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

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 16 Juin 2025

Le Hacking Éthique

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

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

SOMMAIRE

Introduction *3*
I. Qu'est-ce qu'un hacker éthique ? *4*
II. Les pratiques du hacking éthique aujourd'hui *5*
III. Un cadre juridique en construction *6*
IV. La place du hacker éthique dans l'écosystème cyber *7*
V. Table ronde et échange : déontologie, gouvernance et bonnes pratiques *8*
VI. Intermède : présentation de Jérôme Notin *9*
VII. Questions / Réponses *10*

Introduction

Le **Lundi de la cybersécurité du 16 juin 2025** s'est penché sur un sujet à la fois technique, juridique et sémantique : **le hacking éthique**. À l'heure où les cyberattaques ne cessent de croître en nombre et en sophistication, les hackers dits « éthiques » occupent une place croissante dans les dispositifs de défense numérique. Mais à quelles conditions leurs actions sont-elles légitimes ? Quel est leur statut juridique ? Quelle reconnaissance leur accorder, et dans quel cadre ?

Pour répondre à ces questions, deux intervenants complémentaires ont partagé leur expertise. **Myriam Quéméner**, magistrate honoraire, docteure en droit, spécialiste reconnue du droit du numérique et de la lutte contre la cybercriminalité, a apporté un éclairage rigoureux sur les **aspects juridiques et déontologiques** du hacking éthique. Elle est également coautrice, avec Amélie Köcke, de l'ouvrage *Hacker éthique et cybersécurité : opportunités et défis*, paru fin 2024.

À ses côtés, **Yassir Kazar**, fondateur et PDG de **Yogosha**, plateforme française de Bug Bounty, a exposé la réalité du terrain du hacking éthique : fonctionnement des programmes de chasse aux failles, motivations des chercheurs, maturité des entreprises, et perspectives d'évolution de cette pratique entre modèle collaboratif et industrialisation croissante.

Comme à l'accoutumée, une **séquence intermédiaire** a été animée par **Jérôme Notin**, directeur général de **cybermalveillance.gouv.fr**, pour présenter les avancées du dispositif **17Cyber**, développé avec la Police nationale et la Gendarmerie.

Ce rendez-vous de juin a permis de clarifier les enjeux juridiques, organisationnels et humains liés à l'intervention des hackers dans les stratégies de cybersécurité des entreprises et des institutions, tout en posant les bases d'une collaboration fondée sur la transparence et la confiance.

I. Qu'est-ce qu'un hacker éthique ?

En introduction de la séance, **Myriam Quéméner** a tenu à clarifier les termes pour éviter toute confusion sémantique, source fréquente de malentendus dans le débat public. Contrairement à l'image populaire du "pirate informatique", le hacker n'est pas nécessairement un acteur malveillant. Le terme **hacker** désigne avant tout un **passionné d'informatique**, souvent autodidacte, animé par la curiosité technique et la volonté de comprendre les systèmes. Il se distingue ainsi du **cracker**, dont l'objectif est délibérément nuisible : exploiter des vulnérabilités pour voler, saboter ou nuire.

Dans cette typologie issue de la culture numérique, **les hackers dits "chapeaux blancs"** (white hats) interviennent dans une démarche constructive, souvent avec l'accord des éditeurs de logiciels ou des entreprises, pour signaler les failles et proposer des correctifs. Les **"chapeaux noirs"** (black hats), au contraire, agissent de manière illégale ou illégitime, souvent à des fins lucratives. **Entre les deux**, on retrouve les "chapeaux gris" (grey hats), qui naviguent sur une ligne plus floue, identifiant des vulnérabilités sans toujours respecter les cadres d'autorisation.

Ce besoin de précision terminologique est d'autant plus important que les **représentations médiatiques** et les discours institutionnels confondent encore trop souvent ces profils. Pour **Myriam Quéméner**, parler de "hacking éthique" permet de légitimer une pratique qui, si elle est bien encadrée, constitue une ressource précieuse pour la cybersécurité. Le hacker éthique agit dans un cadre **contractuel, proportionné et coopératif**, souvent à travers des programmes officiels comme les **Bug Bounty**, ou dans des missions de **test d'intrusion autorisé** (pentests).

Elle souligne que la **valeur ajoutée du hacker éthique** réside dans sa capacité à penser "hors cadre", à détecter des vulnérabilités parfois invisibles aux yeux des développeurs ou des équipes de sécurité internes. C'est précisément cette agilité – longtemps perçue comme suspecte – qui fait aujourd'hui l'objet d'un réexamen favorable, à condition que la **légalité**, la **traçabilité** et le **respect des droits fondamentaux** soient au cœur de la démarche.

Ce travail de reconnaissance passe aussi par une meilleure **acculturation des décideurs**, encore trop frileux à ouvrir leurs systèmes à des acteurs extérieurs. Le hacking éthique, insiste-t-elle, ne relève pas de l'improvisation, mais d'une **approche méthodique**, souvent formalisée par des chartes, des clauses de confidentialité, et des protocoles d'action rigoureux.

Ainsi posées, ces définitions ont permis de situer le débat à venir dans une perspective claire : celle de la **coopération entre expertise technique et exigence juridique**, socle indispensable pour intégrer les hackers éthiques dans l'écosystème de cybersécurité.

II. Les pratiques du hacking éthique aujourd'hui

Yassir Kazar, entrepreneur et fondateur de **Yogosha**, une plateforme française de Bug Bounty, a pris la parole pour illustrer concrètement le rôle du hacker éthique dans l'écosystème actuel de la cybersécurité. S'appuyant sur son expérience opérationnelle, il a décrit les différentes modalités par lesquelles les hackers éthiques interviennent aujourd'hui auprès des entreprises, en particulier dans le cadre de **tests d'intrusion encadrés**.

Il existe plusieurs approches pour tester la robustesse d'un système informatique. La plus classique est le **pentest**, ou test d'intrusion, commandé par une entreprise auprès d'un prestataire de cybersécurité. Le périmètre est défini contractuellement, les actions sont encadrées dans le temps, et le rapport final reste confidentiel. Cette pratique est aujourd'hui bien intégrée, mais elle présente certaines limites : coût élevé, dépendance à quelques profils, manque de diversité dans les approches.

C'est dans ce contexte que s'est développée la pratique du **Bug Bounty**. Inspirée des États-Unis mais de plus en plus adoptée en Europe, elle repose sur un principe simple : **récompenser la découverte de failles de sécurité**. Concrètement, une entreprise met à disposition une partie de son système ou de son application sur une plateforme comme Yogosha, YesWeHack ou HackerOne, et des hackers volontaires – préalablement sélectionnés – sont invités à chercher des vulnérabilités. Si une faille est identifiée, elle est transmise de manière confidentielle à l'entreprise, et le chercheur reçoit une **prime proportionnelle à la gravité** de la vulnérabilité.

Yassir Kazar insiste sur la rigueur de ces dispositifs. Les hackers sont **vérifiés, encadrés contractuellement**, soumis à des règles de confidentialité strictes. Les entreprises peuvent choisir entre des programmes **privés** (sur invitation uniquement) ou **publics**, selon leur niveau de maturité et de tolérance au risque. Le Bug Bounty ne s'oppose pas au pentest : il vient **le compléter**, notamment par sa capacité à **mobiliser une communauté diverse**, à générer une **veille continue**, et à **offrir un retour sur investissement dynamique**.

Il a aussi évoqué les motivations des hackers éthiques. Contrairement à certaines idées reçues, tous ne cherchent pas uniquement la récompense financière. Beaucoup s'engagent par **passion**, par **envie de challenge technique**, ou encore pour se faire connaître dans un écosystème où la reconnaissance de la compétence est précieuse. Yogosha fonctionne d'ailleurs selon un modèle fermé, basé sur une sélection rigoureuse des profils, afin de garantir un **haut niveau de professionnalisme**.

Enfin, Yassir Kazar a mis en garde contre une vision naïve ou purement opportuniste du Bug Bounty. Ce modèle n'est pas adapté à toutes les organisations, et nécessite une **bonne préparation en amont**, une **capacité à trier, corriger et suivre les signalements**, et surtout une **culture de la sécurité** qui valorise l'ouverture et l'humilité face à la vulnérabilité.

III. Un cadre juridique en construction

Dans un second temps, **Myriam Quéméner** est revenue en détail sur la question centrale du **cadre juridique applicable au hacking éthique**. Si la démarche des hackers « chapeaux blancs » peut sembler moralement justifiée, elle ne va pas toujours de soi sur le plan du droit. La juriste insiste d'abord sur une évidence trop souvent négligée : en droit français, **l'intrusion dans un système informatique sans autorisation explicite reste pénalement répréhensible**, même si elle se fait avec de « bonnes intentions ».

Le cœur de l'enjeu réside dans **l'existence d'un cadre contractuel clair**. Pour être licite, toute opération de recherche de failles doit s'inscrire dans un périmètre défini et validé par l'organisation concernée. À défaut, l'action peut être requalifiée en **accès frauduleux** ou en **atteinte à un système de traitement automatisé de données** (STAD), infractions prévues par le Code pénal. En d'autres termes, **la seule intention éthique ne suffit pas à rendre une action licite**.

Myriam Quéméner a souligné la nécessité de respecter des principes fondamentaux :

- **Proportionnalité** : l'action du hacker doit être limitée à ce qui est strictement nécessaire à la détection de la faille.
- **Autorisation préalable** : l'intervention doit être autorisée par le responsable du système concerné.
- **Traçabilité** : toutes les actions menées doivent être documentées et conservées dans une logique probatoire.
- **Confidentialité** : les failles découvertes ne doivent en aucun cas être divulguées publiquement sans validation préalable.

Elle a aussi rappelé que le droit positif reste en **évolution** sur ce sujet. Le **RGPD**, par exemple, encourage la notification des failles, mais ne couvre pas directement la question des tests proactifs. La jurisprudence est encore limitée, mais des précédents récents tendent à mieux distinguer les pratiques malveillantes des démarches collaboratives – à condition que ces dernières soient formalisées.

Le sujet du **Bug Bounty spontané** a également été abordé : peut-on alerter une entreprise d'une faille découverte « par hasard » ? En théorie, oui – mais cela suppose une **extrême prudence**, et une posture de **neutralité technique**. Sans contrat préalable, tout acte technique effectué sur le système peut être considéré comme une tentative d'intrusion. D'où l'importance de plateformes de Bug Bounty encadrées, qui **institutionnalisent un canal de communication sécurisé** entre les hackers et les organisations.

Enfin, la juriste a rappelé que le **droit à l'erreur** du collaborateur ne s'applique pas dans ce contexte : les actions de test doivent être menées dans le respect total des règles établies. Si un salarié, même de bonne foi, explore les systèmes de son entreprise sans autorisation, il s'expose à des sanctions.

En résumé, pour **Myriam Quéméner**, il est temps que le droit français reconnaisse pleinement le rôle du hacker éthique, tout en **structurant les conditions de son intervention**. L'encadrement juridique ne doit pas être un frein, mais une **garantie de confiance mutuelle** entre les parties.

IV. La place du hacker éthique dans l'écosystème cyber

Lors de son intervention, **Yassir Kazar** a mis en lumière l'évolution progressive de la place accordée aux hackers éthiques dans l'écosystème de la cybersécurité. Longtemps considérés avec suspicion, ces profils sont aujourd'hui de plus en plus intégrés dans les stratégies des entreprises, à mesure que leur **expertise** est reconnue comme complémentaire à celle des équipes internes.

Le **hacker éthique** n'est plus une figure marginale, mais un acteur à part entière des politiques de sécurité numérique, notamment via des dispositifs structurés comme les **Bug Bounty**, les **tests de pénétration mandatés**, ou encore les programmes de **divulgation coordonnée de vulnérabilités** (CVD – Coordinated Vulnerability Disclosure). Ces dispositifs permettent d'encadrer la relation entre le chercheur et l'organisation, en instaurant des règles de collaboration claires.

Cependant, **intégrer un hacker éthique** dans une logique opérationnelle de sécurité suppose plusieurs conditions :

- Une **maturité de la structure**, capable d'accepter une certaine transparence sur ses vulnérabilités
- Une **capacité de traitement**, pour analyser et corriger rapidement les signalements
- Et surtout une **culture interne ouverte**, qui valorise l'amélioration continue plutôt que le déni.

À ce titre, Yassir Kazar a mis en garde contre les effets de mode : le Bug Bounty n'est **ni un gadget**, ni une solution miracle. Il s'intègre dans une **approche globale** de la sécurité, en complément des audits, des tests automatisés, de la supervision et de la sensibilisation. Il ne remplace pas les tests d'intrusion classiques, mais permet de prolonger leur efficacité dans le temps en mobilisant une **communauté hétérogène, répartie, et souvent très réactive**.

L'enjeu, selon lui, est d'éviter deux écueils opposés :

1. Une **hostilité excessive** envers les hackers, qui bride l'innovation et prive les entreprises d'alliés précieux ;
2. Une **naïveté technophile**, qui surestime la capacité du modèle à tout régler sans cadre ni effort.

De son côté, **Myriam Quéméner** a souligné que cette évolution vers une reconnaissance du rôle des hackers s'accompagne d'un **besoin de structuration déontologique**. Si les Bug Bounty créent de nouvelles opportunités, ils génèrent aussi de nouveaux risques : défaut de contrôle sur les méthodes utilisées, absence de garanties sur la confidentialité des données manipulées, ou encore tentation, pour certains acteurs, de mettre en œuvre une **cybersécurité "low cost"**.

Enfin, tous deux s'accordent sur un point : la collaboration entre hackers et entreprises ne pourra se généraliser que si elle repose sur un **socle clair de confiance mutuelle**, fondé sur des **règles de gouvernance**, des **mécanismes de responsabilité partagée**, et une **valorisation du travail bien fait**.

V. Table ronde et échange : déontologie, gouvernance et bonnes pratiques

En fin de présentation, un temps d'échange a permis à **Myriam Quéméner** et **Yassir Kazar** de croiser leurs regards sur la **gouvernance** et la **déontologie** qui doivent encadrer le recours aux hackers éthiques. À travers leurs interventions respectives, un consensus s'est rapidement dégagé sur un point essentiel : la **cybersécurité est d'abord une affaire d'organisation humaine, avant d'être une question purement technique**.

Yassir Kazar a insisté sur l'importance, pour les entreprises, de construire un cadre d'intervention clair et responsabilisant. Cela passe par l'élaboration d'une **charte de Bug Bounty**, la définition d'un **périmètre précis**, et la mise en place d'un **processus structuré** de réception, de qualification, puis de remédiation des signalements de failles. Sans ce socle de gouvernance, l'efficacité de la démarche est rapidement compromise, et les relations avec les hackers peuvent se détériorer.

Il a aussi souligné que l'intégration des hackers éthiques ne peut réussir que si l'entreprise assume une **culture de l'ouverture et de la transparence**. Autrement dit : il faut accepter d'être vulnérable pour pouvoir progresser. L'enjeu, pour les RSSI et les équipes de sécurité, est de dépasser le réflexe défensif ou la tentation du déni.

Myriam Quéméner, quant à elle, a rappelé que toute collaboration de ce type doit s'inscrire dans un **cadre juridique robuste**, mais aussi **éthique**. Elle appelle à **formuler une véritable déontologie du hacker éthique**, incluant :

- La loyauté vis-à-vis de l'entreprise ;
- Le respect de la confidentialité des informations manipulées ;
- L'abstention de toute tentative d'exploitation, même si une faille critique est découverte.

Elle note également que certaines situations ambiguës peuvent survenir, notamment en cas de **signalement spontané d'une faille par un hacker sans contrat**. Dans ce cas, la posture de l'entreprise est déterminante : une réponse disproportionnée pourrait décourager les bonnes volontés, tandis qu'une réponse trop ouverte pourrait créer un précédent risqué. La solution réside dans la mise en place de **canaux officiels de divulgation coordonnée**, permettant de traiter ces signalements hors du Bug Bounty mais dans un cadre sécurisé.

Enfin, les deux intervenants se sont accordés sur l'importance d'une **sensibilisation des directions générales** : intégrer un hacker dans une stratégie de sécurité, ce n'est pas sous-traiter une tâche technique, mais **accueillir une expertise extérieure dans un rapport de confiance**. Cela suppose de l'anticipation, une réflexion stratégique, et un engagement à long terme.

VI. Intermède : présentation de Jérôme Notin

Comme à l'accoutumée dans le format des *Lundi de la cybersécurité*, un temps d'intermède a été consacré à une intervention extérieure, en l'occurrence celle de **Jérôme Notin**, directeur général de **cybermalveillance.gouv.fr**, le dispositif national d'assistance aux victimes d'actes de cybermalveillance.

Ancien cadre de l'ANSSI, Jérôme Notin a rappelé les grandes missions du **GIP ACYMA**, structure qu'il dirige depuis sa création. Son objectif est double : **informer le grand public, les entreprises et les collectivités sur les risques cyber**, et **fournir une aide concrète aux victimes** d'attaques numériques, qu'il s'agisse de particuliers, de TPE/PME ou de mairies.

L'intervention a porté plus spécifiquement sur un nouveau service en développement : le **17Cyber**, un projet co-construit avec la **Police Nationale**, la **Gendarmerie Nationale** et les équipes de cybermalveillance.gouv.fr. Ce dispositif vise à proposer une plateforme d'assistance aux victimes, équivalent numérique de l'appel 17, permettant en fonction de la menace d'échanger en 24/7 avec un policier ou un gendarme par messagerie instantanée. Il s'agit de **simplifier et centraliser les démarches**, tout en assurant une prise en charge rapide, adaptée à la nature de l'attaque.

Jérôme Notin a également mis en avant l'importance de la **coopération entre acteurs publics et privés**, saluant l'intérêt croissant porté par les entreprises à la prévention, à la formation et à la gestion des crises. Il a insisté sur la nécessité de **désacraliser la cybersécurité**, encore perçue comme technique ou inaccessible, pour mieux toucher les dirigeants, les élus locaux et les utilisateurs finaux.

Enfin, il a rappelé que la plateforme cybermalveillance.gouv.fr met à disposition de nombreux outils gratuits : kits de sensibilisation, simulateurs d'attaques, fiches pratiques, mais aussi un **réseau de prestataires de proximité** pour aider les structures victimes à redémarrer rapidement après un incident.

Cet intermède a été l'occasion de rappeler que, face à la montée continue des cyberattaques, **l'accessibilité, la pédagogie et la réactivité** sont devenues des piliers essentiels de la cybersécurité nationale.

VII. Questions / Réponses

Un document non critique peut-il, par recoupement, devenir sensible ?

Myriam Quéméner confirme que oui : ce sont souvent des enchaînements d'informations anodines, collectées séparément, qui permettent d'aboutir à des fuites à fort impact métier. C'est une des techniques courantes des cyberattaquants, et cela doit être anticipé dans la gouvernance de l'information.

Quels outils permettent de prévenir les fuites dans les environnements collaboratifs (Teams, etc.) ?

Des solutions comme **Microsoft Purview** offrent des capacités de classification, de gouvernance et de rétention des données dans les outils de collaboration. Ces environnements sont devenus des cibles majeures.

Quel est le coût réel d'un projet de DLP ou de Bug Bounty ? Pour 1€ de licence, combien en services ?

Selon **Yassir Kazar**, le coût de service peut représenter jusqu'à **10 à 20 fois le prix de la licence**, en raison des besoins d'intégration, de traitement des signalements et de coordination interne. Le retour sur investissement dépend fortement de la maturité de l'organisation.

Est-il pertinent d'interdire des requêtes identifiables sur Internet depuis une entreprise ?

L'idée exprimée est ancienne mais toujours valable : une **recherche identifiable** peut révéler des informations sensibles (projet en cours, recherche de solutions techniques, etc.). Des **règles internes de prudence** doivent encadrer les usages.

Existe-t-il des moteurs internes d'entreprise pour éviter la dépendance aux moteurs publics ?

Pas de réponse technique unifiée, mais les intervenants suggèrent que certaines grandes entreprises développent leurs **moteurs internes** ou systèmes fermés de documentation, selon leur taille et leurs enjeux.

Quelles obligations juridiques lors du déploiement d'un DLP ou d'un Bug Bounty ?

Myriam Quéméner rappelle que la mise en œuvre d'un dispositif de surveillance nécessite une **information claire des collaborateurs**, souvent via la **charte informatique**. La CNIL recommande la transparence sur les outils déployés, leur finalité et les données concernées.

Existe-t-il des guides ou des canaux internes pour signaler un doute ou une faille ?

Yassir Kazar recommande de mettre en place une **adresse email dédiée**, voire un canal de type chat sécurisé, pour poser des questions ou signaler une suspicion. Cela permet de créer une culture de sécurité accessible et réactive.

Faut-il adapter les bonnes pratiques de cybersécurité selon les métiers ?

Oui. Les règles générales sont utiles, mais l'**adaptation métier** est essentielle : un salarié en relation client n'a pas les mêmes risques ni les mêmes besoins qu'un ingénieur système. Des **guides personnalisés** par métier sont recommandés.

Faut-il interdire l'accès aux réseaux sociaux au sein de certaines équipes ?

Cela dépend du contexte. Si les réseaux sociaux n'ont **aucun lien avec les missions de l'équipe**, ils peuvent être bloqués. C'est aussi un moyen de limiter les **fuites involontaires** d'informations sensibles.