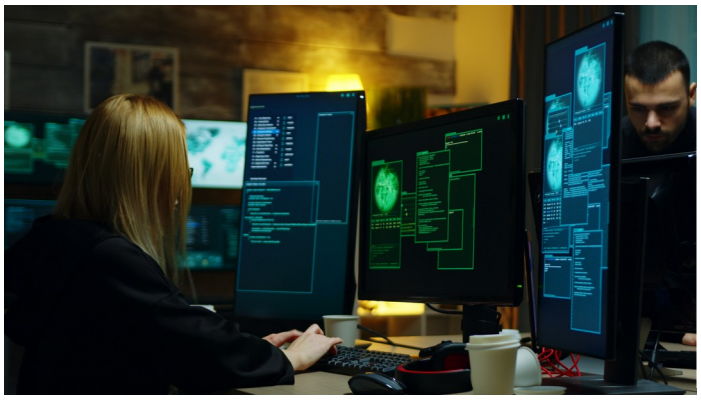
The CREOGN Research Notes

Gendarmerie Nationale Officers College Research Center

Issue 89 – June 2023

Georges-Axel JALOYAN (PhD)



©DCStudio sur Freepik

Priorité stratégique de la prospective

L'avenir des territoires numériques

ETHICAL HACKER: AN ENDANGERED SPECIES?[1]

Ethical hacking refers to a set of standards and practices aimed at identifying and correcting vulnerabilities in information systems through a cooperative approach with the owners of the targeted systems. More specifically, it revolves around responsible disclosure mechanisms, which consist of transmitting all the constituent elements of the attack to the target, while maintaining the confidentiality and exclusivity of the vulnerability between the parties for an agreed period (called an embargo), until a patch is published. This note traces the evolution of ethical hacking, from its underground origins to its normalization within corporate cybersecurity departments. It details the leading causes to a gradual separation between the cybersecurity and hacking communities, partly due to the lack of complementarity between hackers and hierarchical, regulatory constraints inherent to companies.

This brief then opts to build on these trends to anticipate the future of ethical hacking, forecasting a gradual return to clandestinely that should fuel a grey market revitalised by inter-state conflict in the cyberspace.

I) Hackers: from clandestinely to stardom

Hacking finds its origins in the pranks pulled by Massachusetts Institute of Technology (MIT) students. These were intended to impress by their ingenuity, often defying the rules, while ultimately causing little damage. It is in this context that the free software movement emerged in the mid-1980s, founded on the values of sharing, openness, free access and decentralisation, coupled with a background of anarchism and libertarianism. The movement's flagship project is the GNU project (introducing the gcc, gdb, emacs, make, gimp, etc. projects), made popular in 1985 with the GNU Manifesto[2]. Hacking draws its roots in the same ideological background. The first clandestine publications include *Die Datenschleuder*[3] (published in 1984 by the Chaos Computer Club) or *Phrack* in 1985[4], the latter bringing out in its inaugural issue articles ranging from methods of phone-based social engineering[5], the manufacture of acetylene bombs[6] or even the cracking of Masterlock padlocks[7].

This highly informal hacking network experienced a very strong development with the popularization of hacker conventions, such as the *Chaos Communication Congress* (1984, Hamburg) or DEF CON[8] (1993, Las Vegas).

1 This piece of work was produced prior to the author joining Amazon.
2 The GNU Manifesto. Available at : 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
8 DEF CON : what is it? [online]. *Futura Sciences*. Available at : https://www.futura-sciences.com/tech/definitions/informatique-def-con-15112/

Clandestine operations still prevail, and the battleground is torn between hackers and intelligence services, trying to unmask each other. One example is the famous "*spot the fed*" game played at DEF CON.

This clash between the services and hackers is gradually fading under the impetus of governments who see it as a breeding ground for candidates. In 2000, at a round table at DEF CON, the *Central Intelligence Agency* (CIA), the *Department of Defense* (DoD) and the *National Security Agency* (NSA) urged hackers to join them[9]. This hybridisation came to the fore during *Operations Olympic Games* (2009: cyber-attacks against Iran's nuclear programme) or Aurora (2010: cyber-attacks against US companies). Despite the Wikileaks and Snowden affairs (2010-2013), this collaboration culminated in 2016 with the DARPA Cyber Grand Challenge at DEF CON 24 and, in 2018, with the speech by the Director of the NSA at DEF CON 26[10], as well as that of the Technical Director of the French External Security Directorate (DGSE) at the Symposium on the Security of Information and Communication Technologies (SSTIC)[11].

These growing interactions were gradually formalised in the 2000s into a white market, embracing responsible disclosure mechanisms such as *bug bounties*, *pentests* and hackathons, mainly centred around specialised companies such as Amossys, Oppida, Atheos, FireEye and Kaspersky, or generalists such as GAFAM (Google, Apple, Facebook, Amazon, Microsoft) and BATX (Baidu, Alibaba, Tencent, Xiaomi). Simultaneously, a grey market was emerging, supplied by a first wave of companies such as Vupen, Qosmos, Hacking Team, FinFisher GmbH and Ennetcom.

This transformation of hacking into "InfoSec" has gone hand in hand with the creation of standards linked to the security of information systems (common criteria ISO 15408, ISO 27001, general security reference framework[12], II 920 on systems handling classified defence information, II 300 on protection against compromising signals), specialised conferences (*Black Hat*). Likewise, the creation of cybersecurity-oriented training courses has resulted in the creation of common assessment grids for professionals, thereby favouring typical profiles to the detriment of atypical profiles, which are often passionate and specialists in their own field of activity.

II) Hacking and InfoSec, a looming divorce

From 2015 onwards, InfoSec went through a period of decline, with the bankruptcy or restructuring of many companies from the first wave of the 2000s. Although governments have invested heavily in this industry, they have failed to provide satisfactory technical solutions and often had had to resort to grey market companies for their operations (as demonstrated by the hacking of *Hacking Team* in 2015).
The security of information systems has failed to improve as expected, with the emergence of new threats via connected objects and vehicles, massive personal data violations (Cambridge Analytica/AggregateIQ scandals, behavioural targeting assisted by artificial intelligence - AI), mass surveillance programmes (backdoors, *Deep Packet Inspection* - DPI –, the fight against encryption, major national firewalls), increasing centralisation (*Digital Rights Management* - DRM -, hardware lock-in, loss of intercompatibility between systems, non-portability of data, software patents).

Compounding this are new regulatory constraints leading to an inflation of compliance to the detriment of technology. Examples include the law of 7 October 2016[13] which provides derisory protection for hackers, the

9 "Law Enforcement Officials Recruit hackers [online]. Forbes, 2 August 2000. Available at : https://www.forbes.com/2000/08/02/mu5.html?sh=3e6ff4ee34e4

10 JOYCE, Rob. DEF CON 26, NSA Talks Cybersecurity [online], *YouTube*, 9 December 2018. Available from : https://www.youtube.com/watch?v=gmgV4r25XxA

11 Symposium on the security of information and communication technologies. Closing conference by Patrick PAILLOUX [online]. Available at : https://www.sstic.org/2018/presentation/2018_cloture/

12 ANSSI. Le référentiel général de sécurité (RGS) [online]. Available at : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs

13 LAW No. 2016-1321 of 7 October 2016 for a Digital Republic [online], Article 47, p. 14. Available at : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

Sapin law[14] which considerably restricts the status of whistleblowers, the RGPD[15] which severely limits the collection of data during a *pentest*, and the law of 30 July 2018[16] on business confidentiality.

III) Towards a return to the roots of hacking

The material degradation of the InfoSec environment, with the growing use of subcontractors - including abroad - as well as the squeeze on cybersecurity budgets within companies, is diverting hackers towards the grey and black[17] markets. Why spend 6 months creating a *Proof of Concept* (PoC) for USD 40,000 in a *bug bounty* programme, when you can earn ten times that on more open targets?

At the end of the day, hackers are not perceived as well suited for the corporate world because they tend to be regarded as high-risk by companies. Vertical management structures struggle to deal with this new wave of Generation Z employees. Deprived of the profiles they need, companies have transferred some of the risk to specialised bodies (Agence nationale de la sécurité des systèmes d'information - ANSSI -, COMCyberGEND, ministries) or Internet giants (cloud, SaaS), which are able to attract these profiles into dedicated teams, such as *Google's Project Zero*[18].

The period 2015-2020 therefore marks the great resurgence of governments in the cyber sector. They devoted structures were set up (COMCYBER in 2017, the rise of the Institut de recherche criminelle de la gendarmerie nationale - IRCGN - and the Centre de lutte contre criminalités numériques - C3N -, with the latter being attached to the COMCyberGEND in 2021, autonomisation of USCYBERCOM in 2017, cyber defence reserves in 2016), Increasing the number of personnel and increasing the number of attractiveness schemes. Training and research have not been left behind, with the recruitment of interns and work/study students, the funding of postgraduate theses, and the establishment of academic partnerships (Pôle d'excellence cyber, 2014[19]).

Nevertheless, the problem of retaining staff remains. A great deal of talents were recruited between 2005 and 2019 in various ministerial entities, but the lack of career advancement and the limited duration of contracts mean that there is a high turnover in positions that require a high degree of specialisation. The Gendarmerie is no exception: the number of commissioned officer and civilian vacancies published in the Journal Officiel (JO) has increased in recent years. At the same time, new methods of organisation and management have become widespread (flexible working hours, remote working, autonomy in the performance of tasks, etc.), requiring further efforts to maintain the attractiveness of government services. The use of general interest contractors can alleviate the shortage of resources in the short term, but only limited long-term solutions are currently on the table. The consequence is that the traditional career development mechanisms in the public sector (grids, steps and career advancement published in the Official Journal) are inadequate when faced with staff on short-term contracts who no longer hesitate to take up employment elsewhere when their contract expire. To this end, government agencies, which were accustomed to managing long-serving staff (military, civil servants), have had to adapt to the mobility of this new category of employees, by bringing in human resources management skills from the private sector.

Ironically, cyber is once again the playground of governments and a new wave of hackers, equipped with the latest tools for clandestine action (cryptocurrencies, *end-to-end* encrypted messaging, amnesiac operating systems). To keep pace with these trends, the grey market is enjoying a rebirth thanks to a new wave of companies such as Clearview AI, Tykelab, RCS lab, NSO and EncroChat.

---

14 Law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life [online]. Available at : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528

15 The General Data Protection Regulation, 23 May 2018 [online]. Available at : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

16 Article L 151-1 of the French Commercial Code [online]. Created by LOI n° 2018-670 of 30 July 2018 - art. 1. Available at : https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000005634379/LEGISCTA000037266547/

17 FRANCESCHI-BICCHIERAI Lorenzo. "Iphone Bugs Are Too Valuable to report to Apple " [online]. *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 [online]. *Google Project Zero blog*. Available at : https://googleprojectzero.blogspot.com/

19 Pôle d'excellence cyber. Presentation of the cluster [online]. Available at : https://www.pole-excellence-cyber.org/presentation-du-pole/

IV) Perspectives

In what follows, three already-initiated trends are identified. Assuming that these trends continue, short- and medium-term outlooks are drawn.

The first trend is the increasing impermeability between the cybersecurity and hacking communities. This leads to a deterioration in the effectiveness of traditional interaction mechanisms between hackers and companies. A study by the *National Telecommunications and Information Administration* (NTIA)[20] in 2016 estimated that 50% of researchers had considered disclosing a vulnerability without responsible disclosure because of the frustration created by the procedure, with 4% having already taken the plunge (Fig. 3 and 4 of the aforementioned document). In 2023, an empirical study[21] of the last 100 Linux vulnerabilities revealed that none had followed the responsible disclosure process established by Linux. This trend is therefore likely to carry on, with more and more vulnerabilities coming to public attention outside the traditional channels of ethical hacking.

The diminishing contribution of hackers to business will be matched by administrative inflation and an invasion of best practice, with a growing share of compliance, ethics and legal positions.
The focus is on procedural errors to the detriment of knowledge-based errors (*rule vs knowledge-based errors*, in SRK terminology[22]). This is a risky strategy, since it makes people blind to change and increases overall fragility in the event of a disruptive breakthrough in the field (and there is no shortage of such fields: AI, formal methods, distributed computing, quantum computing, etc.).

The second trend is the overall increase in cyber risk, both in terms of quality and quantity. Attacks are becoming ever more daunting, and ever more frequent. A Google search using the keyword "data breach" already confirms this trend. The outsourcing and centralisation of players will lead to an increase in the impact of attacks, with isolated vulnerabilities, such as the log4Shell[23] vulnerability, affecting almost all web players. Only a few major players will retain full-spectrum competence, capable of withstanding devastating attacks, such as a DoS attack at over one terabit/sec.

The third trend is that hackers are gradually reverting to the underground. This is reflected in a growing rejection of exclusivity contracts for vulnerabilities found, and the refusal of non-disclosure agreements (NDAs), favouring reverse-engineering efforts to avoid being linked to a company. Conversely, companies' interest in hackers is likely to wane as it becomes increasingly complex to engage with them.

As funding sources evolve, some hackers will turn to governments, either directly or indirectly *via* a Private Military Company (PMC)-style model. Imitating this model, companies are often founded by former service personnel and recruit primarily from these same profiles, transitioning to the private sector. Hacking is thus becoming a service that can be bought by geopolitically close states.

Finally, some of them will turn to sources of funding (and customers) that are ever less legitimate, fuelling traditional cybercriminal activities - sometimes under state cover - such as payment fraud, cryptocurrency theft, identity theft or extortion combining ransomware and data blackmail[24].

Georges-Axel Jaloyan *is a lieutenant in the operational reserve of the Gendarmerie Nationale, a graduate of the Ecole Normale Supérieure, and a PhD in formal methods applied to cybersecurity.*

Translated by Aude GREGORY, Reserve assistant gendarme

20 « Vulnerability Disclosure Attitudes and Actions. A Research Report from the NTIA Awareness and Adoption Group » [online], 16 p. Available at : 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 » [online], 4 p. Available at : 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 » [online]. *Journal of Occupationnal Accidents*, Vol. 4, n° 2-4, septembre 1982. Available at : https://www.sciencedirect.com/science/article/abs/pii/0376634982900414

23 ANSSI. L'ANSSI alerte sur la faille de sécurité Log4Shell [online]. Available at : https://www.ssi.gouv.fr/publication/lanssi-alerte-sur-la-faillede-securite-log4shell/

24 "From relentless adversaries to resilient businesses" [online]. Available at : https://www.crowdstrike.com/global-threat-report/