Installation, Organisation, Régulation et Gouvernance des risques industriels et cyber : une comparaison

Jean-Christophe Le Coze, François Masse, Paul Leroy, Albin Tarrisse

▶ **To cite this version:**

Jean-Christophe Le Coze, François Masse, Paul Leroy, Albin Tarrisse. Installation, Organisation, Régulation et Gouvernance des risques industriels et cyber : une comparaison. Congrès Lambda Mu 23 " Innovations et maîtrise des risques pour un avenir durable " - 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques, Oct 2022, Paris Saclay, France. hal-03875791

HAL Id: hal-03875791
https://hal.science/hal-03875791

Submitted on 28 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Installation, Organisation, Régulation et Gouvernance des risques industriels et cyber : une comparaison

LE COZE Jean-Christophe
INERIS
Parc Alata, 60 550 Verneuil-en-Halatte
jean-christophe.lecoze@ineris.fr

MASSE François
INERIS
Parc Alata, 60 550 Verneuil-en-Halatte
francois.masse@ineris.fr

Albin Tarrisse
INERIS
Parc Alata, 60 550 Verneuil-en-Halatte
albin.tarisse@ineris.fr

LEROY Paul
INERIS
Parc Alata, 60 550 Verneuil-en-Halatte
paul.leroy@ineris.fr

Résumé *— le but de cette communication est de proposée une première comparaison des domaines des risques industriels et de la cybersécurité. La méthode suivie est celle d'une mise à plat de ce qui est appelé dans cette communication, d'un côté, les installations et organisations à risques (IOR) et de l'autre leurs régimes de régulation et de gouvernance des risques (RRGR), tout en indiquant leur articulation. Cette mise à plat, graphique, permet à des experts en SHS (sciences humaines et sociales) et SPI (sciences pour l'ingénieur) des domaines des risques industriels et de la cybersécurité de produire une vision 'macro' permettant la mise en évidence des spécificités des deux domaines. Cette comparaison montre les similitudes et différences, de l'externalisation en passant par l'expertise, la normalisation et une notion comme celle de territoire.*

Mots-clefs — risques industriels, cybersécurité, analyse de risque, ICPE, OIV

Abstract*— The purpose of this communication is to propose a first comparison of the fields of industrial risks and cybersecurity. The method followed is that of a flattening of what is called in this communication, on the one hand, the facilities and organizations at risk (IOR) and on the other their risk regulation and governance regimes (RRGR), while indicating their articulation. This flattening, graphic, allows experts in SHS (human and social sciences) and SPI (sciences for the engineer) of the fields of industrial risks and cybersecurity to produce a 'macro' vision allowing the highlighting of specificities of the two fields. This comparison shows the similarities and differences, from outsourcing to expertise, standardization and a notion like that of territory.*

Keywords — industrial risks, cybersecurity, risk analysis, ICPE, OIV

I. INTRODUCTION (*HEADING 1*)

Avec l'accroissement de la digitalisation des industries, la thématique de la cybersécurité devient un enjeu fort pour la gestion des risques industriels majeurs (RIM). Le but de cette présentation est de s'y intéresser par le prisme des artefacts, acteurs, instruments, organisations et institutions impliqués dans les installations et organisations à risques (IOR) et leurs régimes de régulation et de gouvernance des risques (RRGR) associés à ces deux types de risques. La méthodologie suivie consiste à comparer les deux domaines en s'interrogeant sur leur différence, ainsi que le degré actuel d'articulation à partir des connaissances disponibles dans la littérature, les connaissances des auteurs et par les apports complémentaires d'entretiens. Les risques industriels dans le domaine des ICPE servent de point de départ pour la comparaison (ce dernier est plus familier et connu des auteurs du fait de son antériorité). Le but est de clarifier la complexité de ce sujet et de dégager des pistes de travail pour des approfondissements ciblés ultérieurs.

II. METHODOLOGIE

La méthodologie suivie repose sur une élaboration, dans un premier temps, d'un cadre structurant l'étude, basé sur la connaissance des IOR et RRGR dans les domaines des risques industriels et des ICPE. Cette étape est basée sur les connaissances empiriques et théoriques des auteurs en SHS (sciences humaines et sociales) portant sur la thématique des risques technologiques. Cette première étape est basée sur une approche graphique. Les auteurs participant à l'étude ayant des compétences différentes, à la fois disciplinaires SPI (sciences pour l'ingénieur) et SHS ainsi que thématique (connaissance ou non du domaine de la cybersécurité), l'usage d'une visualisation est apparu comme une option pertinente. Le schéma permet de mettre à plat la complexité sans entrer dans un niveau de détail, tout en permettant la coordination des auteurs autour de l'objectif de l'étude. Dans un second temps, les connaissances du domaine de la cybersécurité des auteurs de l'étude ont été mises à contribution afin de décrire les IOR et RRGR impliqués, complétées par des entretiens avec les membres d'une direction des systèmes d'information (DSI) au sein d'une organisation. Le troisième temps a consisté à comparer les deux domaines une fois décrits à ce niveau d'analyse, en cherchant les points d'articulation entre cybersécurité et sécurité industrielle.

III. LES RISQUES INDUSTRIELS ET LES ICPE

Grâce aux apports combinés des sciences pour l'ingénieur (SPI) et des sciences humaines et sociales (SHS), les risques technologiques dans le domaine des installations classées pour la protection de l'environnement (ICPE) sont éclairés sous de multiples angles qui permettent de progressivement dégager plusieurs des grandes facettes de la complexité de leur prévention [8]. Cette communication repose sur une articulation de plusieurs de ces sources d'éclairages pour mettre en lumière la grande complexité des multiples interactions entre artefacts, instruments, acteurs, organisations et institutions qui façonnent ce paysage. Le but de cette partie est de poser un 'décor' à partir duquel proposer des questionnements et perspectives de comparaison entre sécurité industrielle et risques cyber.

A. *"Interne" et "externe"*

Tout d'abord, une distinction est proposée entre les installations et organisations à risques (IOR) d'un côté, et les régimes de régulation et de gouvernance des risques de l'autre (RRGR). Cette première distinction introduit un découpage que l'on peut résumer de manière simplifiée par les regards « interne » et « externe » sur les risques. Il existe en effet dans la littérature des études qui sont traditionnellement portées sur l'analyse de risques des installations ainsi que les problématiques de travail et d'organisation en matière de sécurité. Elles sont ainsi plutôt tournées vers « l'interne » des entreprises (ici décrit avec l'acronyme IOR). D'autres études sont intéressées par l'interaction des entreprises et leur environnement, réglementaire et urbain, avec les riverains, les communes et les différents services de l'état. Cette approche est plutôt qualifiée « d'externe » car elle n'étudie pas les interactions entre les opérateurs, ingénieurs et managers au sein même des entreprises au quotidien. Elle se penche sur plutôt sur ce qu'il convient de décrire comme les régimes de régulation et de gouvernance des risques (acronyme RRGR).

Les angles d'analyses, l'accès aux données, les corpus théoriques associés à ces deux grands types de regards (IOR-RRGR) procèdent ainsi à des découpages qui sont maintenus parce qu'il est difficile de mobiliser des ressources pluridisciplinaires dans le temps long pour réunir, articuler ou combiner ces coupes « interne » et « externe ». Par ailleurs, le regard « interne » est lui-même découpé en spécialités comme les sciences pour l'ingénieur, la psychologie, l'ergonomie, la sociologie ou les sciences de gestion qui communiquent peu. Le regard « externe » sur la régulation et la gouvernance est aussi caractérisé par des approches différentes légales, sociologiques, politiques ou géographiques qui ne communiquent pas non plus vraiment. Cette pluri ou multidisciplinarité est bien connue et est utilisée pour enrichir les connaissances. Elle n'est pas un problème mais une source bienvenue de pluralisme d'approches [1] [2]. Ces découpages sont donc attendus et reflètent d'une part la science comme institution, et la complexité du réel d'autre part.

B. *Artefacts, instruments, acteurs, organisations et institutions*

Ensuite, si cette distinction heuristique, « *interne* » (IOR) et « *externe* » (RRGR), est structurante car elle renvoie à de multiples angles d'analyse complémentaires, il est aussi possible de mettre à plat, visuellement, cette dichotomie pour rendre compte des différentes facettes qu'elles abordent. C'est ce à quoi invite cette visualisation suivante, qui, en tirant partie d'études en provenance de champs différents [3] [4] [5] [6] et d'enquêtes empiriques [7] permet de fournir un point de vue sur les IOR-RRGR en identifiant des artefacts, instruments, acteurs, organisations ou institutions (figure 1). Même si sur le plan des connaissances il existe de très grandes zones d'ombres sur toutes ces interactions d'un point de vue empirique, ce passage par la visualisation, sans grande élaboration théorique, permet une vue d'ensemble témoignant de la complexité du sujet.

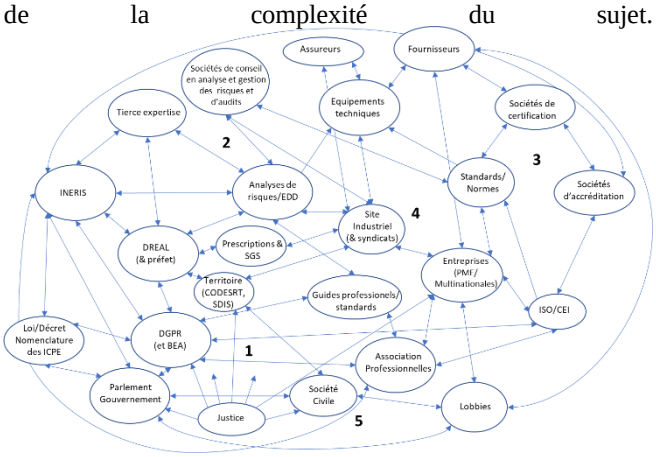

Figure 1. IOR-RRG des ICPE

Cette visualisation permet de mettre en évidence également les transformations à la fois des IOR et des RRGR dans les dernières décennies dans le contexte de la globalisation [9]. Par globalisation, il faut entendre au moins trois choses pour cette étude : l'accroissement des flux (information, personnes, capitaux, biens) entre les pays nécessitant de nouvelles formes de coordination et de coopération (1), la transformation des entreprises au sein de chaines globales de valeur combinant multinationales et PME sous-traitantes à l'échelle de la planète (2) et l'évolution de l'Etat et des territoires dans cette nouvelle donne globalisée (3) ([10] [11] [12]). Cette globalisation s'est ainsi accompagnée d'évolutions des principes de régulation et de gouvernance des risques moins portés sur la prescription en faveur de la standardisation et de la normalisation, mais aussi de l'essor du conseil dans de nombreux domaines d'expertise. Un paysage en réseaux se dessine, et une complexification des frontières « internes » et « externes » telles qu'introduites dans cette communication.

Commentons maintenant brièvement cette visualisation.

La gestion des risques accidentels repose dans le domaine des ICPE sur le principe de l'analyse de risque. L'analyse de risque est cadrée réglementairement par la production d'une étude de danger (EDD) pour un site industriel d'une entreprise qui présente des dangers par rapport à ces installations. Les risques de ces installations sont distingués dans les rubriques d'une nomenclature prévue pour fixer les exigences attendues et de processus administratifs associés, plus ou moins contraignant en fonction des installations industrielles. Ces analyses de risques sont bien souvent produites par des sociétés extérieures, des cabinets d'expertise et de conseil pour le compte des entreprises soumises à la réglementation, qui doivent produire ce document, l'étude de danger (EDD) pour instruction à l'administration. Ces dossiers sont en effet instruits par un inspecteur de la DREAL, pour le compte du préfet, implanté dans une région et au sein d'unités territoriales (UT), plus ou moins spécialisées dans ce domaine en fonction de l'organisation des DREAL locales.

Les inspecteurs ont la possibilité d'un recours à la tierce expertise, c'est un à dire à un regard critique par une société de conseil experte sur la production de l'EDD en cas de besoin. Sa prise en charge revient à l'entreprise. L'Ineris (l'institut national de l'environnement industriel et des risques), dans ce paysage, joue un rôle à l'interface entre la recherche, l'appui au pouvoir public et le service aux entreprises sur les questions de risques technologiques, et peut aussi jouer ce rôle de tiers expert. Cette expertise technique et scientifique produite par l'Ineris sert d'appui à l'administration pour la production de connaissances dans divers domaines (par exemple explosion, incendie, résistance des structures, facteurs humains) qui viennent épauler la formation des inspecteurs ainsi que la production de réglementations, dans un contexte national et européen (dont les directives dites « Seveso » depuis 1982). Cette activité réglementaire est portée au niveau de l'état à la direction générale de la prévention des risques (DGPR) au sein du ministère de la transition écologique, qui dispose désormais, depuis peu, d'un bureau d'enquête accident (BEA), suite à l'incendie de Lubrizol et de Normandie Logistique en 2019.

Le processus réglementaire de production d'une étude de danger (EDD) comporte également une dimension territoriale avec des instances qui jalonnent la validation de ce dossier dans lesquels siègent des représentants des collectivités ainsi que de la société civile (conseil départemental de l'environnement et des risques sanitaires et technologiques, CODERST). Il existe par ailleurs des démarches structurées de concertation pour le suivi des installations comme des commissions locales d'information et de surveillance (CLIS) notamment dans le cadre de la mise en œuvre des plans de prévention des risques technologiques (PPRT), apportés par la loi Bachelot de 2003. Ces différentes instances et conseils constituent des dimensions fortes de la gouvernance des risques technologiques par rapport à leur ancrage territorial et à la société civile, dont la thématique de l'acceptabilité et de la perception des risques est souvent associée. C'est aussi à ce niveau que les services d'incendie et de secours (SDIS), à l'intersection des communautés, de l'état et des entreprises, se préparent et interviennent pour les situations d'urgence. La société civile est également bien sûr représentée au niveau national par l'activité du parlement et du gouvernement qui décident d'évolutions réglementaires ainsi que des orientations et ressources budgétaires pour l'activité des administrations centrale (DGPR) et régionale déconcentrée (DREAL), ainsi que de l'Ineris et des territoires, dans leurs prérogatives décentralisées. Bien entendu, la justice (administrative, pénale et civile) joue un rôle important dans ce paysage, à la suite d'accident par exemple (mais pas seulement).

Les EDD servent aussi de trame pour la production d'arrêts préfectoraux que les inspecteurs des installations classées utilisent pour l'inspection de la conformité des entreprises à ces prescriptions réglementaires. Ils visitent ainsi les installations selon des rythmes définis en fonction des risques, mais également des priorités données chaque année par l'administration centrale (DGPR). Ces orientations dépendent de l'actualité et des problématiques remontées par le retour d'expérience. C'est aussi au niveau de l'administration centrale que les évolutions de la nomenclature se décide, dans des interactions entre les industriels, l'expertise de l'état (Ineris) et les syndicats professionnels. Une forme de lobbying est incontournable à ce niveau d'enjeux. Et c'est également dans ce type d'instances que sont produits des guides professionnels qui servent de repère pour l'élaboration des EDD en fonction des domaines industriels. Ces guides permettent de cadrer davantage l'exercice pour permettre des repères forts et une harmonisation des approches au sein d'une profession (par exemple la pétrochimie, la chimie ou les entrepôts). A noter également que les assureurs jouent un rôle par leur activité de prévention des risques incendies auprès des entreprises.

Ce principe d'harmonisation est également au cœur de l'importante activité de normalisation, de certification et d'accréditation dans le domaine des risques. Cette facette de la prévention dans l'industrie et la réglementation joue un rôle croissant depuis de nombreuses années. Les normes, établies par des consortiums regroupant états, industriels et experts au niveau français (AFNOR) européen (CE) et mondial (ISO ou IEC) sont à l'origine d'une importante source de cadrage des pratiques ainsi que d'atteinte de fiabilité et de sécurité des installations industrielles. La certification des fournisseurs de technologies (dont le rôle du COFRAC en tant qu'accréditeur des organismes certificateurs) utilisées pour la prévention des scénarios d'accidents identifiés par les EDD permet ainsi d'orienter et de conforter les entreprises dans leur choix (par exemple pour un équipement dans une zone inflammable qui ne doit pas produire d'électricité statique, pour la fiabilité d'un capteur dans son action de détection d'un gaz). Ces certifications peuvent par ailleurs être volontaires (fiabilité des équipements) ou réglementaire (ATEX par exemple). L'Ineris joue un rôle de certification sur plusieurs thématiques de la gestion des risques.

Dans le domaine des risques procédés, les standards de sûreté de fonctionnement ont ainsi fourni des principes qui ont été utilisés pour la définition des attendus et contenu des EDD, notamment par rapport aux calculs de probabilités, de niveaux de confiance dans les mesures de maitrise des risques à la suite des évolutions réglementaires des PPRT. La normalisation n'est donc pas toujours associée à la certification, et peut servir de référence internationale. Cette production normative non étatique fait ainsi l'objet d'une intense activité d'expertise, de conseil et d'audit depuis de nombreuses années. Elle se combine à la normativité légale, comme avec l'exemple des standards de management de la sécurité qui font l'objet d'audits privés pour la certification, qui sont proches des demandes réglementaires des systèmes de gestion de la sécurité (SGS), qui font eux l'objet d'inspection. Les entreprises multinationales, dans leurs activités de supervision et de centralisation de multiples entités ou filiales, regroupés au sein de siège (ou corporate), ont également recours à ce travail de standardisation pour leurs sites industriels, qu'elles appliquent également à leurs sous-traitants.

Cette visualisation combinée à cette description succincte, macroscopique et 'athéorique' de la prévention des risques technologiques indique un très grand nombre de 'boites noires' (artefacts, instruments, acteurs, organisations et institutions) et leurs myriades d'interactions. Cette mise en plat montre la complexité, si besoin était, de la prévention des risques technologiques. Un découpage de cette visualisation associée à cette visualisation est proposé en 5 grands 'blocs', repérés par des chiffres sur le schéma :

L'Etat (dont la justice) et les territoires (1),

L'expertise et le conseil (2),

La standardisation et la normalisation (3),

L'industrie (4),

La société civile (5).

La question qui est maintenant posée est de savoir ce qu'il en est de la problématique de la cybersécurité en la comparant à l'approche des risques industriels telle que présentée pour les ICPE (figure 1). Quels acteurs administratifs de l'état, des territoires et quels instruments réglementaires engagés sur cette thématique (1), quelle expertise et conseil disponibles en la matière, en matière d'analyse de risques cyber pour les procédés (2), quelle standardisation, normalisation et certification sur cette problématique (3), quelles applications en œuvre dans l'industrie et quelle production de guides par les syndicats professionnels (4) et enfin, quelle mobilisation de la société civile autour de ce sujet au niveau des territoires, du parlement et du gouvernement?

IV. LES RISQUES CYBER ET LES ICPE

Le sujet de la cybersécurité est une préoccupation relativement récente pour les ICPE. Il ne s'agit en effet pas de la maîtrise d'un risque intrinsèque au procédé lui-même et directement à la dangerosité des substances manipulées, mais d'un risque lié à l'évolution des technologies utilisées pour contrôler ces procédés. Par ailleurs, les risques cyber pour les ICPE comprennent des risques économiques, liés par exemple à des arrêts de production ou au vol de données confidentielles, et des risques physiques, humains ou matériels, dus à la manipulation ou à la perte de contrôle du procédé.

L'expertise en cybersécurité vient avant tout du domaine des systèmes d'information, qui ont été les premiers visés, dès les années 1980, puis plus massivement avec la démocratisation d'internet dans les années 1990. Si des systèmes industriels avaient déjà été visés par des attaques dans le passé, c'est l'attaque Stuxnet, en 2011, qui a été le premier événement d'ampleur et médiatisé. Cette prise de conscience a été concomitante avec le début du développement rapide de réglementations, de normalisations ainsi que d'offres de produits et de services spécifiques au domaine industriel.

L'acteur central pour la maîtrise de la cybersécurité en France est l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). Cette agence, créée en 2009, est rattachée au Secrétariat Général de Défense et de sécurité Nationale (SGDSN) placé sous l'autorité du premier ministre. Le parlement vote des orientations et des budgets qui sont ensuite alloués aux différentes initiatives dans ce domaine. Cet organisme a un rôle d'autorité nationale en matière de sécurité des systèmes d'information auprès du secteur public et des administrations et auprès des opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE).

L'ANSSI est également chargée de la rédaction des exigences réglementaires et des règles en matière de cybersécurité, rempli un rôle d'accompagnement auprès des OIV et plus largement de dissémination de la culture de cybersécurité auprès des entreprises et des citoyens. L'agence agit également pour le développement d'un écosystème souverain en matière de produits et services dédiés à la cybersécurité au travers de l'affectation des financements public et de son rôle de qualification de produits ou de services auprès des entreprises de ce secteur.

Différentes exigences réglementaires concernant la cybersécurité peuvent s'appliquer aux systèmes d'information. Pour le cas spécifique des installations industrielles, les exigences réglementaires concernant la cybersécurité s'appliquent aux OIV (Opérateurs d'Importance Vitale) qui exploitent des sites particuliers identifiés comme PIV (Points d'importance Vitale) pour lesquels ils doivent déclarer à l'ANSSI des SIIV (Systèmes d'information d'importance vitale) auxquels s'appliquent les règles de sécurité.

Les opérateurs d'importance vitale sont désignés par des ministres coordonnateurs s'ils exploitent des installations qui sont considérées comme essentielles à la vie de la nation et appartenant à l'un des 12 des Secteurs d'Activité d'Importance Vitale désignés par la réglementation. Certaines ICPE peuvent être identifiées comme PIV en raison de leurs activités ou des risques qu'elles font peser sur les populations. La liste des OIV est confidentielle mais on estime à environ 250 le nombre d'OIV, chacun pouvant exploiter un ou plusieurs PIV.

Par ailleurs, la directive européenne NIS défini des opérateurs des services essentiels (OSE) sur des principes similaires à ceux des OIV. Les listes des OIV et des OSE se recouvrent partiellement. L'ANSSI est également désigné comme autorité nationale pour l'application de cette directive.

Pour les OIV et les OSE, des exigences réglementaires de cybersécurité s'appliquent donc. Pour les entreprises qui ne rentrent pas dans ce champ réglementaire, y compris certaines ICPE, l'application de politique de sécurité des systèmes d'information tend à se développer, y compris pour les systèmes de conduite des installations industrielles. Cette mise en œuvre volontaire de politiques de cybersécurité repose sur des guides ou des référentiels normatifs qui peuvent être issus par exemple de l'ANSSI ou d'organismes de normalisation internationaux (comme l'IEC avec la série IEC 62443). Les exigences peuvent être également issues d'organismes étranger ou de politiques de groupes pour les entreprises multinationales.

Quels que soient les référentiels réglementaires ou volontaires applicables, la maîtrise de la cybersécurité repose sur des activités et des expertises à plusieurs niveaux. Cinq étapes sont décrites. La première étape est de définir une Politique de Sécurité des Systèmes d'Information comprenant l'identification des rôles et responsabilités et la formation et sensibilisation des personnels internes et externes. Les politiques et les formations peuvent suivre des référentiels de l'ANSSI par exemple.

On cherche ensuite, dans une deuxième étape, à développer la connaissance du système d'information en décrivant son contenu, ses fonctions et ses limites (cartographie) puis en réalisant une analyse de risque. Le développement de cette connaissance repose sur les informations issues des fournisseurs d'équipements et de logiciels et sur les sociétés ayant réalisé la conception et l'intégration du système si ces tâches sont externalisées. Des prestataires extérieurs peuvent apporter un appui sur la cartographie. L'analyse de risque fait également appel à des expertises spécifiques sur les vulnérabilités, vecteurs d'attaques, menaces….

La protection des systèmes d'information doit être cohérente avec l'analyse de risques, c'est la troisième étape. Elle vise à limiter la surface d'attaque en mettant en œuvre des règles de conception du réseau, de protection des communications et durcissement des équipements, de gestion

des accès et des identités, d'administration du réseau, etc. Ces mesures peuvent reposer sur des prestataires qualifiés en phase de conception, sur des produits de sécurité, potentiellement qualifiés par l'ANSSI. Le maintien du niveau de sécurité nécessite de réaliser une veille sur les vulnérabilités qui peut être faite soit auprès des fournisseurs, soit auprès des CSIRT (*Computer Security Incident Response Team*). L'ensemble de ces éléments doivent être audités annuellement par des prestataires qualifiés pour les OIV (PASSI : *Prestataires d'Audit de Sécurité des Systèmes d'Information*)

La détection et la réponse aux incidents de cybersécurité, quatrième étape, fait également appel à des systèmes techniques qui peuvent être qualifiés selon des référentiels de l'ANSSI (sondes de détection) et à des prestataires qualifiés pour l'analyse d'événements (PDIS : *Prestataires de Détection d'Incidents de Sécurité*) et la réponse aux incidents (PRIS : *Prestataires de Réponses aux incidents de Sécurité*). Enfin, la cinquième étape consiste à préparer des procédures de gestion de crise pour les cas d'attaques majeures. Pour les OIV l'activation de ses plans en cas d'attaque majeure peut être décidée par l'ANSSI.

Au-delà de l'application de ces règles, les OIV et les OSE sont tenus de déclarer leurs Systèmes d'information d'Importance Vitale à l'ANSSI, de tenir à disposition de l'ANSSI les informations sur ces systèmes et sur l'application des différentes règles et de déclarer à l'ANSSI les incidents de sécurité qui les affectent. L'application par un industriel d'une politique de cybersécurité repose donc sur l'implication de différents acteurs à même de lui apporter des expertises qui ne sont pas propre à son activité. La définition du cadre réglementaire et le contrôle de son application est porté par l'ANSSI. Ce cadre réglementaire s'applique aux OIV et aux OSE.

Pour l'ensemble des industriels, visés par la réglementation ou non, un élément clé de la construction de l'expertise vient des guides, des bonnes pratiques et des normes. Ceux-ci peuvent être portés par les pouvoirs publics (ANSSI en France, ENISA en Europe) et par les organismes de normalisation (IEC, afnor). L'existence de référentiels internationaux est primordiale pour les industriels, car ils permettent d'harmoniser certaines pratiques, et pour les fournisseurs de produits et de service car ils permettent de répondre aux besoins de différents marchés. La construction de cette expertise, récente pour les industriels, se fait également au travers de sociétés savantes ou groupes de travail (MITRE, Clusif, ISA, Exera…).

Le processus de mise en œuvre des exigences normatives ou réglementaires peut faire appel à des expertises spécifiques portées par des prestataires externes, éventuellement qualifiés. Ces expertises permettent de répondre à des exigences techniques spécifiques ou à des exigences plus générales d'analyse de risque et d'audit par exemple. La sécurité repose également sur les fournisseurs de produits, qu'il s'agisse de fournisseurs de solutions de sécurité (pare-feu, sondes de détection…) ou des fournisseurs des différents équipements constituant le système de conduite d'une installation (supervision , automates, réseaux de communication…) qui peuvent être des sources de vulnérabilité. Certains fournisseurs peuvent mettre en place des mesures de sécurité au niveau de leur produit qui peuvent être qualifiés par l'ANSSI.

Ainsi, cette description de la cybersécurité selon les différentes facettes 'internes' et 'externes' à savoir l'Etat (dont la justice) et les territoires (1), l'expertise et le conseil (2), la standardisation et la normalisation (3), l'industrie (4) et la société société civile (5) peut être représentée comme pour les risques industriels (figure 2).

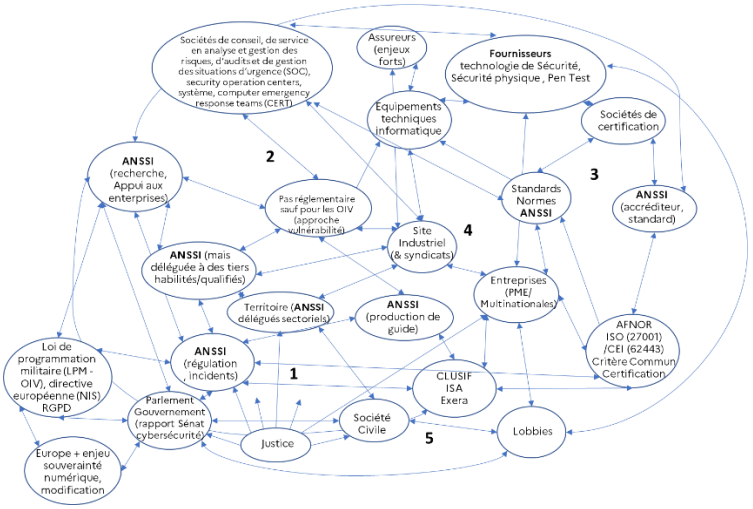

Figure 2. IOR-RRG de la cybersécurité

V. DISCUSSION

Dans cette discussion nous souhaitons aborder quelques points de comparaisons qui nous permettent de poser quelques jalons pour des étapes d'analyses ultérieures. Tout d'abord, il est évident que les deux domaines ont des historiques très distincts. L'un est très récent, l'autre beaucoup plus ancien. Depuis de nombreuses décennies, les risques industriels font l'objet d'une intense régulation, et des moyens importants y sont consacrés. Ils ont accompagné l'essor de l'industrie depuis la révolution industrielle, et les évolutions de sociétés sur le thème des risques, les catastrophes technologiques ayant joué un rôle dans ces étapes, des amonitrates en passant par la pyrotechnie ou le raffinage du pétrole. Pour la cybersécurité, cette trajectoire se construit aussi avec l'émergence de nouvelles menaces et l'occurrence d'attaques dont les implications industrielles sont avérées.

De deux domaines plutôt séparés au départ, ces deux univers de risques se rapprochent avec l'évolution des systèmes productifs, vers une digitalisation accrue. Pour le moment, ces rapprochements, à la fois méthodologiques, normatifs mais également réglementaires sont embryonnaires mais bien présents, notamment dans la recherche par exemple, avec des travaux sur la combinaison dans les analyses de risques, des deux domaines. De ce point de vue, des similitudes existent dans les démarches (identification des risques, estimation de leur gravité et probabilité – ou « *vraisemblance* » en cybersécurité, moyens de prévention ou gestion de risques) même si, dans la mise en œuvre, les différences entre les problématiques posent des questions de compatibilité [14].

Ensuite, on constate dans les deux domaines, une configuration à la fois similaire et différente de la production et disponibilité de l'expertise. Pour les risques industriels, l'Ineris et les cabinets de conseil ont un rôle important. Les sociétés conseil constituent une facette de l'externalisation de la mise en œuvre de la réglementation dans leur apport aux études de danger notamment. L'Ineris apporte une compétence technique et scientifique sur le sujet au niveau des

entreprises et de l'état. Un schéma similaire existe dans la cybersécurité (de la certification en passant par l'expertise, recherche, la formation, réglementation et contrôle) mais le rôle de l'ANSSI apparait plus étendu dans son activité d'organisation de l'écosystème externalisé de l'expertise apportées par les sociétés de conseil. En particulier, son rôle dans la certification est plus fort par la définition des référentiels à une autre échelle que celle de l'Ineris, aussi dans la qualification des attendus en matière d'externalisation (société de services et de conseil notamment). L'externalisation est effet plus importante dans le domaine de la cybersécurité (PRIS, PDIS, PASSI) par le fait même d'une transformation digitale qui favorise son expansion. Les entreprises sont aujourd'hui dans des situations de dépendance à des expertises qui se développent en dehors de leur cœur de métier (serveurs, cloud, logiciels, sûreté, réseaux).

Ce point sur l'étendue des prérogatives de l'ANSSI s'applique également dans le domaine réglementaire car cette agence produit directement des réglementations pour le ministère de la Défense (loi de programmation militaire, soumises au vote du parlement) alors que l'Ineris est en interaction avec le ministère (DGPR). Ces différences tiennent aux statuts différents d'agence (service à compétence nationale) et d'institut (Ineris, Epic). Nous indiquons seulement quelques différences sans entrer dans un très haut niveau de détail, en guise d'illustration. Il nous semble intéressant de souligner dans les deux cas l'importance de la normalisation, de la certification et de l'externalisation de la gestion des risques industriels et cyber, avec une facette plus prégnante dans la cybersécurité.

Nous voudrions conclure en ouvrant sur une dimension particulièrement intéressante qui témoigne de la spécificité des deux domaines, la notion de territoire. Dans les risques industriels, la question du territoire est celle de l'ancrage physique des installations dans leur environnement urbain. Dans la cybersécurité, la notion de territoire correspond à une toute autre définition et réalité, qui nous renvoie à la particularité de ce domaine. L'infrastructure informationnelle du monde digital et son lien avec la cybersécurité implique en effet un territoire qui n'est plus régional ou national, mais directement mondial et global. Les frontières du monde digital ne se superposent pas aux frontière étatiques ou supra étatiques (Europe). Le risque cyber est fondamentalement ancré dans cette spécificité 'territoriale' du digital, et permet de contraster fondamentalement la nature des menaces.

REFERENCES

[1] Dupré, Le Coze, 2014
[2] Le Coze, 2019
[3] Gilbert, 2003,
[4] Beccara, Lalanne,
[5] Borraz, 2008
[6] Dupré, Le Coze, 2014
[7] Weisben, 2016
[8] Dupré, Le Coze, 2021
[9] Le Coze, 2016
[10] Le Coze, 2020
[11] Veltz, 2008,
[12] Veltz, 2012,
[13] Veltz, 2017
[14] Abdo et al, 2017