Université de Montréal

CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 6, Num. 1
2025

L'épuisement professionnel en cybersécurité

Tom Verstichel, étudiant à la maîtrise en criminologie

Introduction

À mesure que les menaces numériques se complexifient et se multiplient, les professionnels de la cybersécurité occupent une place stratégique au sein des organisations. Chargés de défendre des systèmes critiques, de réagir aux incidents et de préserver la continuité des opérations, **ces acteurs sont constamment confrontés à une pression opérationnelle soutenue face à l'intensité, à la sévérité et à la persistance des cybermenaces**. Ce contexte les expose à des risques psychosociaux élevés, encore peu étudiés malgré leur caractère structurel. En parallèle des efforts techniques pour contrer les cybermenaces, **un nouveau défi émerge : celui de préserver la santé mentale et les capacités cognitives d'un personnel en première ligne, dans un contexte de pénurie structurelle de talents**.

Depuis quelques années, le phénomène d'épuisement professionnel dans le secteur de la cybersécurité attire l'attention d'une communauté croissante de chercheurs et de praticiens [1]. Des termes comme **« cyber fatigue »** ou **« surcharge cognitive »** s'imposent dans les débats professionnels et scientifiques. L'épuisement professionnel (ou *burnout*), défini comme un état d'épuisement émotionnel, de dépersonnalisation et de réduction de l'efficacité professionnelle [2], touche désormais les métiers de la cybersécurité, dans lesquels les contraintes techniques s'ajoutent à une instabilité chronique des environnements de travail.

Les études récentes montrent que **les analystes en cybersécurité, les responsables des centres opérationnels (SOC) ou les équipes de réponse aux incidents sont particulièrement exposés à des niveaux de stress aigus, du fait de la nature continue, réactive et imprévisible de leurs missions** [3, 4]. À cela s'ajoutent **des facteurs organisationnels**, comme le manque de reconnaissance, l'isolement, la rotation rapide des effectifs et l'absence de soutien psychologique, qui aggravent les risques de désengagement et d'attrition. Plus alarmants encore, **certains travaux comparent désormais le niveau d'épuisement professionnel des professionnels de la cybersécurité à celui observé parmi le personnel soignant en milieu hospitalier** [5].

Dans ce contexte, il devient important de mieux comprendre les mécanismes à l'origine du stress professionnel en cybersécurité, d'en évaluer les impacts humains et organisationnels, et d'explorer des pistes de prévention réellement adaptées à la réalité de ce secteur. Cette note de synthèse vise ainsi à dresser un état des lieux structuré de la question. Elle s'articulera en trois temps : une analyse des spécificités cognitives et opérationnelles du travail en en cybersécurité ; un examen des causes et des conséquences de l'épuisement professionnel; enfin, une exploration des approches ergonomiques, psychologiques et organisationnelles susceptibles d'en limiter l'occurrence.

Un secteur sous tension : surcharge cognitive et fatigue en cybersécurité

Le domaine de la cybersécurité se caractérise par une intensité cognitive et émotionnelle rarement égalée dans les autres secteurs des technologies de l'information. La mission des professionnels qui y œuvrent consiste à détecter, analyser, prévenir et contrer des menaces souvent masquées, évolutives, et à fort potentiel destructeur. **Ces fonctions critiques nécessitent une vigilance constante, une capacité de réaction rapide, et une anticipation des comportements adverses**. Ces exigences sont renforcées par un environnement instable, une pression temporelle constante, et une lourde responsabilité en cas de défaillance.

La spécificité cognitive des métiers de la cybersécurité

Plusieurs études montrent que les professionnels de la cybersécurité doivent maintenir un niveau d'attention élevé sur de longues périodes, souvent sans retour immédiat sur l'efficacité de leurs actions [3, 5]. Les analystes de centres de sécurité opérationnelle, par exemple, passent leurs journées à analyser des flux d'alertes, dont une grande majorité représente de faux positifs. **Cette répétition génère une fatigue de sécurité, combinant surcharge cognitive, lassitude décisionnelle et désengagement progressif** [6]*. Le concept de cyberfatigue désigne **une forme particulière d'épuisement émotionnel et cognitif induit par l'exposition continue à des signaux d'alerte et à des exigences sécuritaires multiples** [3]. Elle se traduit par une baisse de vigilance, une perte d'engagement, et parfois une minimisation inconsciente des risques. Il existe plusieurs formes spécifiques de fatigue: la fatigue d'alarme, causée par la fréquence élevée de faux positifs, la fatigue informationnelle, liée à la sur-charge de directives, et la fatigue décisionnelle, due à l'incertitude dans les choix à faire face aux incidents [6].

Le *Cyber Operations Stress Survey* (COSS) a permis de mesurer cette surcharge de manière systématique, en la reliant à la fatigue, à la frustration, et à la charge mentale [7]. Les résultats confirment que **le niveau de stress dans les opérations tactiques cyber est comparable à celui observé chez les contrôleurs aériens ou les chirurgiens confrontés à des interventions d'urgence à haut risque** [7]. Le stress est ici chronique, lié à l'incertitude, à l'anticipation permanente, et au manque de marges d'erreur.

Afin de comprendre ces phénomènes, **le modèle des exigences et ressources au travail (*JD-R model*) est souvent mobilisé** [8]. Ce cadre théorique stipule que **le stress résulte d'un déséquilibre entre les exigences professionnelles** (charge de travail, urgence, complexité des tâches) **et les ressources disponibles** (soutien hiérarchique, autonomie, reconnaissance, outils adaptés) [8]. Des chercheurs ont appliqué ce modèle à un échantillon de professionnels de la cybersécurité et leurs résultats confirment que **la surcharge de travail, les attentes irréalistes, et la faiblesse du soutien organisationnel figurent parmi les principaux prédicteurs de l'épuisement professionnel** [9]. Par exemple, de nombreux répondants rapportent l'absence de renfort en cas de surcharge, ou encore un manque de reconnaissance même après la résolution rapide d'un cyberincident [9]. Le même déséquilibre est observé dans les situations de réponse à un incident. Une autre équipe de chercheurs ont montré que **les analystes d'incident vivent une triple pression : temporelle, cognitive et émotionnelle**. L'imprévisibilité des attaques, les heures de travail prolongées, et l'isolement face à la décision créent un terrain propice à l'épuisement [10].

* Voir la note de synthèse "Les sources menant à la fatigue de sécurité chez les employés" (Vol. 4, num. 4).

Le rôle de facteurs contextuels et personnels

Les causes de la surcharge cognitive ne sont pas uniquement liées à la nature du travail. **D'autres facteurs, comme le genre, la hiérarchie, ou la qualité du sommeil, modulent la perception du stress**. Par exemple, **les femmes travaillant comme consultantes en cybersécurité déclarent des niveaux d'épuisement émotionnel plus élevés que leurs homologues masculins** [11]. Ce différentiel est accentué par leur sous-représentation dans le secteur (16,8% de l'échantillon) et les attentes implicites liées à la performance. Il existe également **un lien significatif entre manque de sommeil et symptômes d'épuisement professionnel, notamment chez les cadres supérieurs**, et ce puisque l'analyse statistique de cette dernière confirme que la qualité subjective du sommeil est un prédicteur significatif de la fatigue émotionnelle [11].

Enfin, **les effets de la surcharge cognitive sont souvent sous-déclarés**. Dans une enquête menée auprès de 50 professionnels de la cybersécurité issus principalement de grandes entreprises (68 % employant plus de 10 000 salariés), 60 % des répondants se disent peu enclins à signaler leur stress ou leur épuisement à leur hiérarchie [9]. **Cette réticence, motivée par la crainte d'être perçus comme faibles ou peu fiables, alimente un tabou organisationnel qui empêche toute reconnaissance formelle du problème**. Ce climat de silence contribue à un cercle vicieux de surmenage invisible, où les symptômes persistent sans accompagnement adéquat.

Des causes structurelles et systémiques

Le modèle des exigences-ressources (*JD-R*), déjà évoqué plus haut, constitue un cadre analytique utile pour comprendre la genèse de l'épuisement professionnel. **Lorsque les exigences professionnelles** (charge cognitive, rythme d'alerte, pression de disponibilité) **dépassent durablement les ressources disponibles** (autonomie, reconnaissance, soutien psychologique), **les individus entrent dans un cycle d'épuisement qui peut conduire au désengagement, voire à la rupture**.

Une étude qualitative reposant sur des entrevues auprès de professionnels a permis de montrer que **dans les phases de crise** (attaque, rançongiciel, perte de données), **les équipes subissent une tension proche de celle observée dans des situations de guerre** [12]. **Le stress est alors multidimensionnel : il est cognitif** (prise de décision sous incertitude), **émotionnel** (peur, culpabilité, isolement), **et relationnel** (conflits de responsabilité, manque de soutien managérial) [12]. Cette intensité explique en partie pourquoi certains professionnels expriment un désir de quitter le secteur après un événement grave.

Le poids des environnements opérationnels fermés

Les centres opérationnels de sécurité (SOC) sont souvent cités comme les environnements les plus propices à l'épuisement professionnel. Par exemple, les analystes en SOC développeraient une forme de désengagement cynique causée par la répétitivité des tâches, la pression du temps réel, l'absence de rétroaction et la surcharge de fausses alertes [13]. Cette dynamique est confirmée par d'autres chercheurs qui ont identifié plusieurs cercles vicieux dans la gestion humaine des SOC : attentes irréalistes, faible reconnaissance, décalage entre compétences et missions, rotation excessive du personnel [14].

Les conséquences sont lourdes : **erreurs d'analyse, perte de vigilance, baisse de productivité, mais aussi démissions massives**. Un analyste sur deux envisage de quitter son poste dans les trois prochaines années selon certaines enquêtes [15]. D'un point de vue organisationnel, ces départs non anticipés entraînent une perte de savoirs critiques et une augmentation des risques de sécurité.

Conséquences de l'épuisement professionnel en cybersécurité: un enjeu humain et organisationnel

Bien qu'il trouve ses racines dans des facteurs structurels et organisationnels analysés précédemment, **l'épuisement professionnel en cybersécurité produit des effets profonds et durables, tant sur les individus que sur les structures qui les emploient**. Cette section met l'accent sur les conséquences humaines telles que les troubles de santé mentale, le désengagement, et l'isolement professionnel, ainsi que sur les répercussions organisationnelles, telles que la baisse de performance, le roulement de personnel élevé et la fragilisation des dispositifs de sécurité, ce qui affecte la performance globale des organisations.

Des effets humains sous-estimés

L'une des spécificités de l'épuisement professionnel dans le secteur de la cybersécurité est qu'**il s'exprime rarement sous des formes visibles**. Les signes précoces de fatigue, de désengagement ou de perte de motivation sont souvent masqués par une culture professionnelle valorisant la résistance, la disponibilité permanente, et la technicité [5]. **Cette culture de la performance empêche souvent les individus de verbaliser leur mal-être, voire de le reconnaître**.

Pourtant, les effets sont bien réels : **troubles anxieux, insomnies, crises de panique, repli social, voire de la dépression**. Dans une enquête auprès de 119 professionnels de la cybersécurité en Australie, des chercheurs ont souligné que **les troubles du sommeil sont particulièrement prévalents chez 30% des responsables de sécurité** [11]. Ils contribuent à une baisse de l'efficacité professionnelle et à une augmentation des conflits internes (irritabilité, perte de patience, confusion décisionnelle).

En parallèle, **l'épuisement professionnel a des effets organisationnels majeurs** : augmentation des erreurs, conflits d'équipe, baisse d'engage-ment, mais aussi hausse du risque d'incident lié à l'humain (négligence, oubli, désobéissance aux protocoles) [16]. Une enquête menée auprès de 245 professionnels de la cybersécurité répartis dans plusieurs secteurs (gouvernement, santé, entreprises privées) montre que **62 % des répondants associent leur fatigue à des oublis ou des erreurs récurrentes, et 58 % reconnaissent avoir désobéi aux procédures de sécurité sous l'effet de la surcharge ou de l'épuisement** [16]. Ce que les auteurs appellent « la fragilité humaine du système cyber » mérite dès lors d'être traité comme un facteur de risque à part entière [16].

Des facteurs transversaux : genre, isolement, reconnaissance

L'épuisement professionnel en cybersécurité n'est pas uniforme : il est modulé par plusieurs facteurs transversaux. D'abord, la question du genre. Les femmes dans les métiers cyber cumulent plusieurs désavantages structurels [11]. D'une part, elles subissent une surcharge émotionnelle c'est-à-dire qu'elles doivent gérer des tensions relationnelles, des attentes implicites de disponibilité et de performance accrues, tout en endossant souvent un travail émotionnel supplémentaire, comme apaiser les tensions ou compenser les défaillances organisationnelles. D'autre part, elles sont confrontées à une invisibilisation professionnelle, une faible représentativité dans les postes décisionnels et une minimisation fréquente de leurs compétences techniques [11]. Ce stress différencié s'ajoute aux exigences déjà élevées de leurs fonctions, renforçant ainsi leur vulnérabilité à l'épuisement professionnel.

Ensuite, **l'isolement professionnel, particulièrement dans les environnements en télétravail ou post-crise sanitaire, renforce les risques d'épuisement**. Plusieurs études notent que la perte de lien social avec les collègues affaiblit la capacité à partager la charge émotionnelle [4, 12]. Enfin, **le manque de reconnaissance constitue un facteur aggravant**. Les professionnels de la cybersécurité

sont souvent perçus comme des « techniciens » et non comme des acteurs stratégiques [17]. Ce statut ambigu, entre invisibilité et responsabilité excessive, alimente un sentiment d'injustice et de désengagement.

Le coût de l'épuisement professionnel pour les organisations

Au-delà des individus, **l'épuisement professionnel constitue un risque systémique pour les organisations**. Il fragilise les équipes de cybersurveillance par une rotation excessive des employés, affaiblit la réponse aux incidents et accroît la vulnérabilité globale aux menaces. D'ailleurs, **la surcharge de travail des équipes techniques est un facteur reconnu dans les failles de sécurité industrielle** [18]. Une équipe fatiguée, mal soutenue, mal formée ou instable, constitue un point de défaillance critique, au même titre qu'un logiciel obsolète ou un mot de passe faible. Ce constat impose une redéfinition de la notion même de « résilience » en cybersécurité : on ne peut pas sécuriser les systèmes sans protéger ceux qui les sécurisent.

Prévenir l'épuisement : mise en place d'approches humanistes et d'environnements capacitant

Face à l'ampleur du phénomène d'épuisement professionnel en cybersécurité, la question n'est plus de savoir s'il existe, mais comment y remédier de façon structurelle et durable. En effet, le *VMWare Global Incident Response Threat Report* de 2022, indique que **plus de la moitié (51 %) des professionnels du secteur présentent des symptômes d'épuisement professionnel, et parmi eux, près des deux tiers (65 %) songent sérieusement à quitter leur poste** [12]. Cette dernière partie examine les pistes d'action concrète en matière de prévention du burnout. Ces approches, qui s'appuient sur les apports de l'ergonomie, de la cyberpsychologie, de la gestion des ressources humaines et des sciences cognitives, visent à favoriser des conditions de travail plus humaines, capacitantes et durables. Elles impliquent aussi une reconfiguration du rôle des professionnels de la cybersécurité dans les organisations.

Dépasser le mythe de « l'erreur humaine »

La culture dominante dans les environnements techniques tend à réduire les incidents à des erreurs humaines, comme si celles-ci relevaient d'une faiblesse individuelle isolée. Or, **plusieurs travaux montrent que ces erreurs sont souvent les symptômes visibles d'un système organisationnel dysfonctionnel**.

Plusieurs auteurs appellent ainsi à un changement de paradigme, pour passer d'une vision culpabilisante à une approche systémique [17, 19]. Dans cette perspective, **la sécurité ne dépend pas seulement de protocoles ou de procédures, mais aussi de la capacité des individus à faire face à l'incertitude, à l'ambiguïté et à la charge émotionnelle**. Cela suppose de reconnaître la valeur du facteur humain comme une ressource stratégique, et non comme une faille potentielle.

Favoriser des environnements capacitant

Le concept d'environnement capacitant désigne un milieu de travail qui permet à chacun d'exercer et de développer ses compétences tout en maintenant sa santé et son bien-être [20]. Dans le contexte de la cybersécurité, ce concept peut être utilisé pour proposer une grille de lecture des conditions favorables au maintien de l'engagement des analystes [21].

Les critères identifiés incluent :

- La reconnaissance des efforts;
- Un équilibre charge/ressources;
- L'accès à la formation continue;
- Une clarté des rôles; et
- Des marges d'autonomie décisionnelle.

Ces dimensions permettent de renforcer le pouvoir d'agir des professionnels, et donc leur résilience face à la pression.

Mesurer le stress pour mieux l'anticiper

Un autre levier de prévention réside dans **la mesure systématique du stress et de la charge mentale**. Par exemple, le *Cyber Operations Stress Survey* (COSS) représente un outil de terrain conçu pour évaluer la fatigue, la frustration et la charge cognitive en environnement SOC [7]. Facile à administrer, **il permet de repérer les signaux faibles d'épuisement avant qu'ils ne se traduisent en arrêts maladie ou démissions**. De tels outils peuvent s'intégrer à une politique plus large de santé organisationnelle, incluant des entretiens réguliers, des temps de décompression, ou encore des canaux de signalement anonymes pour les situations de détresse.

Former à la résilience et au soutien mutuel

La prévention passe aussi par **le développement des compétences psychosociales** des professionnels de la cybersécurité. Les programmes de formation à l'inoculation du stress (*stress inoculation training*), inspirés de la psychologie militaire, permettent aux individus de développer des stratégies d'adaptation face aux situations critiques [5]. Ce type de formation comprend généralement plusieurs phases :

- **Prise de conscience des manifestations physiques et psychologiques du stress** (accélération du rythme cardiaque, pensées envahissantes, etc.).
- **Apprentissage de techniques d'adaptation** telles que les exercices de respiration contrôlée, la visualisation positive ou la restructuration cognitive des pensées anxiogènes.
- **Mises en situation simulées**, parfois en réalité virtuelle, pour entraîner ces stratégies dans des environnements réalistes, mais sécuritaires.

Ces méthodes, déjà utilisées dans des domaines à haute intensité comme l'armée ou la médecine d'urgence, peuvent renforcer la résilience mentale des équipes de cybersécurité confrontées à des attaques ou à des situations de crise. Par ailleurs, des auteurs insistent sur **l'importance de la cohésion des équipes**, **de la reconnaissance entre pairs, et du soutien hiérarchique**. Ils proposent un modèle de gestion du capital humain en SOC, dans lequel le bien-être des analystes est vu comme une ressource à entretenir, au même titre que l'infrastructure technique [14]. En effet, des actions simples (rétroaction, mobilité interne, mentorat) peuvent significativement réduire les effets de l'épuisement professionnel.

Une organisation du travail à repenser

Enfin, la question de la structure organisationnelle ne peut être éludée. **Le modèle JD-R montre qu'une organisation ne peut durablement protéger ses agents si elle ne veille pas à équilibrer les charges imposées avec des ressources adaptées** [9]. Cela suppose de :

- Revoir les horaires;
- Diversifier les missions; et
- Favoriser une culture du droit à la pause.

De plus, une étude portant sur les profils neuroatypiques (TDA/H) montre que **des aménagements personnalisés** (temps de concentration protégé, routines stables, soutien émotionnel) **peuvent aussi bénéficier à l'ensemble des équipes**. Une telle réorganisation repose sur une vision humaniste de la cybersécurité, dans laquelle les professionnels ne sont plus considérés comme des remparts techniques, mais comme des êtres humains dotés de vulnérabilité et de ressources à valoriser [22].

Les leviers de prévention de l'épuisement professionnel en cybersécurité ne résident pas uniquement dans des solutions individuelles, mais dans des transformations collectives et structurelles. Il s'agit de **créer des environnements où le travail n'est plus synonyme de tension permanente, mais de défi soutenable**, d'apprentissage et de collaboration.

Conclusion

L'épuisement professionnel dans le secteur de la cybersécurité n'est ni un phénomène marginal ni une défaillance individuelle. **Il s'inscrit dans une réalité de travail marquée par la surcharge cognitive, la pression temporelle constante, la faible reconnaissance des efforts, et la complexité croissante des menaces numériques**. Les professionnels du domaine tel que les analystes, ingénieurs et gestionnaires se retrouvent au cœur d'une tension permanente entre efficacité technique et vulnérabilité humaine.

La littérature récente met en lumière des facteurs convergents à l'origine de cette fatigue professionnelle : **des environnements de travail hypernormés, des alertes constantes (souvent injustifiées), une pression à la performance dans un secteur où l'échec n'est pas permis, et un manque puissant de dispositifs de soutien organisationnel**. En résulte une spirale de stress chronique, de désengagement et, dans les cas les plus sévères, d'épuisement professionnel avéré.

Mais cette réalité, si préoccupante soit-elle, n'est pas une fatalité. Plusieurs pistes d'action émergent : **repenser l'organisation du travail, intégrer des outils de mesure du stress, former les équipes à la gestion de la charge mentale, valoriser le rôle du facteur humain dans la performance collective**. Des modèles comme le JD-R ou les environnements capacitant apportent un cadre pour équilibrer exigences et ressources, et favoriser des dynamiques de travail plus soutenables.

Ce changement de perspective implique de reconnaître la subjectivité des travailleurs de la cybersécurité, leurs émotions, leurs fragilités et leur droit à un cadre de travail sain. **Il s'agit, en somme, de sécuriser non seulement les systèmes, mais aussi ceux et celles qui les protègent**.

À l'heure où la sécurité numérique devient un pilier de la souveraineté économique et institutionnelle, il est urgent de comprendre que la résilience des infrastructures repose sur la santé mentale des professionnels qui les maintiennent. Promouvoir une cybersécurité durable, c'est aussi penser une organisation du travail juste, humaine, et capable de faire face aux défis de demain.

Recommandations

À la lumière des constats développés dans cette note de synthèse, plusieurs leviers d'action peuvent être proposés pour réduire l'occurrence de l'épuisement professionnel en cybersécurité et renforcer la résilience humaine du secteur. Ces recommandations s'adressent à la fois aux milieux académiques et scientifiques qui étudient ce phénomène, ainsi qu'aux organisations et employeurs du domaine cyber.

<u>Recommandations pour la recherche</u>

- **Inclure davantage de profils neuroatypiques dans les études** : Les personnes présentant des traits cognitifs spécifiques (TDA/H, hypersensibilité, etc.) peuvent être à la fois vulnérables et performantes dans des contextes cyber [22]. Il est essentiel de mieux comprendre leurs besoins pour concevoir des environnements inclusifs et protecteurs.
- **Développer des outils de diagnostic du stress et de l'épuisement professionnel adaptés aux contextes cyber** : Le COSS (*Cyber Operations Stress Survey*) constitue une base solide [7]. Il conviendrait d'enrichir ce type d'outils pour mieux détecter les signaux faibles d'épuisement, y compris dans des environnements hybrides ou dématérialisés.
- **Approfondir les recherches sur les facteurs cognitifs et comportementaux** : La charge mentale, la vigilance prolongée, la fatigue d'alerte ou encore la désensibilisation sont encore peu modélisées dans la littérature.

Une meilleure compréhension de ces phénomènes permettrait d'adapter les stratégies de formation, de gestion et de soutien psychologique.

- **Explorer les effets différenciés selon les genres, les rôles et les trajectoires professionnelles** : Certains profils (notamment les femmes dans des fonctions de conseil ou de coordination) sont plus exposés à l'épuisement professionnel [11]. Une analyse fine des parcours est nécessaire pour concevoir des mesures ciblées.

Recommandations pour les entreprises et les organisations :

- **Assurer un équilibre entre exigences professionnelles et ressources disponibles** : En s'appuyant sur le modèle JD-R, les employeurs doivent veiller à fournir des ressources suffisantes : temps de repos, reconnaissance, autonomie, soutien émotionnel [9]. Cela suppose une évaluation régulière de la charge de travail réelle.
- **Mettre en place des programmes de prévention de la fatigue** : Inspirés par les approches en psychologie du travail, ces programmes peuvent inclure des formations à la gestion du stress, des temps de déconnexion planifiés, des cellules d'écoute ou des dispositifs d'alerte internes pour les situations de surmenage [5].
- **Favoriser des environnements de travail capacitant** : Il est possible de construire des environnements qui valorisent les compétences, qui offrent des marges d'autonomie, et reconnaissent les efforts [[21]. Cela passe par une évolution de la culture managériale et un accompagnement des équipes.
- **Inclure la santé mentale dans les indicateurs de performance des équipes cyber** : Au même titre que les temps de réponse aux incidents ou les indicateurs techniques, le bien-être des analystes doit devenir un critère stratégique, intégré aux tableaux de bord des responsables de sécurité.
- **Mettre fin à la banalisation du surengagement et du présentéisme** : Une culture organisationnelle qui valorise la disponibilité 24/7 ou la surproductivité favorise l'épuisement. Il est crucial de légitimer les pauses, les ralentissements et la parole sur la fatigue, sans les considérer comme des faiblesses.

Références

[1] Ogbanufe, O. et Spears, J. (2019, décembre). *Burnout in cybersecurity professionals. Communication.* Présentée au Workshop on Information Security and Privacy (WISP 2019), Munich, Allemagne.

[2] Maslach, C. et Jackson, S. E. (1981). The measurement of experienced burnout. J*ournal of Occupational Behavior*, *2*(2), 99–113.

[3] Reeves, A., Delfabbro, P. et Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, *11*(1), 1–18.

[4] Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, *13*(1), 49-72.

[5] Wiederhold, B. K. (2024). Wired for exhaustion: The urgent need for human-centric cybersecurity. Cyberpsychology, *Behavior, and Social Networking*, *27*(10), 677–679.

[6] Desjardins, L. (2024). Les sources menant à la fatigue de sécurité chez les employés. *Notes de synthèse*, *4*(4), 1–5. Chaire de recherche en prévention de la cybercriminalité.

[7] Dykstra, J. et Paul, C. L. (2018, août). *Stress and burnout in the cyber workforce*. Communication présentée au 11e USENIX Workshop on Cyber Security Experimentation and Test (CSET '18), Baltimore, MD, États-Unis.

[8] 1.Bakker, A. B. et Demerouti, E. (2007). The Job Demands–Resources model: State of the art. *Journal of Managerial Psychology*, *22*(3), 309–328.

[9] Arora, S. et Hastings, J. D. (2024). *A Survey-Based Quantitative Analysis of Stress Factors and Their Impacts Among Cybersecurity Professionals*. arXiv preprint arXiv:2409.12047.

[10] Nepal, S., Hernandez, J., Lewis, R., Chaudhry, A., Houck, B., Knudsen, E., ... et Czerwinski, M. (2024). Burnout in cybersecurity incident responders: Exploring the factors that light the fire. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1), 1-35.

[11] Reeves, A., Pattinson, M. et Butavicius, M. (2024). The sleepless sentinel: factors that predict burnout and sleep quality in cybersecurity professionals. *Information & Computer Security*, *32*(4), 477-491

[12] Virtanen, T. (2024, juin). Psychological Effects of Continuity-Threatening Cyber Incidents on Incident Response Professionals. *Communication présentée à la 23e Conférence européenne sur la cyber-guerre et la sécurité* (ECCWS 2024), Athènes, Grèce.

[13] Hull, J. L. (2017). *Analyst burnout in the cyber security operation center-CSOC: A phenomenological study* (Thèse de doctorat, Colorado Technical University).

[14] Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J. et Rajagopalan, S. R. (2015). A human capital model for mitigating security analyst burnout. In *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 347-359)

[15] Reeves, A. et Coroneos, C. (2022). Why cybersecurity analysts leave: The state of burnout in SOC teams. *Cybermind Research Brief*.

[16] Singh, T., Johnston, A. C., D'Arcy, J. et Harms, P. D. (2023). Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(2), 100-126.

[17] Weber, C. (2017). La place de l'homme dans les enjeux de cybersécurité. *Stratégique*, *117*(4), 83-98.

[18] Lamy P., Perrin N., Nisrine G. (2024). Cybersécurité des machines et prévention des risques professionnels : état des lieux. *Congrès Lambda Mu 24 « Les métiers du risque : clés de la réindustrialisation et de la transition écologique »*, Institut pour la Maîtrise des Risques (IMdR), Oct 2024, Bourges, France. ‹hal-04895908›

[19] Teboul, B. (2022). Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive. *HAL*.

[20] Raspaud, A. et Falzon, P. (2020). De Sen à la pratique ergonomique : Conditions et moyens pour une intervention ergonomique capacitante. *Perspectives interdisciplinaires sur le travail et la santé*, *22*(1).

[21] Bourhim, A., Guillet, L., Lassalle, J. et Petr, C. (2023, juillet 4–7). Vers des environnements capacitants pour la cybersécurité : Proposition d'un cadre de recherche adapté. *Communication présentée au 12e Colloque EPIQUE – Psychologie ergonomique et ergonomie*, École du Val de Grâce, Paris, France.

[22] 1.Vézina, É. (2024). *Technologies de l'information, TDA/H et inclusion : vers de meilleures pratiques pour les employés et gestionnaires* [Mémoire de maîtrise, Université de Sherbrooke]. Savoirs UdeS.