ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 18 Novembre 2024

Le guide de survie du RSSI Intergalactique

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

Introduction

La session des Lundis de la Cybersécurité du 18 novembre 2024, organisée en partenariat avec l'Université Paris Cité et l'ARCSI, a offert une perspective unique et pragmatique sur les défis contemporains du RSSI (Responsable de la Sécurité des Systèmes d'Information). Cédric Cartau, fort de son expérience au sein du CHU de Nantes, a captivé l'audience avec une présentation mêlant humour et analyse stratégique, intitulée « Le guide de survie du RSSI intergalactique dans un monde de dingues ».

En complément, Laure Duhesme de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a apporté un éclairage institutionnel, en insistant sur les initiatives nationales pour renforcer la cyberrésilience, particulièrement dans le secteur de la santé et des infrastructures critiques.

I. Le rôle et les pressions du RSSI

Cédric Cartau a ouvert sa présentation en retraçant l'évolution du métier de Responsable de la Sécurité des Systèmes d'Information (RSSI). Historiquement considéré comme un rôle purement technique, souvent limité à la gestion des infrastructures et des systèmes, le poste a progressivement gagné en importance à mesure que les enjeux de cybersécurité devenaient critiques pour les organisations. Toutefois, cette montée en visibilité n'est pas sans conséquences, car elle place les RSSI dans une position à la fois stratégique et vulnérable. En effet, ils se trouvent à la croisée de multiples attentes et pressions émanant de divers interlocuteurs au sein de l'entreprise.

L'intervenant a insisté sur un paradoxe majeur : alors que les RSSI sont devenus essentiels pour protéger les organisations contre des menaces toujours plus sophistiquées, leur rôle reste souvent marginalisé dans les décisions stratégiques. Cette situation découle, selon Mr Cartau, de la nature même de leurs responsabilités. Contrairement à d'autres fonctions qui célèbrent leurs succès, les RSSI interviennent principalement en prévention ou en gestion de crise. Leur travail est souvent invisible tant qu'il est efficace, mais ils sont immédiatement exposés lorsque des problèmes surviennent. Cela contribue à une perception biaisée de leur valeur ajoutée, les cantonnant à un rôle de « porteur de mauvaises nouvelles ».

Cette pression est exacerbée par ce que Mr Cartau a décrit avec humour comme le « Big Boss Syndrome ». Il a illustré ce concept en expliquant que les RSSI doivent répondre à plusieurs figures d'autorité dans l'entreprise – le DRH, le DAF, et le DSI – qui agissent chacun comme des "Big Boss", imposant leurs propres contraintes tout en limitant les ressources disponibles. Par exemple, lorsque le RSSI demande des ressources humaines pour renforcer l'équipe, le DRH peut opposer des restrictions budgétaires ou organisationnelles. De la même manière, une demande de financement pour des outils ou des infrastructures de sécurité peut être refusée par le DAF, tandis que le DSI, souvent accaparé par d'autres priorités, peut ne pas être en mesure d'apporter le soutien technique nécessaire. Cette multiplicité de contraintes place le RSSI dans une position où il doit constamment « faire avec ce qu'il a », tout en restant garant de la sécurité globale de l'organisation.

L'intervenant a également mis en lumière les conséquences psychologiques et professionnelles de cette situation. La nature stressante et souvent solitaire du rôle pousse de nombreux RSSI à l'épuisement professionnel. Cette fatigue est particulièrement visible dans les moments de crise, lorsque les responsabilités du RSSI atteignent leur paroxysme, mais que les moyens pour gérer ces crises sont souvent insuffisants. Mr Cartau a partagé des anecdotes marquantes, notamment celle d'un déploiement de logiciel critique qu'il avait dû retarder d'un an en raison de failles de sécurité majeures identifiées à la dernière minute. Bien que cette décision ait permis d'éviter un désastre potentiel, elle lui a valu des critiques sévères, illustrant une autre dimension des pressions auxquelles les RSSI sont confrontés : leur rôle de « frein nécessaire » aux projets d'innovation ou de transformation.

En résumé, le métier de RSSI oscille entre la reconnaissance de son importance et la réalité d'une fonction exposée, isolée et souvent sous-équipée. Cette dualité alimente une tension permanente, que Mr Cartau a brillamment illustrée avec un mélange d'humour et de réalisme, capturant ainsi les défis d'un rôle clé dans un monde où la sécurité des systèmes d'information est devenue une priorité absolue.

II. Trois stratégies pour éviter l’épuisement

Monsieur Cartau a consacré une partie de son intervention à décrire les mécanismes que les RSSI peuvent adopter pour préserver leur santé mentale et leur efficacité professionnelle face aux défis constants de leur métier. Ces stratégies, bien que parfois teintées d’ironie, reflètent une profonde compréhension des enjeux auxquels sont confrontés les RSSI au quotidien. En les présentant, il a cherché à transmettre des pistes concrètes pour mieux gérer les multiples pressions du rôle, tout en rappelant les limites intrinsèques de chaque approche.

La première stratégie qu’il a développée est celle dite technique, souvent la plus instinctive pour un RSSI. Elle consiste à s’appuyer sur des outils et des méthodologies éprouvés pour sécuriser les systèmes d’information. Cette approche implique une analyse fine des risques à travers des méthodologies comme EBIOS ou ISO 27005, suivie de la mise en place de solutions techniques telles que des systèmes d’authentification multifactorielle (MFA), des Endpoint Detection and Response (EDR), ou encore des Security Operations Centers (SOC). Cependant, Monsieur Cartau a souligné que cette approche, bien qu’efficace sur le plan opérationnel, montre rapidement ses limites si elle n’est pas accompagnée d’un soutien institutionnel suffisant. En l’absence de moyens financiers ou humains adéquats, le RSSI risque de se retrouver dans une situation d’échec apparent, même après avoir déployé les meilleures solutions techniques disponibles. Il a aussi rappelé que cette stratégie, trop exclusivement centrée sur la technique, peut isoler le RSSI des dimensions humaines et organisationnelles, pourtant essentielles à une gestion efficace des risques.

La deuxième stratégie, qu’il a qualifiée de conseil, repose sur une posture plus détachée et consultative. Ici, le RSSI se limite à un rôle de prescripteur et de conseiller, laissant les autres départements ou la direction prendre les décisions finales. Cette approche permet au RSSI de se protéger des conséquences directes des choix organisationnels tout en se concentrant sur la sensibilisation et la communication des risques. En se dédouanant de la responsabilité opérationnelle, il peut ainsi éviter de porter seul le poids des échecs ou des incidents. Monsieur Cartau a cependant mis en garde contre les écueils de cette stratégie. Si elle offre une forme de résilience personnelle, elle peut également nuire à l’efficacité globale, car une posture purement consultative réduit l’impact du RSSI sur les décisions clés. Par ailleurs, elle peut être mal perçue au sein de l’organisation, donnant l’impression que le RSSI se décharge de ses responsabilités, ce qui pourrait affecter sa crédibilité et ses relations professionnelles.

Enfin, la troisième stratégie, plus provocatrice, est celle qu’il a appelée la stratégie "Detritus", en référence au personnage d’Astérix connu pour semer le chaos. Cette approche consiste à soumettre l’organisation à des stress-tests intentionnels, parfois à la limite du subversif, afin de révéler les failles systémiques ou les incohérences organisationnelles. Monsieur Cartau a donné plusieurs exemples concrets : envoyer des tests de phishing internes pour évaluer la vigilance des employés, ou encore installer des outils de simulation de failles pour mesurer la capacité de l’équipe à réagir face à une intrusion. L’objectif de cette stratégie est double : éprouver la résilience de l’organisation et sensibiliser, parfois brutalement, les acteurs internes à la réalité des menaces. Bien que cette approche puisse s’avérer extrêmement efficace pour démontrer les lacunes d’un système, elle n’est pas sans risques. Monsieur Cartau a rappelé qu’elle peut engendrer des tensions importantes, voire des conflits, avec d’autres départements ou avec la direction. Par conséquent, il a conseillé de l’utiliser avec parcimonie et, si possible, dans un cadre contrôlé et transparent.

Ces trois stratégies, bien que distinctes, ne sont pas mutuellement exclusives. Monsieur Cartau a insisté sur l'importance de les adapter au contexte spécifique de chaque organisation, tout en cherchant à maintenir un équilibre entre implication professionnelle et santé mentale. Il a conclu en soulignant que, quelle que soit la stratégie adoptée, la clé réside dans la capacité du RSSI à faire preuve de recul et à garder à l'esprit que sa mission, bien qu'essentielle, ne peut être menée à bien sans le soutien actif de l'ensemble de l'organisation. Cette réflexion s'inscrit dans une démarche de long terme, où la résilience personnelle du RSSI est aussi importante que celle des systèmes qu'il protège.

III. Les axes de réflexion pour une résilience accrue

Monsieur Cartau a abordé les pistes de réflexion essentielles pour renforcer la résilience des organisations face à des menaces numériques de plus en plus complexes et fréquentes. Il a identifié quatre axes majeurs qui, selon lui, permettent non seulement de mieux gérer les crises, mais aussi de transformer les organisations pour les rendre plus robustes et efficaces sur le long terme.

Le premier axe concerne les frontières organisationnelles. Monsieur Cartau a souligné que les organisations modernes, bien qu'elles investissent massivement dans des dispositifs de cybersécurité en interne, sont encore largement vulnérables en raison de leur interdépendance avec des tiers. Les attaques dites de « supply chain » sont devenues une menace dominante, exploitant les failles chez des prestataires ou partenaires pour accéder aux systèmes critiques d'une organisation cible. Cette situation reflète la difficulté qu'ont les entreprises à sécuriser non seulement leurs propres accès, mais aussi ceux de leur écosystème. Monsieur Cartau a insisté sur l'importance de mettre en place des approches telles que le modèle « Zero Trust », où les accès externes sont par défaut fermés et ne sont ouverts que sur demande et avec une supervision stricte. Bien qu'exigeantes sur le plan opérationnel, ces pratiques peuvent réduire considérablement les risques liés aux intrusions par des tiers.

Le deuxième axe porte sur la gestion de l'entropie des systèmes d'information. Monsieur Cartau a décrit cette entropie comme une accumulation de complexité dans les infrastructures informatiques, souvent liée à des strates successives de technologies et de processus, sans vision globale ni cartographie actualisée. Ce désordre rend difficile, voire impossible, une gestion efficace des risques, car personne ne dispose d'une vue complète des flux d'interopérabilité ou des interdépendances critiques. Pour contrer cette dérive, il a recommandé de s'inspirer des approches Lean Management et des méthodologies issues du secteur industriel, comme celles développées par Toyota. Ces outils permettent de rationaliser les processus et de réorganiser les systèmes pour réduire les zones de vulnérabilité. Cependant, il a averti que cette démarche nécessite un engagement organisationnel fort, car elle implique souvent une remise en question de pratiques établies depuis des années.

Le troisième axe, selon Monsieur Cartau, est lié aux moyens alloués à la cybersécurité. Contrairement à une idée répandue, il ne s'agit pas seulement d'investir davantage, mais de mieux utiliser les ressources disponibles. Il a donné l'exemple du système éducatif français, dont les budgets, bien qu'élevés, ne se traduisent pas nécessairement par de meilleurs résultats en raison de problèmes structurels et organisationnels. En cybersécurité, la logique est similaire : il est crucial d'optimiser les moyens existants avant de réclamer de nouveaux financements. Cela passe notamment par une meilleure priorisation des initiatives, un suivi rigoureux des investissements et une clarification des responsabilités.

Enfin, le quatrième axe touche à la perception du temps au sein des organisations. Monsieur Cartau a expliqué que de nombreuses structures souffrent d'un « écrasement du temps », se concentrant uniquement sur les urgences immédiates, au détriment de la réflexion stratégique et prospective. Ce phénomène empêche les organisations d'anticiper les crises et de se préparer aux ruptures de paradigme, comme celles provoquées par l'intelligence artificielle ou les nouvelles réglementations. Pour y remédier, il a suggéré de consacrer des espaces dédiés à la réflexion et à la planification à long terme, permettant ainsi de rééquilibrer les priorités entre court et long terme.

En conclusion, Monsieur Cartau a insisté sur la nécessité pour les organisations de dépasser une vision purement technique de la cybersécurité pour embrasser une approche systémique et intégrée. Les quatre axes qu'il a décrits – frontières, entropie, moyens et temps – offrent un cadre de travail clair pour renforcer la résilience organisationnelle. Cependant, il a rappelé que cette démarche exige un changement culturel et un engagement de la part de tous les niveaux de l'organisation, de la direction générale aux équipes opérationnelles.

IV. Intervention de Laure Duhesme de l’ANSSI

Laure Duhesme, représentante de l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information), a présenté le rôle, les missions et les initiatives clés de l'agence, tout en soulignant l'importance de la cyberrésilience dans des secteurs critiques tels que la santé, les infrastructures stratégiques et les services publics.

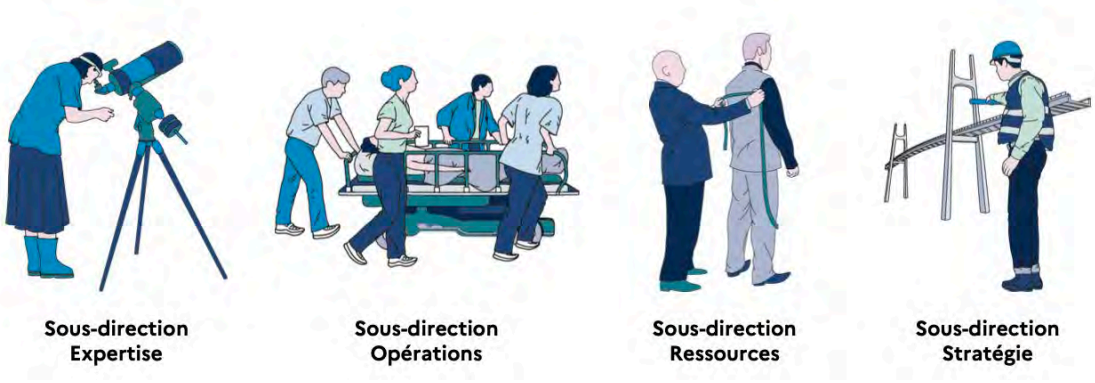
Elle a débuté en expliquant que l’ANSSI, créée en 2009, est une autorité nationale exclusivement défensive en matière de cybersécurité et de cyberdéfense. Rattachée au Premier ministre via le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), l'agence se concentre principalement sur la protection des systèmes d’information des Opérateurs d’Importance Vitale (OIV), des Opérateurs de Services Essentiels (OSE) définis par la directive européenne NIS, et des administrations publiques. Cependant, dans des situations de grande ampleur impactant la sécurité nationale ou les citoyens, l’ANSSI peut intervenir au-delà de son périmètre habituel pour soutenir les entités affectées.

Les missions de l’ANSSI s’articulent autour de quatre piliers principaux : défendre, connaître, partager, et accompagner. La défense consiste à protéger les systèmes d’information critiques et à intervenir en cas de cyberattaques majeures. La mission de connaissance repose sur une veille continue des menaces, la publication d’états de la menace, et la mise à disposition d’analyses techniques détaillées. Le partage s’incarne par la production de guides pratiques et pédagogiques adaptés à différents publics, allant des experts techniques aux dirigeants d’entreprises ou responsables de petites structures. Enfin, l’accompagnement se traduit par un soutien actif à l’écosystème national et international à travers des audits, des formations et des projets spécifiques.

Laure Duhesme a illustré l’impact de l’ANSSI à travers des chiffres-clés de l’année 2023. L’agence comptait 634 agents répartis sur quatre sites : l’Hôtel National des Invalides, la Tour Mercure, le Campus Cyber à Paris, et le récent site ArteFact à Rennes. Ce dernier renforce la présence opérationnelle en Bretagne et facilite la collaboration avec l’écosystème local. En 2023, l’ANSSI a traité 3 703 événements de sécurité, dont 1 112 incidents confirmés impliquant des acteurs malveillants. L’agence a également délivré 269 visas de sécurité, 57 823 attestations via son MOOC « SecNumacadémie », et labellisé 105 formations en cybersécurité.

L’organisation interne de l’ANSSI repose sur quatre sous-directions : expertise, opérations, ressources, et stratégie. Laure Duhesme a mis en avant le rôle de la sous-direction stratégie, dont elle dépend, et plus particulièrement de son bureau Santé et Affaires Sociales. Ce bureau est responsable de la coordination sectorielle dans le domaine de la santé, de la protection sociale, et des projets transverses liés au ministère du Travail, de la Santé et des Solidarités.

Parmi les actions phares, elle a cité le programme CARE, destiné à renforcer la cyberrésilience des hôpitaux à travers des audits, des ateliers, et des outils d'évaluation des risques tels que ceux appliqués aux Active Directory.



Elle a également abordé les défis spécifiques liés à la transposition de la directive NIS2 et à la mise en œuvre de la loi résilience cyber. Ces initiatives visent à élever les exigences réglementaires pour les secteurs critiques, en mettant l'accent sur une gouvernance renforcée, une meilleure gestion des crises, et une mise en conformité adaptée aux enjeux actuels.

En conclusion, Laure Duhesme a insisté sur l'importance de collaborer avec les différents acteurs, qu'il s'agisse d'établissements de santé, d'entreprises, ou d'institutions publiques, pour construire une véritable culture de la cybersécurité en France. Elle a encouragé les participants à explorer les ressources disponibles sur le site de l'ANSSI, à suivre les formations gratuites comme SecNumacadémie, et à consulter les rapports annuels tels que le panorama de la cybermenace, pour se tenir informés des évolutions du paysage cyber. Enfin, elle a rappelé que l'ANSSI recrute activement des talents, aussi bien techniques que stratégiques, pour relever les défis croissants de la cybersécurité.

V. Questions/Réponses avec Cédric Cartau et Laure Duhesme

Question 1 : Comment sont organisés les CHU en France ? Existe-t-il un RSSI par CHU ou un réseau de RSSI ? Les systèmes d'information (SI) sont-ils propres à chaque CHU ? Et existe-t-il une direction des risques dans le domaine de la santé, comme cela existe dans d'autres secteurs ?

Il y a plusieurs volets à votre question. En France, il y a 31 CHU, et en principe 31 RSSI, un pour chaque CHU. Depuis la loi de santé de 2016, les CHU se sont regroupés en Groupements Hospitaliers de Territoire (GHT). Cela implique un regroupement administratif à l'échelle départementale, sous l'égide d'un établissement support, généralement le CHU du département, car c'est le plus grand établissement. Par exemple, je suis le RSSI du CHU de Nantes, mais aussi du GHT du département 44, qui regroupe tous les hôpitaux publics du département. Cela signifie que je suis, par défaut, le RSSI de tous ces établissements. Évidemment, je ne peux pas tout gérer seul, donc je délègue certaines responsabilités à des relais dans les autres établissements.

Cependant, la réalité hospitalière est très hétérogène : un petit hôpital local peut avoir un informaticien à mi-temps, tandis qu'un CHU comme Nantes dispose d'une équipe de 120 informaticiens. Cela nous pousse à mutualiser et à regrouper les moyens au niveau départemental. Il existe aussi un réseau national de RSSI hospitaliers qui échangent régulièrement, notamment via des messageries sécurisées. Cela permet de partager rapidement des informations, par exemple sur des attaques ou des vulnérabilités.

En ce qui concerne les rattachements organisationnels, il y a une grande variété. Dans certains cas, le RSSI est rattaché à la Direction de la Qualité et des Risques (comme à Bordeaux), mais la plupart du temps, il est rattaché à la DSI, ce qui est une anomalie. Avec l'évolution réglementaire, notamment la directive NIS2, on observe une tendance à rattacher les RSSI directement à la Direction Générale, ou parfois à des directions des risques physiques, car il existe des points communs entre les risques numériques et physiques.

Question 2 : On observe une multiplication des réglementations en matière de cybersécurité. Est-ce vraiment une solution efficace pour renforcer la cyberrésilience des hôpitaux ?

Ma première réaction face à NIS2 était de penser que cela n'apportait rien de nouveau. Les exigences de NIS2 sont similaires à celles de NIS1, et elles s'appuient principalement sur des normes ISO 27001. Cependant, j'ai changé de perspective avec le temps. Si une réglementation impose, par exemple, la maîtrise de la cartographie réseau ou des comptes à privilèges, c'est souvent parce que cela n'a pas été fait auparavant. Si nous étions plus proactifs, ces obligations n'auraient pas besoin d'être inscrites dans la loi. Paradoxalement, ces réglementations deviennent alors une opportunité pour imposer des exigences à des acteurs qui ne prenaient pas ces sujets au sérieux.

Bien que la multiplication des réglementations puisse paraître lourde, elle sert à pallier les lacunes en matière de sécurité. NIS2, par exemple, permet d'appuyer des demandes auprès de partenaires ou fournisseurs avec une base légale solide, ce qui renforce la crédibilité et la légitimité des RSSI.

Question 3 : Pourquoi n'y a-t-il pas d'homogénéisation des applications entre hôpitaux, comme cela a pu être fait dans l'industrie automobile, par exemple chez PSA, il y a des années ?

La réponse est assez simple : chez PSA, il y a un patron unique. En France, nous avons 3 000 hôpitaux avec 3 000 directeurs généraux, chacun ayant son autonomie de gestion. Cela rend une homogénéisation nationale très difficile. Par ailleurs, les besoins diffèrent fortement entre établissements. Un CHU avec des blocs opératoires et des urgences vitales n'a pas les mêmes contraintes qu'un petit hôpital local ou un établissement médico-social. Cette diversité des missions et des tailles complique toute standardisation des systèmes d'information.

De plus, contrairement à l'industrie, un hôpital ne peut pas simplement arrêter son activité ou rediriger ses "clients". Si un CHU ne peut plus fonctionner en raison d'une panne informatique, les patients doivent être pris en charge ailleurs. Cela implique une responsabilité collective qui dépasse le cadre de l'établissement, rendant la standardisation encore plus complexe.

Question 4 : Dans l'aéronautique, des travaux explorent les liens entre les risques cyber et les risques de sûreté. Ces travaux peuvent-ils inspirer le secteur de la santé ?

Les différences entre les établissements de santé sont si grandes qu'elles compliquent toute transposition directe de modèles issus d'autres secteurs comme l'aéronautique. Par exemple, un hôpital psychiatrique et un CHU avec des blocs opératoires ont des besoins en cybersécurité complètement différents. Cependant, certains concepts de gestion des risques peuvent être adaptés. La prise en compte de l'impact des pannes informatiques dans le secteur de la santé, par exemple, va bien au-delà de l'hôpital lui-même, affectant l'ensemble de la chaîne de soins et les pouvoirs publics.

Cela étant dit, il y a des similitudes à explorer. Dans l'aéronautique, une panne peut avoir des conséquences graves en cascade, tout comme dans un hôpital. Par exemple, une panne du système de gestion des repas peut rapidement devenir critique pour un hôpital avec des milliers de patients à nourrir chaque jour. Ce type d'incident montre l'importance d'intégrer des approches transversales dans l'analyse des risques, même si les contextes restent très différents.

Conclusions

La session du Lundi de la Cybersécurité du 18 novembre 2024 a offert une vision riche des défis actuels en cybersécurité, avec les interventions marquantes de Monsieur Cartau et de Madame Laure Duhesme de l'ANSSI. Monsieur Cartau a exposé, avec humour et réalisme, les pressions et paradoxes du rôle de RSSI, tout en proposant des stratégies pragmatiques pour éviter l'épuisement. Madame Duhesme a présenté les efforts de l'ANSSI pour renforcer la résilience nationale, notamment dans le secteur de la santé.

L'échange final a permis d'approfondir des sujets clés, comme l'organisation des CHU et la pertinence des réglementations. Cette conférence a souligné l'importance d'une collaboration accrue et d'une approche intégrée pour relever les défis numériques, tout en offrant des pistes concrètes pour renforcer la résilience des organisations.