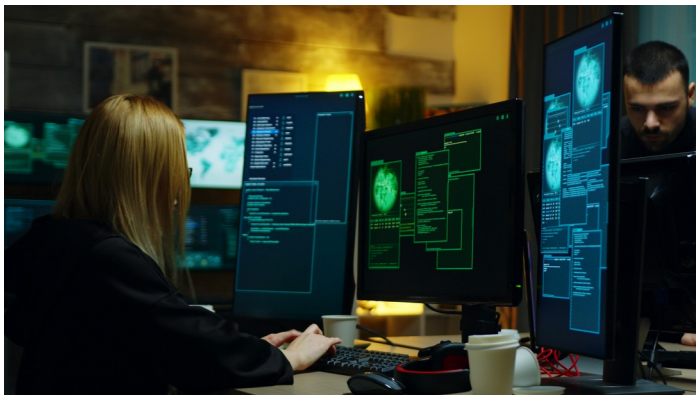
LES NOTES DU CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Numéro 89 – Juin 2023

Georges-Axel JALOYAN (Dr)



©DCStudio sur Freepik

Priorité stratégique de la prospective

L'avenir des territoires numériques

Le CREOGN certifie que ce document a été rédigé par un humain

HACKER ÉTHIQUE: UNE ESPÈCE EN VOIE D'EXTINCTION ?[1]

Le hacking éthique désigne un ensemble de normes et de pratiques visant à l'identification et la correction de vulnérabilités des systèmes d'informations par une approche coopérative avec les propriétaires des systèmes ciblés. Il s'articule en particulier autour de mécanismes de divulgation responsable, consistant à transmettre l'intégralité des éléments constitutifs de l'attaque à la cible, tout en maintenant pour une période convenue (appelée embargo) la confidentialité et l'exclusivité de la vulnérabilité entre les parties, le temps qu'un correctif soit publié.
Cette note retrace l'évolution du hacking éthique, de ses origines dans la clandestinité à sa normalisation au sein des départements de cybersécurité des entreprises. Elle détaille les causes conduisant à une séparation progressive entre le milieu de la cybersécurité et celui du hacking, les profils des hackers n'étant finalement que peu adaptés aux contraintes hiérarchiques et réglementaires des entreprises. Puis nous prolongerons ces tendances pour anticiper le futur du hacking éthique, présageant un retour progressif à la clandestinité qui devrait alimenter un marché gris revitalisé par la conflictualité interétatique dans le cyberespace.

I) Hacker: de la clandestinité à la célébrité

Le hacking trouve son origine dans les plaisanteries réalisées par les étudiants du *Massachusetts Institute of Technology* (MIT). Celles-ci se devaient d'impressionner par leur ingéniosité, bravant souvent les règles, tout en ne causant, *in fine*, que peu de dégâts. C'est dans ce terreau qu'apparaît le mouvement du logiciel libre au milieu des années 1980, fondé sur les valeurs de partage, d'ouverture, de gratuité et de décentralisation, sur un fond anarchiste et libertarien. Son « vaisseau amiral » est le projet GNU (dont les projets phares sont gcc, gdb, emacs, make, gimp...), popularisé en 1985 par le manifeste GNU[2]. Le hacking naît du même fond idéologique, avec les premières publications clandestines comme *Die Datenschleuder*[3] (publié en 1984 par le *Chaos Computer Club*) ou *Phrack* en 1985[4], ce dernier publiant dans son numéro inaugural des articles allant de méthodes d'ingénierie sociale par téléphone[5] à la fabrication de bombes à acétylène[6], en passant par l'ouverture fine des serrures Masterlock[7].

Ce réseau de hacking, très informel, connaît un très fort développement avec la popularisation des conventions de hackers, comme le *Chaos Communication Congress* (1984, Hambourg) ou DEF CON[8] (1993, Las Vegas). La clandestinité règne toujours, et le terrain se partage entre hackers et services de renseignement, qui cherchent à

1 Ce travail a été réalisé avant que l'auteur ne rejoigne Amazon.
2 Le manifeste GNU [traduit de l'anglais]. Disponible sur : https://www.gnu.org/gnu/manifesto.fr.html
3 Cf. : https://ds.ccc.de/download.html
4 Cf. : http://phrack.org/issues/1/1.html
5 Cf. : http://phrack.org/issues/1/4.html#article
6 Cf. http://phrack.org/issues/1/7.html#article
7 Cf. http://phrack.org/issues/1/6.html#article

mutuellement se démasquer. On peut citer, par exemple, le célèbre jeu « *spot the fed* » (repérer l'agent fédéral) pratiqué à DEF CON.

Cette opposition entre services et hackers s'estompe progressivement sous l'impulsion des États y voyant un vivier de candidats. En 2000, lors d'une table ronde à DEF CON, la *Central Intelligence Agency* (CIA), le *Department of Defense* (DoD) et la *National Security Agency* (NSA) exhortent les hackers à les rejoindre[9]. Cette hybridation apparaît au grand jour lors des *Opérations Olympic Games* (2009 : cyberattaques contre le programme nucléaire iranien) ou Aurora (2010 : cyberattaques contre les entreprises américaines). Malgré les affaires Wikileaks et Snowden (2010-2013), cette idylle culmine en 2016 avec le DARPA Cyber Grand Challenge à DEF CON 24 et, en 2018, avec le discours du directeur de la NSA à DEF CON 26[10], ainsi que celui du directeur technique de la Direction générale de la sécurité exterieure (DGSE) au Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)[11].

Ces interactions croissantes se formalisent progressivement dans les années 2000 en un marché blanc, dans lequel on retrouve les mécanismes de divulgation responsable incluant les *bug bounties*, *pentests* et hackathons, majoritairement autour d'entreprises spécialisées comme Amossys, Oppida, Atheos, FireEye, Kaspersky, ou généralistes comme les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) et BATX (Baidu, Alibaba, Tencent, Xiaomi). En parallèle se crée un marché gris, approvisionné par une première vague d'entreprises comme Vupen, Qosmos, Hacking Team, FinFisher GmbH ou Ennetcom.

Cette transformation du hacking en « InfoSec » (« *Information Security* » ; en français : regroupé sous le terme de cybersécurité), s'accompagne de la création de normes liées à la sécurité des systèmes d'information (critères communs ISO 15408, ISO 27001, référentiel général de sécurité[12], II 920 relative aux systèmes traitant des informations classifiées de défense, II 300 relative à la protection contre les signaux compromettants), de conférences spécialisées (*Black Hat*). De même, la création de formations orientées cybersécurité crée des grilles d'évaluation communes aux professionnels, avantageant de fait les profils types au détriment de profils atypiques, souvent passionnés et spécialistes de leur propre domaine d'activité.

II) Hacking et « InfoSec », un divorce à l'horizon

L'« InfoSec » connaît une période à vide à partir de 2015, avec la faillite ou la restructuration de nombreuses entreprises de la première vague des années 2000. Les États, bien qu'ayant beaucoup investi dans le domaine, ne fournissent que peu de solutions techniques satisfaisantes et se reposent souvent sur des entreprises du marché gris pour leurs opérations (comme démontré lors du piratage de *Hacking Team* en 2015).

La sécurité des systèmes d'informations ne s'améliore pas comme escompté, avec l'apparition de nouvelles menaces *via* les objets et véhicules connectés, les atteintes massives aux données personnelles (scandales Cambridge Analytica/AggregateIQ, ciblage comportemental assisté par l'intelligence artificielle – IA), les programmes de surveillance de masse (portes dérobées, *Deep Packet Inspection* – DPI –, lutte contre le chiffrement, grands pare-feux nationaux), la centralisation croissante (*Digital Rights Management* – DRM –, verrouillage matériel, perte d'intercompatibilité des systèmes, non-portabilité des données, brevets logiciels).

À cela s'ajoutent de nouvelles contraintes réglementaires conduisant à une inflation de la conformité au détriment de la technique. On peut, par exemple, citer la loi du 7 octobre 2016[13] qui n'apporte qu'une protection dérisoire aux

8 DEF CON : qu'est-ce que c'est ? [en ligne]. *Futura Sciences*. Disponible sur : https://www.futura-sciences.com/tech/definitions/informatique-def-con-15112/

9 « Law Enforcement Officials Recruit hackers » [en ligne]. *Forbes*, 2 août 2000. Disponible sur : https://www.forbes.com/2000/08/02/mu5.html?sh=3e6ff4ee34e4

10 JOYCE, Rob. DEF CON 26, NSA Talks Cybersecurity [en ligne], *YouTube*, 9 décembre 2018. Disponible sur : https://www.youtube.com/watch?v=gmgV4r25XxA

11 Symposium sur la sécurité des technologies de l'information et des communications. Conférence de clôture par Patrick PAILLOUX [en ligne]. Disponible sur : https://www.sstic.org/2018/presentation/2018_cloture/

12 ANSSI. Le référentiel général de sécurité (RGS) [en ligne]. Disponible sur : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

13 LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique [en ligne], article 47, p. 14. Disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

hackers, la loi Sapin[14] qui contraint considérablement le statut de lanceur d'alerte, le RGPD[15] qui limite fortement la collecte de données lors d'un *pentest*, ou encore la loi du 30 juillet 2018[16] sur le secret des affaires.

III) Vers un retour aux sources du hacking

La dégradation matérielle du milieu de l'« InfoSec », avec l'utilisation croissante de la sous-traitance – y compris à l'étranger – et la compression des budgets de cybersécurité au sein des entreprises, détourne les hackers vers les marchés gris et noir[17]. Pourquoi passer 6 mois à créer un *Proof of Concept* (PoC) rémunéré 40 000$ dans un programme de *bug bounty*, quand on peut gagner dix fois plus sur des cibles plus libres ?

Les hackers s'avèrent finalement peu adaptés au monde de l'entreprise car ils sont considérés comme à risque par ces dernières. Le management vertical a beaucoup de difficultés à encadrer cette nouvelle vague issue de la génération Z. Privées de ces profils dont elles ont pourtant besoin, les entreprises ont transféré une partie du risque vers des entités spécialisées (Agence nationale de la sécurité des systèmes d'information – ANSSI –, COMCyberGEND, ministères) ou les géants de l'Internet (cloud, SaaS), capables d'attirer ces profils au sein d'équipes dédiées, à l'instar du *Google Project Zero*[18].

La période 2015-2020 marque donc le grand retour des États dans le cyber. Ils s'équipent de structures dédiées (COMCYBER en 2017, montée en puissance de l'Institut de recherche criminelle de la gendarmerie nationale – IRCGN – et du Centre de lutte contre les criminalités numériques – C3N –, et rattachement de ce dernier au COMCyberGEND en 2021, autonomisation de l'USCYBERCOM en 2017, réserves de cyberdéfense en 2016), augmentent les effectifs et multiplient les plans d'attractivité. La formation et la recherche ne sont pas en reste, avec le recrutement de stagiaires et d'alternants, le financement de thèses, et la mise en place de partenariats académiques (Pôle d'excellence cyber, 2014[19]).

Cependant, la fidélisation des profils demeure un problème d'actualité. De nombreux talents ont été recrutés entre 2005 et 2019 dans les différentes entités ministérielles, mais l'absence d'avancement ainsi que la limitation de la durée des contrats conduisent à un renouvellement des effectifs important sur des postes qui demandent une grande spécialisation. La gendarmerie n'est pas en reste : le nombre de postes d'officiers commissionnés ou de civils publiés au Journal Officiel (JO) s'est accru ces dernières années. Concomitamment, de nouveaux modes d'organisation et de management se sont généralisés (horaires flexibles, télétravail, autonomie dans l'exécution des tâches...), nécessitant de nouveaux efforts afin de maintenir l'attractivité des administrations. Le recours aux entrepreneurs d'intérêt général peut pallier sur le court terme le manque de ressources, mais peu de solutions sur le long terme sont actuellement proposées.

La conséquence est l'inadéquation des mécanismes d'évolution de carrière traditionnels en administration (grilles, échelons et avancements publiés au JO) face à des personnels sur contrat court qui n'hésitent plus à partir ailleurs à échéance. À cette fin, les administrations, habituées à diriger des personnels de carrière (militaires, fonctionnaires), ont dû s'adapter à la mobilité de cette nouvelle catégorie de personnels, en important des compétences en gestion des ressources humaines issues du privé.

Ironie de l'histoire, le cyber redevient donc le terrain de jeu des États, et d'une nouvelle vague de hackers, dotés de nouveaux outils favorisant l'action clandestine (cryptomonnaies, messageries chiffrées *end-to-end*, systèmes d'exploitation amnésiques). Accompagnant le mouvement, le marché gris connaît une renaissance grâce à une nouvelle vague d'entreprises comme Clearview AI, Tykelab, RCS lab, NSO ou EncroChat.

14 LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique [en ligne]. Disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528

15 Le règlement général sur la protection des données, 23 mai 2018 [en ligne]. Disponible sur : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

16 Article L 151-1 du Code de commerce [en ligne]. Création de la LOI n° 2018-670 du 30 juillet 2018 – art. 1. Disponible sur : https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000005634379/LEGISCTA000037266547/

17 FRANCESCHI-BICCHIERAI Lorenzo. « Iphone Bugs Are Too Valuable to report to Apple » [en ligne]. *Vice.* 6 juillet 2017. Disponible sur : https://www.vice.com/en/article/gybppx/iphone-bugs-are-too-valuable-to-report-to-apple

18 « News and updates from the Project Zero team at Google » [en ligne]. Blog Google Project Zero. Disponible sur : https://googleprojectzero.blogspot.com/

19 Pôle d'excellence cyber. Présentation du pôle [en ligne]. Disponible sur : https://www.pole-excellence-cyber.org/presentation-du-pole/

IV) Perspectives

Dans ce qui suit, nous identifions trois tendances déjà amorcées. En ayant pour hypothèse qu'elles continueront, nous en dégageons des perspectives à court et moyen terme.

La première tendance est l'accroissement de l'étanchéité entre le milieu de la cybersécurité et celui du hacking. Cela entraîne une perte d'efficacité des mécanismes traditionnels d'interaction entre hackers et entreprises. Une étude du *National Telecommunications and Information Administration* (NTIA)[20] estime en 2016 à 50 % la proportion de chercheurs ayant envisagé de révéler une vulnérabilité sans divulgation responsable à cause de la frustration créée par la procédure, avec 4 % ayant déjà franchi le pas (Fig. 3 et 4 du document précité). En 2023, une étude empirique[21] sur les 100 dernières vulnérabilités de Linux montre qu'aucune n'a suivi le processus de divulgation responsable établi par Linux. Cette tendance devrait donc continuer, avec de plus en plus de vulnérabilités portées à la connaissance du public en dehors des canaux traditionnels du hacking éthique.

La diminution de la contribution des hackers aux entreprises sera compensée par une inflation administrative et une invasion des bonnes pratiques, avec une part grandissante des postes de conformité, d'éthique et de juridique. L'attention est focalisée sur les erreurs de procédures au détriment des erreurs de connaissances (*rule* vs *knowledge-based errors*, selon la terminologie SRK[22]). Cette stratégie est risquée, puisqu'elle rend aveugle au changement et augmente la fragilité globale en cas d'avancée disruptive dans le domaine (et de tels domaines ne manquent pas : IA, méthodes formelles, calcul distribué, quantique...).

La deuxième tendance est l'augmentation globale du risque cyber, en qualité comme en quantité. Les attaques sont de plus en plus impressionnantes, et à une fréquence de plus en plus élevée. Une recherche Google avec pour mot clé « *data breach* » confirme déjà la tendance. L'externalisation et la centralisation des acteurs conduiront à l'augmentation de l'impact des attaques, avec des points de défaillance uniques, à l'exemple de la vulnérabilité log4Shell[23], impactant la quasi-totalité des acteurs du web. Seuls quelques grands acteurs garderont la compétence sur la totalité du spectre, capables de résister à des attaques dévastatrices, par exemple une attaque DoS à plus d'un terabit/sec.

La troisième tendance est le retour progressif à la clandestinité des hackers. Cela se traduit par un refus croissant des contrats d'exclusivité des vulnérabilités trouvées, le refus des accords de non-divulgation (NDA), privilégiant les efforts de rétro-ingénierie pour éviter d'être lié à une entreprise. En symétrique, l'intérêt des entreprises vis-à-vis des hackers diminuera à mesure qu'il devient de plus en plus difficile de traiter avec eux.

Les sources de financement évoluant, une partie des hackers bascule vers les gouvernements soit directement, soit indirectement *via* un modèle de type société militaire privée (SMP). Imitant ce modèle, des entreprises sont souvent fondées par des anciens des services et recrutent prioritairement parmi ces mêmes profils, en reconversion dans le privé. Le hacking devient ainsi un service achetable par des États géopolitiquement proches.

Enfin, une partie se tournera vers des sources de financement (et une clientèle) de moins en moins légales, alimentant des activités cybercriminelles traditionnelles – parfois sous couverture étatique – comme des fraudes au paiement, des vols de cryptomonnaies, des usurpations d'identité ou des extorsions combinant *ransomware* et chantage à la révélation de données[24].

***Georges-Axel JALOYAN** est lieutenant de la réserve opérationnelle de la gendarmerie nationale, normalien, docteur en méthodes formelles appliquées à la cybersécurité.*

20 « Vulnerability Disclosure Attitudes and Actions. A Research Report from the NTIA Awareness and Adoption Group » [en ligne], 16 p. Disponible sur : https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

21 BAI, Weiheng, WU, Qiushi. « Towards More Effective Responsible Disclosure for Vulnerability Research » [en ligne], 4 p. Disponible sur : https://www.ndss-symposium.org/wp-content/uploads/2023/02/ethics2023-235691-paper.pdf

22 RASMUSSEN, Jens. « Human errors. A taxonomy for describing human malfunction in industrial installations » [en ligne]. *Journal of Occupationnal Accidents*, Vol. 4, n° 2-4, septembre 1982. Disponible sur : https://www.sciencedirect.com/science/article/abs/pii/0376634982900414

23 ANSSI. L'ANSSI alerte sur la faille de sécurité Log4Shell [en ligne]. Disponible sur : https://www.ssi.gouv.fr/publication/lanssi-alerte-sur-la-faille-de-securite-log4shell/

24 « From relentness adversaries to resilient businesses » [en ligne]. Disponible sur : https://www.crowdstrike.com/global-threat-report/

ISSN : 2428-7733