEvidence .
    ?ForensicProcess :validates ?RiskAssessment .
    ?Risk            :isSubjectTo ?RiskAssessment .
}
```

FIGURE 5.11 : Requête SPARQL utilisée pour répondre à la question de compétence CQ5.

Les résultats montrent que l'organisation `USHOP Company` possède l'actif `Web Server 192 168 187 128`, lequel supporte l'opération critique `Ecommerce Operations USHOP`. Le risque `Business Continuity Risk` affecte cette organisation. Cette réponse confirme que l'ontologie intégrée permet de relier les actifs et opérations affectés aux risques.

5.2.5 CQ5 — CONTRIBUTION DE L'INVESTIGATION NUMÉRIQUE À L'ÉVALUATION DES RISQUES

Question de compétence : Quels éléments issus de l'investigation numérique contribuent à l'évaluation ou à la réévaluation de ces risques ?

Cette question vise à valider le lien sémantique entre les résultats d'investigation numérique et l'évaluation des risques. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.11. Cette requête permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `ForensicProcess`, `DigitalEvidence`, `RiskAssessment` et `Risk`.

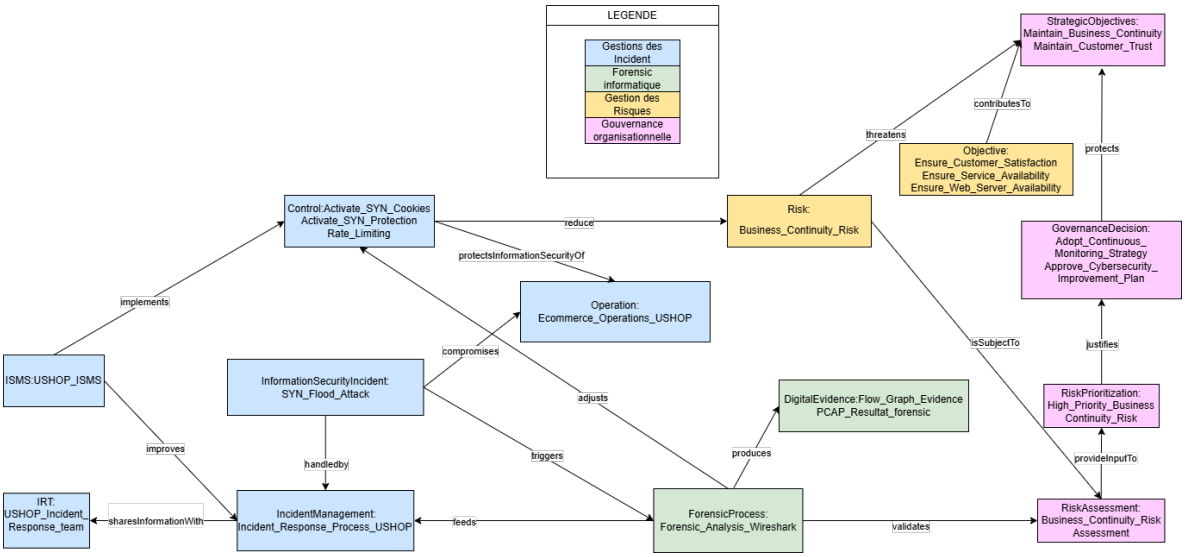

FIGURE 5.12 : Instances et relations identifiées par l'ontologie intégrée pour répondre aux questions de compétence CQ6 à CQ8.

Les résultats montrent que le processus `Forensic Analysis Wireshark` produit les preuves numériques `Flow Graph Evidence` et `PCAP Resultat forensic`. Ce même processus valide l'évaluation `Business Continuity Risk Assessment`, à laquelle est soumis le risque `Business Continuity Risk`. Cette relation démontre que les éléments issus de l'investigation forensic contribuent directement à l'évaluation ou à la réévaluation des risques.

5.2.6 CQ6 — DÉCISIONS DE GOUVERNANCE ASSOCIÉES AUX RISQUES

Question de compétence : Quelles décisions de gouvernance sont associées aux risques identifiés ?

Cette question vise à vérifier que l'ontologie intégrée relie les risques évalués aux mécanismes de priorisation et aux décisions de gouvernance. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.13. Cette requête permet d'interroger

```
SELECT ?Risk ?RiskAssessment ?RiskPrioritization ?GovernanceDecision
WHERE {
    ?Risk                rdf:type :Risk .
    ?RiskAssessment      rdf:type :RiskAssessment .
    ?RiskPrioritization  rdf:type :RiskPrioritization .
    ?GovernanceDecision  rdf:type :GovernanceDecision .

    ?Risk               :isSubjectTo ?RiskAssessment .
    ?RiskAssessment     :provideInputTo   ?RiskPrioritization .
    ?RiskPrioritization :justifies   ?GovernanceDecision .
}
```

FIGURE 5.13 : Requête SPARQL utilisée pour répondre à la question de compétence CQ6.

l'ontologie intégrée pour identifier les relations entre les instances de `Risk`, `RiskAssessment`, `RiskPrioritization` et `GovernanceDecision`.

Les résultats présentés dans la Figure 5.12 montrent que le risque `Business Continuity Risk` est soumis à l'évaluation `Business Continuity Risk Assessment`. Cette évaluation fournit les données d'entrée à la priorisation `High Priority Business Continuity Risk`, laquelle justifie les décisions de gouvernance `Approve Cybersecurity Improvement Plan` et `Adopt Continuous Monitoring Strategy`. Ces résultats confirment que l'ontologie intégrée permet de relier l'évaluation des risques à la prise de décision organisationnelle.

5.2.7 CQ7 — CONTRÔLES DE SÉCURITÉ ASSOCIÉS AUX RISQUES

Question de compétence : Quels contrôles de sécurité sont associés aux risques identifiés et aux décisions de gouvernance ?

Cette question vise à vérifier que l'ontologie intégrée permet de relier les décisions de gouvernance aux contrôles de sécurité mis en œuvre pour réduire les risques. Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.14. Cette requête

```
SELECT ?GovernanceDecision ?Control ?ISMS ?Risk
WHERE {
    ?GovernanceDecision rdf:type :GovernanceDecision .
    ?Control            rdf:type :Control .
    ?ISMS               rdf:type :ISMS .
    ?Risk               rdf:type :Risk .

    ?RiskPrioritization :justifies   ?GovernanceDecision .
    ?ISMS               :implements  ?Control .
    ?Control            :reduces     ?Risk .
}
```

FIGURE 5.14 : Requête SPARQL utilisée pour répondre à la question de compétence CQ7.

permet d'interroger l'ontologie intégrée pour identifier les relations entre les instances de `GovernanceDecision`, `Control`, `ISMS` et `Risk`

Les résultats montrent que le système de management de la sécurité de l'information `USHOP ISMS` implémente plusieurs contrôles de sécurité, notamment `Activate SYN Cookies`, `Activate SYN Protection` et `Rate Limiting`. Ces contrôles contribuent à réduire le risque `Business Continuity Risk`. Cette réponse montre que l'ontologie intégrée permet de relier les risques identifiés aux contrôles de sécurité mis en œuvre dans le cadre de management de la sécurité de l'information.

5.2.8 CQ8 — OBJECTIFS STRATÉGIQUES EXPOSÉS PAR LES RISQUES

Question de compétence : Quels objectifs stratégiques de l'organisation sont exposés par les risques résultant de ces incidents ?

Cette question vise à vérifier que l'ontologie intégrée permet de relier les risques aux objectifs stratégiques de l'organisation.Cette vérification a été réalisée au moyen d'une requête SPARQL présentée à la Figure 5.15. Cette requête permet d'interroger l'ontologie intégrée

```
SELECT ?Risk ?Organization ?GoverningBody ?StrategicObjective
WHERE {
    ?Risk              rdf:type :Risk .
    ?Organization      rdf:type :Organization .
    ?GoverningBody     rdf:type :GoverningBody .
    ?StrategicObjective rdf:type :StrategicObjective .

    ?Risk          :harms            ?Organization .
    ?Risk          :threatens         ?StrategicObjective .
    ?GoverningBody :governs          ?Organization .
    ?GoverningBody :defines          ?StrategicObjective .
}
```

FIGURE 5.15 : Requête SPARQL utilisée pour répondre à la question de compétence CQ8.

pour identifier les relations entre les instances de `Risk`, `Organization`, `GoverningBody` et `Strategic_Objective`.

Les résultats montrent que le risque `Business Continuity Risk` affecte les objectifs stratégiques `Maintain Business Continuity` et `Maintain Customer Trust`. L'organe de gouvernance `USHOP Governance Board` gouverne l'organisation `USHOP Company` et définit ces objectifs stratégiques. Cette réponse confirme que l'ontologie intégrée permet de représenter l'exposition des objectifs stratégiques aux risques résultant d'un incident de sécurité de l'information.

5.2.9 SYNTHÈSE

Les huit questions de compétence ont permis de valider progressivement les différentes dimensions de l'ontologie intégrée. Les questions CQ1 à CQ5 ont confirmé la capacité à représenter la chaîne reliant une menace à une vulnérabilité exploitée, à un événement de sécurité puis à un incident, aux preuves numériques produites lors de l'investigation numérique, ainsi qu'aux actifs informationnels, aux opérations critiques et aux risques organisationnels

affectés. Les questions CQ6 à CQ8 ont ensuite montré que les risques identifiés peuvent être reliés aux mécanismes de gouvernance, aux décisions organisationnelles, aux contrôles de sécurité mis en œuvre ainsi qu'aux objectifs stratégiques de l'entreprise.

La Figure 5.16 présente une vue consolidée des instances et des relations mobilisées pour répondre à l'ensemble des questions de compétence. Cette représentation met en évidence la continuité sémantique entre la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle. Elle illustre notamment comment une menace exploitant une vulnérabilité peut conduire à un événement de sécurité puis à un incident, déclencher une investigation numérique produisant des preuves numériques, contribuer à l'évaluation et à la priorisation des risques, et finalement soutenir des décisions de gouvernance visant à protéger les objectifs stratégiques de l'organisation.

Ainsi, les résultats obtenus montrent que l'ontologie intégrée ne constitue pas uniquement une représentation statique des concepts issus de plusieurs référentiels de cybersécurité, mais qu'elle est également capable de soutenir un raisonnement inter-domaines couvrant la gestion des incidents, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle, tel qu'illustré par les questions de compétence satisfaites.

5.3 VALIDATION PAR RAISONNEMENT AUTOMATIQUE

Afin d'évaluer la cohérence logique de l'ontologie intégrée, le raisonneur HermiT a été exécuté sous Protégé. HermiT est un moteur de raisonnement conforme au standard OWL 2 permettant de vérifier la cohérence logique d'une ontologie, de détecter les classes insatisfiables et de déduire automatiquement de nouvelles connaissances à partir des axiomes définis (Glimm *et al.*, 2014). La validation par raisonnement automatique a été réalisée en trois étapes. Dans un premier temps, une première exécution de HermiT a permis d'exami-

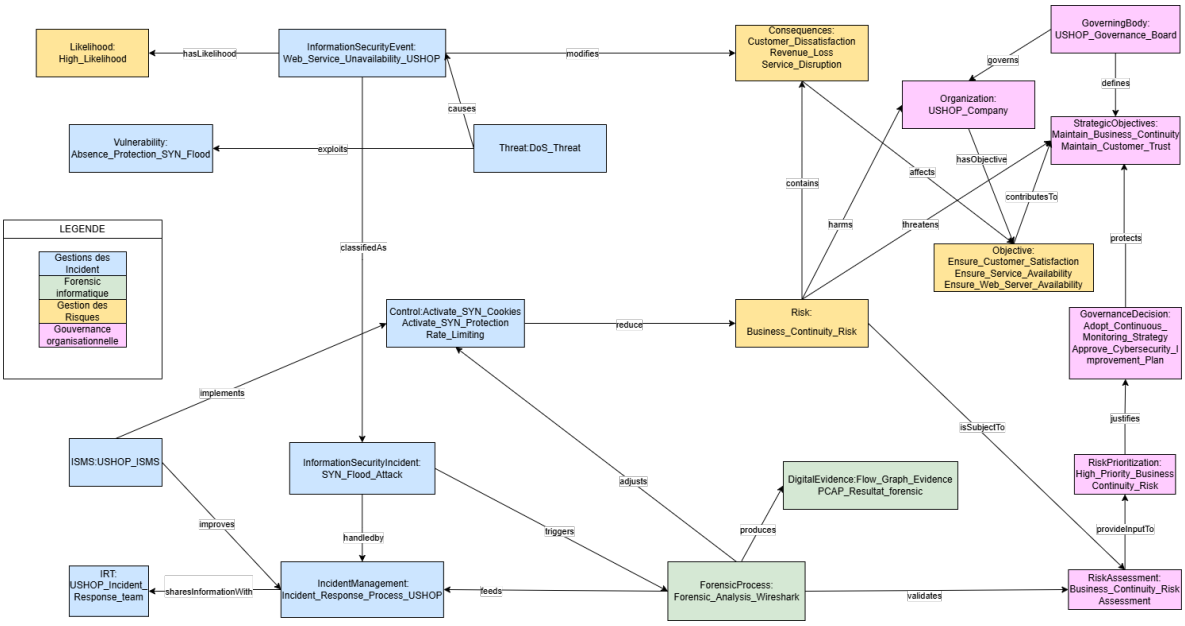

FIGURE 5.16 : Chaîne sémantique complète reliant une menace exploitant une vulnérabilité aux objectifs stratégiques de l'organisation à travers les processus de gestion des incidents, d'investigation forensic, de gestion des risques et de gouvernance.

ner les classifications produites par l'ontologie intégrée et d'identifier certaines erreurs de modélisation. Ces erreurs se manifestaient par des classifications de certains individus ne correspondant pas aux relations attendues au regard des cadres de référence formalisés dans l'ontologie. Dans un deuxième temps, les erreurs identifiées ont été corrigées en révisant les domaines et les portées de certaines propriétés objets, afin d'éviter des classifications non conformes au domaine modélisé.

Dans un troisième temps, HermiT a été exécuté de nouveau sur l'ontologie corrigée. Cette seconde exécution n'a révélé aucune classe insatisfiable, ce qui confirme la cohérence logique de l'ontologie finale. Le raisonneur a produit trois nouvelles assertions de classes, faisant passer leur nombre de 61 à 64. Le Tableau 5.4 présente les principales métriques obtenues avant et après l'exécution finale du raisonneur HermiT.

TABLEAU 5.4 : Comparaison des métriques avant et après le raisonnement final.

Métrique	**Avant**	**Après**	**Diff.**
Nombre total d'axiomes	385	388	+3
Axiomes logiques	245	248	+3
Individus	61	61	0
Assertions de classes	61	64	+3

TABLEAU 5.5 : Assertions de classes inférées après correction.

Individu	**Classe inférée**
Web_Service_Unavailability_USHOP	*InformationSecurityEvent*
Maintain_Business_Continuity	*Objective*
Protect_Digital_Assets	*Objective*

L'augmentation identique de trois unités observée pour le nombre total d'axiomes, les axiomes logiques et les assertions de classes traduit le même phénomène. En effet, chaque assertion de classe inférée par HermiT est représentée sous la forme d'un axiome logique, lequel est lui-même comptabilisé dans le nombre total d'axiomes. Ces trois métriques ne constituent donc pas des résultats indépendants, mais décrivent les inférences produites selon trois niveaux de granularité différents. Cette correspondance confirme que les trois nouvelles assertions de classes représentent l'ensemble des connaissances supplémentaires déduites par le raisonneur. Les trois assertions de classes inférées par le raisonneur HermiT après correction sont présentées dans le Tableau 5.5.

Ces inférences sont cohérentes avec le scénario USHOP. L'individu *Web_Service_Unavailability_USHOP*, initialement typé comme instance de `InformationSecurityIncident`, est inféré par le raisonneur comme instance de `InformationSecurityEvent`, ce qui reflète le fait qu'une indisponibilité du service Web constitue également un événement de sécurité affectant les opérations de l'organisation. De même, les individus *Maintain_Business_Continuity*

et *Protect_Digital_Assets*, initialement typés comme instances de `Strategic_Objectives`, sont inférés comme instances de `Objective`, dans la mesure où ils représentent des objectifs organisationnels liés à la continuité des activités et à la protection des actifs numériques.

Ainsi, la validation par raisonnement automatique confirme la cohérence logique de l'ontologie et illustre sa capacité à produire des connaissances implicites cohérentes avec le domaine modélisé.

5.4 LIMITES DE LA RECHERCHE

Malgré les résultats obtenus, plusieurs limites doivent être soulignées.

La première limite concerne le scénario de validation utilisé. L'évaluation repose sur un unique scénario SYN Flood implémenté dans un environnement contrôlé. Bien que ce scénario permette de valider les relations entre les incidents, les investigations numériques, les risques et la gouvernance, il ne couvre pas toute la diversité des cybermenaces auxquelles les organisations sont confrontées. Des scénarios plus complexes impliquant des rançongiciels, du phishing ou des compromissions d'identifiants permettraient d'évaluer plus largement la capacité de l'ontologie intégrée à représenter des situations réelles de cybersécurité.

La deuxième limite concerne le processus de construction et de mapping ontologique. Malgré l'utilisation de méthodologies reconnues, l'identification des concepts pertinents et l'établissement des correspondances entre les différents référentiels reposent sur l'expertise du chercheur. Cette démarche peut introduire une certaine subjectivité dans l'ontologie intégrée obtenue. Une validation complémentaire réalisée par des experts du domaine ou par l'application de l'ontologie intégrée à des données réelles permettrait de renforcer davantage sa validité externe.

Enfin, les capacités d'inférence reposent essentiellement sur les mécanismes standards du langage OWL et du raisonneur HermiT. Des approches plus avancées fondées sur des règles SWRL, des graphes de connaissances ou des techniques d'intelligence artificielle pourraient permettre d'enrichir les capacités de raisonnement de l'ontologie intégrée.

5.5 PERSPECTIVES DE RECHERCHE

Plusieurs pistes peuvent être envisagées afin de prolonger cette recherche.

Une première perspective consiste à valider l'ontologie intégrée à travers d'autres scénarios de cyberattaque, notamment des attaques par rançongiciel, des campagnes de phishing, des compromissions d'identifiants ou encore des incidents touchant des environnements infonuagiques.

Une deuxième perspective concerne l'expérimentation de l'ontologie intégrée dans des environnements opérationnels réels, notamment dans des contextes de gestion des incidents, d'investigation numérique, d'évaluation des risques et de gouvernance, afin d'améliorer l'interopérabilité entre ces domaines au sein des organisations.

Enfin, l'automatisation du processus de mapping ontologique à l'aide de techniques d'intelligence artificielle pourrait faciliter l'intégration de nouveaux référentiels et l'évolution continue de l'ontologie intégrée.

CONCLUSION

La fragmentation des cadres normatifs en cybersécurité, chacun couvrant un domaine spécifique avec sa propre terminologie et ses propres structures conceptuelles, limite la capacité des organisations à disposer d'une vision unifiée de leur exposition aux cyberrisques. Bien que plusieurs ontologies aient déjà été développées pour répondre à des besoins spécifiques en cybersécurité, aucune, à notre connaissance, n'intègre conjointement la gestion des incidents de sécurité, l'investigation numérique, la gestion des risques et la gouvernance organisationnelle. C'est dans ce contexte que ce mémoire avait pour objectif de proposer une ontologie intégrée de cybersécurité permettant de relier, au sein d'une représentation commune des connaissances, les normes ISO/IEC 27035, ISO/IEC 27001, ISO/IEC 27005, le guide NIST SP 800-86 et le cadre COSO ERM.

La méthodologie adoptée repose sur la combinaison de l'approche de développement d'ontologies proposée par Noy *et al.* (2001) et de la méthodologie de mapping ontologique de Fenz *et al.* (2009). L'ontologie développée à partir d'ISO/IEC 27035 a été retenue comme référentiel d'ancrage en raison de son rôle central dans les processus de gestion des incidents de sécurité de l'information ainsi que de ses liens explicites avec le système de gestion de la sécurité de l'information défini par ISO/IEC 27001. Les connaissances relatives à la gestion des risques issues d'ISO/IEC 27005 ont été réutilisées à partir de l'ontologie proposée par Agrawal (2016), tandis que des ontologies ont été développées pour le guide NIST SP 800-86 et le cadre COSO ERM avant leur intégration au référentiel d'ancrage.

L'ontologie intégrée proposée a été implémentée sous Protégé en langage OWL puis validée au moyen d'une évaluation par questions de compétence et par raisonnement automatique, en s'appuyant sur un scénario d'attaque par déni de service de type TCP SYN Flood contre la plateforme USHOP dans un environnement simulé sous GNS3. Ce scénario a permis

d'instancier les différents concepts de l'ontologie et d'évaluer sa capacité à répondre à des questions de compétence mobilisant des connaissances issues de plusieurs domaines, notamment les incidents de sécurité, les investigations numériques, les risques organisationnels et les mécanismes de gouvernance. Les résultats obtenus montrent que l'ensemble de ces questions ont été satisfaites et que le raisonnement automatique, réalisé au moyen du raisonneur HermiT, confirme l'absence d'incohérence logique dans l'ontologie.

Cette recherche contribue à la réduction de la fragmentation des connaissances observée entre les référentiels de cybersécurité. Certaines limites demeurent néanmoins. La validation de l'ontologie a été réalisée dans un environnement expérimental simulé et le processus de mise en correspondance des concepts repose encore en partie sur une intervention manuelle. Des travaux futurs pourraient ainsi porter sur l'automatisation de ce processus, ainsi que sur l'expérimentation de l'ontologie dans des environnements opérationnels réels, notamment dans des contextes de gestion des incidents, d'investigation numérique, d'évaluation des risques et de gouvernance.

L'ontologie intégrée proposée constitue une contribution vers une représentation unifiée des connaissances en cybersécurité et fournit une base pouvant être exploitée pour le développement de systèmes d'aide à la décision en matière d'analyse des incidents, de gestion des risques et de gouvernance des cyberrisques.

BIBLIOGRAPHIE

Agrawal, V. (2016). Towards the Ontology of ISO/IEC 27005 : 2011 Risk Management Standard. Dans *HAISA*, pp. 101–111.

Agrawal, V. (2017). A framework for the information classification in ISO 27005 standard. Dans *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 264–269. IEEE.

Allahrakha, N. (2024). Impacts of cybercrimes on the digital economy. *Uzbek Journal of Law and Digital Policy*, *2*(3), 29–36.

Arbanas, K. & Čubrilo, M. (2015). Ontology in information security. *Journal of information and organizational sciences*, *39*(2), 107–136.

Ariyani, S. & Sudarma, M. (2016). Implementation of the ISO/IEC 27005 in risk security analysis of management information system. *J. Eng. Res. Appl*, *6*(8), 1–6.

Bernsmed, K., Undheim, A., Meland, P. H. & Jaatun, M. G. (2013). Towards an Ontology for Cloud Security Obligations. Dans *2013 International Conference on Availability, Reliability and Security*, pp. 577–581. IEEE.

Blackwell, C. (2010). A security ontology for incident analysis. Dans *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pp. 1–4.

Boinski, T., Orlowski, P., Szymanski, J. & Krawczyk, H. (2011). Security Ontology Construction and Integration. Dans *KEOD*, pp. 369–374.

Breitman, K. K., Casanova, M. A. & Truszkowski, W. (2007). *Semantic web : concepts, technologies and applications*. Springer.

Chockalingam, S. & Maathuis, C. (2022). An ontology for effective security incident management. Dans *International Conference on Cyber Warfare and Security*, Vol. 17, pp. 26–35. Academic Conferences International Limited.

COSO. (2017). *Enterprise Risk Management : Integrating with Strategy and Performance – Volume II : Appendices*. New York, NY, USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

dos Santos Moreira, E., Andréia Fondazzi Martimiano, L., José dos Santos Brandão, A. & César Bernardes, M. (2008). Ontologies for information security management and governance. *Information Management & Computer Security*, *16*(2), 150–165.

Efe, A. (2023). A comparison of key risk management frameworks : Coso-erm, nist rmf, iso 31.000, cobit. *Denetim ve Güvence Hizmetleri Dergisi*, *3*(2), 185–205.

Ekelhart, A., Fenz, S., Klemen, M. & Weippl, E. (2007). Security ontologies : Improving quantitative risk analysis. Dans *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pp. 156a–156a. IEEE.

Felahi, Y. & El Yousfi, H. (2025). L'impact économique des cyberattaques à l'ère de l'intelligence artificielle : une évaluation des coûts et des risques. *Revue Internationale du Marketing et Management Stratégique*, *7*(2), 363–385.

Fenz, S., Pruckner, T. & Manutscheri, A. (2009). Ontological mapping of information security best-practice guidelines. Dans *International Conference on Business Information Systems*, pp. 49–60. Springer.

Gao, J.-b., Zhang, B.-w., Chen, X.-h. & Luo, Z. (2013). Ontology-based model of network and computer attacks for security assessment. *Journal of Shanghai Jiaotong University (Science)*, *18*(5), 554–562.

Glimm, B., Horrocks, I., Motik, B., Stoilos, G. & Wang, Z. (2014). HermiT : an OWL 2 reasoner. *Journal of automated reasoning*, *53*(3), 245–269.

Hasan, A. M., Brankovic, L., Paul, D. & Sanin, C. (2025). A Systematic Literature Review on Cybersecurity Ontology. *Procedia Computer Science*, *270*, 3598–3607.

Hasbullah, M. A. (2022). Identifying the effects of cybercrime on business laws : implications for businesses and consumers. *International Journal of Cyber Criminology*, *16*(2), 119–130.

Herzog, A., Shahmehri, N. & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, *1*(4), 1–23.

Hung, S.-S. & Liu, D. S.-M. (2008). A user-oriented ontology-based approach for network intrusion detection. *Computer Standards & Interfaces*, *30*(1-2), 78–88.

ISO/IEC (2022). *ISO/IEC 27005 :2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva, Switzerland.

ISO/IEC (2023). *ISO/IEC 27035-1 :2023 Information technology — Information security incident management — Part 1 : Principles and process*. Geneva, Switzerland.

Janpitak, N. & Sathitwiriyawong, C. (2011). Data center physical security ontology for automated evaluation. Dans *Proceedings of the International Conference on Security and Management (SAM)*, p. 1. The Steering Committee of The World Congress in Computer Science, Computer . . ..

Kang, W. & Liang, Y. (2013). A security ontology with MDA for software development. Dans *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 67–74. IEEE.

Kent, K., Chevalier, S. & Grance, T. (2006). Guide to integrating forensic techniques into incident. *Guide to Integrating Forensic Techniques into Incident Response*, pp. 800–86.

Knublauch, H., Fergerson, R. W., Noy, N. F. & Musen, M. A. (2004). The Protégé OWL plugin : An open development environment for semantic web applications. Dans *International semantic web conference*, pp. 229–243. Springer.

Korniyenko, B., Galata, L. & Ladieva, L. (2019). Research of information protection system of corporate network based on GNS3. Dans *2019 IEEE international conference on advanced trends in information theory (ATIT)*, pp. 244–248. IEEE.

Luthfi, A. *et al.* (2024). Comparison study of nist sp 800-86 and iso/iec 27037 standards as a framework for digital forensic evidence analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718.

Martimiano, A. & Moreira, E. d. S. (2005). An owl-based security incident ontology. Dans *Proceedings of the Eighth International Protege Conference*, pp. 43–44.

Massacci, F., Mylopoulos, J., Paci, F., Tun, T. T. & Yu, Y. (2011). An extended ontology for security requirements. Dans *International Conference on Advanced Information Systems Engineering*, pp. 622–636. Springer.

Maunero, N., De Rosa, F. & Prinetto, P. (2023). Towards cybersecurity risk assessment automation : An ontological approach. Dans *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 0628–0635. IEEE.

Mdaki, J. (2025). A hybrid cybersecurity framework for small businesses : integrating NIST CSF, ISO 27001, and CEO engagement.

Merah, Y. & Kenaza, T. (2021). Ontology-based cyber risk monitoring using cyber threat intelligence. Dans *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1–8.

Milicevic, D. & Goeken, M. (2010). Ontology-based evaluation of ISO 27001. Dans *Conference on e-Business, e-Services and e-Society*, pp. 93–102. Springer.

Mndeep, K., Navreet, K. & Suman, K. (2016). A Literature Review On Cyber Forensic And Its Analysis Tools International Journal Of Advanced Research In Computer And Communication Engineering Vol. 5. *Issue*, *1*, 2278–1021.

Noy, N. F., McGuinness, D. L. *et al.* (2001). *Ontology development 101 : A guide to creating your first ontology*.

Obrst, L., Chase, P. & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. *STIDS*, *966*, 49.

Oladoyinbo, T. O., Adebiyi, O. O., Ugonnia, J. C., Olaniyi, O. O. & Okunleye, O. J. (2023). Evaluating and establishing baseline security requirements in cloud computing : an enterprise risk management approach. *Asian journal of economics, business and accounting*,

23(21), 222–231.

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I. & Oladoyinbo, T. O. (2024). CyberFusion protocols : Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 31–49.

Parkin, S. E., Van Moorsel, A. & Coles, R. (2009). An information security ontology incorporating human-behavioural implications. Dans *Proceedings of the 2nd International Conference on Security of Information and Networks*, pp. 46–55.

Poetiray, I. F. Z. & Salman, M. (2023). Information security incident management using iso 27035 standard. *Gema Wiralodra*, *14*(3), 168–178.

Ramanauskaitė, S., Olifer, D., Goranin, N. & Čenys, A. (2013). Security ontology for adaptive mapping of security standards.

Sánchez-Zas, C., Villagrá, V. A., Vega-Barbas, M., Larriva-Novo, X., Moreno, J. I. & Berrocal, J. (2023). Ontology-based approach to real-time risk management and cyber-situational awareness. *Future Generation Computer Systems*, *141*, 462–472.

Shawe, R. & Mengnjo, G. B. (2026). Governance Fragmentation and Cybersecurity Blind Spots in Critical Infrastructure Organizations. *International Journal of Advanced Engineering and Management Research*, *11*(2), 33–40. doi: 10.51505/ijaemr.2026.11204

Simmonds, A., Sandilands, P. & Van Ekert, L. (2004). An ontology for network security attacks. Dans *Asian applied computing conference*, pp. 317–323. Springer.

Soepeno, R. (2023). Wireshark : An effective tool for network analysis. *CYBV-Introd. Methods Netw. Anal*, pp. 1–15.

Tailhardat, L., Chabot, Y. & Troncy, R. (2024). NORIA-O : an ontology for anomaly detection and incident management in ICT systems. Dans *European Semantic Web Conference*, pp. 21–39. Springer.

Takahashi, T., Kadobayashi, Y. & Fujiwara, H. (2010). Ontological approach toward cybersecurity in cloud computing. Dans *Proceedings of the 3rd international conference on Security of information and networks*, pp. 100–109.

Tsoumas, B., Dritsas, S. & Gritzalis, D. (2005). An ontology-based approach to information systems security management. Dans *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, pp. 151–164. Springer.

Vorobiev, A., Han, J. & Bekmamedova, N. (2008). An ontology framework for managing security attacks and defences in component based software systems. Dans *19th Australian Conference on Software Engineering (ASWEC 2008)*, pp. 552–561. IEEE.

Wang, J. A. & Guo, M. (2009). OVM : an ontology for vulnerability management. Dans *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research : Cyber Security and Information Intelligence Challenges and Strategies*, pp. 1–4.

Xu, H., Xiao, D. & Wu, Z. (2009). Application of security ontology to context-aware alert analysis. Dans *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, pp. 171–176. IEEE.

Youseff, L., Butrico, M. & Da Silva, D. (2008). Toward a unified ontology of cloud computing. Dans *2008 Grid Computing Environments Workshop*, pp. 1–10. IEEE.