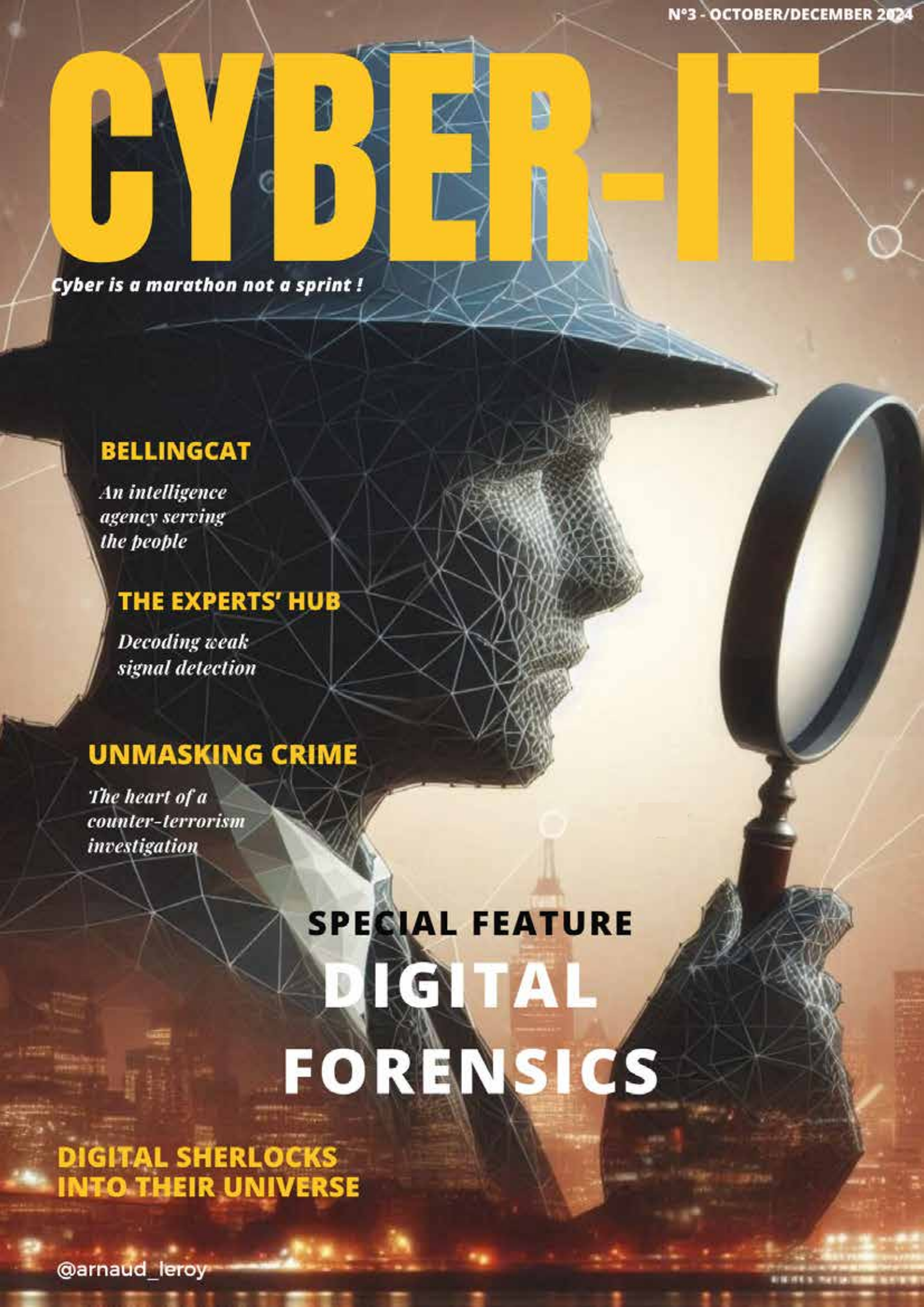
N°3 - OCTOBER/DECEMBER 2024

CYBER-IT

Cyber is a marathon not a sprint !



BELLINGCAT

An intelligence agency serving the people

THE EXPERTS' HUB

Decoding weak signal detection

UNMASKING CRIME

The heart of a counter-terrorism investigation

SPECIAL FEATURE

DIGITAL FORENSICS

DIGITAL SHERLOCKS INTO THEIR UNIVERSE

@arnaud_leroy

Inquiry / Requests?
cyberit.magazine@gmail.com

EDITORIAL

Have you ever wished you could get right into the heart of a thrilling investigation just like the ones you see in your favorite TV shows?
Are you curious to know what really goes on behind the scenes when they solve a case?

In this third issue of Cyber-IT Mag, dive into a real-life multi-day investigation. Join a team of expert citizens as they tackle the challenges and uncertainties they face while they help major intelligence agencies like Europol and the FBI to combat cybercrime.

Discover the compelling story of Bellingcat and its founder, who reveals how he identified a protester involved in criminal activity using just a single photo.

Ever heard of BlockInt? No? Perfect, two experts will guide us through the intricacies of this fascinating field.

We are also introducing a new section in the magazine: 'The Experts' Hub,' dedicated to technical and in-depth topics. For its debut, we will decode and explore weak signal detection.

And let's not forget our exciting interviews! They will always be a core part of the magazine.

Enjoy your reading, and most importantly, welcome to the world of digital Sherlocks!

Arnaud Leroy

We are excited to launch our Solidarity Sponsorship Campaign !

The idea ? You want your logo featured in the magazine or wish to showcase a project through a publication ? Let's make it happen! Just make a donation to one of the charities selected by the Cyber-IT Ethics Committee, and that's it !

It is a win-win project as your support makes a real difference for those in need!
(For more information, please visit the Cyber-IT LinkedIn page or contact us by email at: cyberit.magazine@gmail.com)

In partnership with CyberVeille

SOMMAIRE

SPECIAL FEATURE

Digital Investigation

Into the universe of digital Sherlocks

Digital Investigation, also known as Cyber Forensics or more broadly Digital Forensics, has become an essential pillar of modern cybersecurity. In an era where cyberattacks are on the rise and digital data is omnipresent, the ability to analyze and interpret digital evidence is crucial for protecting information systems and ensuring justice.

Digital investigators are the detectives dedicated to the virtual world, using sophisticated tools to track down cybercriminals, reconstruct events, and preserve the integrity of evidence.

In a constantly evolving threat landscape, digital investigation goes beyond simple data recovery. It encompasses a series of complex processes, from the collection and preservation of evidence to its meticulous analysis and presentation in court. Professionals in this field must not only possess advanced technical skills but also have an in-depth knowledge of current legal and regulatory frameworks.

Various specific tools are used in digital investigation. Software such as EnCase and FTK provide detailed analysis of computer systems, while tools like Wireshark are essential for network traffic analysis. These technologies make it possible for investigators to uncover hidden clues within vast amounts of data, reconstruct communications, and trace the actions of cybercriminals.

However, digital forensics also presents significant challenges. The volume of data to process can be immense, and investigators must exercise discernment to distinguish relevant information from distractions. Besides, they must constantly stay up-to-date with new techniques and technological advancements to remain effective against increasingly sophisticated adversaries.

Digital forensics is a dynamic and ever-evolving discipline, essential for the protection of digital infrastructures and the fight against cybercrime.
The future of cybersecurity largely depends on the ability of digital investigators to thwart cyber threats and ensure the safety of our data.

Digital forensics is not limited to cybercrime cases. Digital data is omnipresent in our daily lives and can serve as evidence in various legal investigations. Investigators can analyze phone communications, online messaging, social media activities, emails, internet browsing history, as well as multimedia and office files. Every digital element can provide valuable clues to establish the facts and identify offenders.

We are about to enter a complex yet incredibly captivating world.
Stephanie Ladel, and her partner StarMD (who wishes to remain anonymous), will revisit an investigation in which they played a key role.

They demonstrate that significant results can be achieved from nearly nothing.

They are not the only ones doing this meticulous work, organizations like the NGO Bellingcat, as well as investigators from OFAC, and various law enforcement agencies like the FBI and Europol, are also engaged in similar efforts.

Welcome to the world of digital Sherlocks !

Focus on Stephanie Ladel & StarMD from OSINT-FR

I am both an investigator and an analyst, and my tools of choice are anything that can be found and exploited, in other words, any source available to those who pay attention and know how to make use of it. In short, I conduct research in OSINT generally, and in GEOINT specifically, meaning OSINT applied to the geospatial domain.
Since early 2023, I have had the pleasure of contributing to Bellingcat's work, regularly.
I also co-host a French-speaking volunteer community within the OSINT-FR server which works to identify and locate specific objects present in pedocriminal crime scenes that have not been geolocated yet, for the benefit of Europol, the Federal Bureau of Investigation (FBI), and the Australian Federal Police.
I come from a background in the humanities and social sciences, and my interest in problem solving and informed decision-making led me to develop skills in these disciplines.
Initially self-taught, I made significant progress thanks to my peers, by studying their tutorials and analyses, getting familiar with the tools they use, tackling challenges known as “CTF”
(Capture the Flag), and participating in theoretical and practical training sessions.

My assignments vary: it could be short missions, such as pinpointing the location of an extremist group’s gathering on a specific date, to medium-term tasks like gathering information across social media platforms, websites, and news articles related to human trafficking.
I can also take on long-term projects, it could be to document civilian damage in Ukraine following Russia’s 2022 invasion, to support the recognition of potential war crimes in court.
Each day, I navigate different domains and work on projects at various stages, each requiring its own set of methods. However, one thing remains consistent: I always start by reviewing the information sources I want to monitor daily. My meal times often change as I get absorbed in research or finalizing a report, and I always end the day with an equally long to-do list for the next day.

I enjoy the challenge of engaging my mind when facing potential pitfalls. I love searching, even for a long time, and, of course, I love finding answers. But I also appreciate being constantly reminded that caution and doubt are crucial when it comes to making sense of what is found, and what is not. The less pleasant side of the job is undoubtedly the type of material we encounter. Many colleagues have been deeply affected by the horrors they have had to analyze, so it is important to remain vigilant, both individually and collectively, about this aspect of the job.

Stephanie Ladel

In our group, I go by the pseudonym StarMD. I contribute to several researches and I am specializing in technical analysis and image editing.

I have a background that blends both science and art. I attended art school and later trained in graphic processing software to diversify and automate my work.
I am passionate about both creative expression and technical precision.
I do both personal projects and commissions. I work with the press and publishing houses, helping them, for instance, to prepare digital files for printing to achieve the desired results.

I do not have a typical workday since I am a freelancer, and I work based on my motivation. I might work one hour a day or up to fifteen hours. However, I almost never take weekends or vacations.
Over the years, I’ve managed to achieve near-total freedom of choice. I can afford to turn down jobs that I do not like, and I almost exclusively take on projects I am passionate about, whenever I feel like it. The downside is financial instability, and I rarely know my schedule more than three months in advance.

OSINT is an endless well of possibilities, where all skills are valuable. You learn a lot through practice, not just technical skills, but also about the world. It is a window into what is currently happening globally.

StarMD

Co-author of “35 days of investigation to decode 2,500 pixels.”

35 days of investigation to decode 2,500 pixels

For several years, the OSINT-FR community has established a research platform in response to Europol's initiative, “Stop Child Abuse - Trace an Object”, which has gradually expanded to include the same initiative from the Australian Federal Police and the FBI's Endangered Children Alert Program (ECAP).

When all other leads have been exhausted, images of objects are revealed to the public by these authorities, each serving as the final clue that could uncover the location of a scene discovered on a pedocriminal's computer or on the internet.

Every day, these volunteer OSINT analysts meet and exchange information in a dedicated category on the Discord server (https://discord.com/invite/dWY-9sWFKYD), which includes a channel for each object being searched.

Once a week, they get together on a vocal channel so they can share their hypotheses, best leads, and progress.
This platform is organized around four co-hosts, along with a written guideline explaining what you need to know before joining them, and numerous volunteers contributing their efforts to the cause.

“We searched together. We found it. So proud of what we achieve in a diverse, respectful, and motivated community!”

Stephanie Ladel
(Investigator of OSINT-FR)

STOP CHILD ABUSE
TRACE an OBJECT

25th July 2023

26th July 27th July 4th August 7th August 18thAugust 24th August 25th August 27th August 28th August 28th October

We discover the image of our new target object on the latest update of the Europol website, on its Stop Child Abuse page (https://www.europol.europa.eu/stopchildabuse). Every single time, the same instincts kick in.

A general glance at the picture, take note of the initial leads, and we open the investigations on our Discord server because the ideas are already flowing, and they need to be organized.

For the sake of victims' protection, Europol removes any details that would allow an individual to be identified, providing only heavily cropped images. All that remains is a fragment of an object, a detail of the setting, the kind of elements that could, in the best-case scenario, help to locate a scene and unblock a pending investigation.

"**School uniform**": this is how Europol describes it, so that will be the name of our investigation among the others that we are currently opening.

Here: we can see white shirt sleeves, the top of a bright blue tie with two white stripes, and a navy-blue vest featuring a crest, likely the emblem of a school according to Europol's description. This institution exists somewhere in the world, and our goal is to find it based on this single image. The resolution of the compressed image is low, barely fifty pixels on each side for the logo, but we will have to work with it.

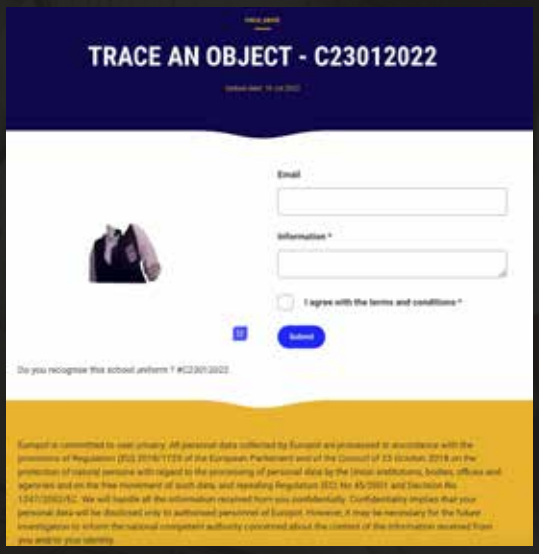


Photo of the uniform provided by Europol
(https://www.europol.europa.eu/cms/sites/default/files/images/C23012022.png)

25th July

26th July 2023

27th July 4th August 7th August 18thAugust 24th August 25th August 27th August 28th August 28th October

Leads have been pouring in since yesterday. The arrival of a new series of objects to identify is generating a lot of activity in our online community. We need to gradually lay out our theories, isolate misleading paths, while ensuring we do not overlook our target. For now, everything is possible, and it must be said that in this kind of research, we never completely close the doors...

We always start by improving the image quality as much as possible. Color correction, straightening, and enlarging areas of interest, we must make it readable without losing or adding any information. We also express our interpretations, define what we see, and try to find common ground for analysis.

On the crest, we initially believe we see an airplane, the nib of a pen, and then a book topped with a torch, the symbol of knowledge.

Two letters are also visible but difficult to discern: I K? J K?

We search for potential meanings. The rest seems too blurry to form a solid hypothesis.

Regarding the uniform, the tie appears to be particularly significant. These two white stripes are quite uncommon, especially worn so high. We quickly find similar models in Indonesia and India, worn by students and showcased on manufacturer and seller's websites.
Interestingly, there is a region in India called Jammu and Kashmir. Jammu and Kashmir - J and K.
We have our first lead.

We decide to focus our initial research on this geographical area.

27th july 2023

Research around the Jammu and Kashmir region continues, but so far, it has not yielded any convincing results. Aside from the long sleeves of the white shirt, which fit a mountainous climate, and the flame and open book symbol, nothing really aligns with our interpretations.

Moreover, this symbol is found in numerous countries, primarily in Asia and the Middle East.

In parallel, we are developing visual prototypes that we submit to reverse image search engines. This technique complements textual research well, but it is quite time-consuming.

Creating a prototype takes time, and we need a version for each hypothesis. With a torch, a pen nib, different combinations of letters... We cannot be sure of anything

One of our members points out that the shape of the crest does not match those typically found in schools in India. However, despite our efforts to capture every useful detail, the message is read and then lost in the flow that characterizes the initial days of the investigation.

Was it too soon to make a judgment?

Unknowingly, we overlook a crucial piece of information.

« Here is the silhouette of the crest as we understand it »

Stephanie Ladel
(Investigator of OSINT-FR)

4th August 2023

The initial leads around India are still not leading to any results. We are multiplying prototypes and conducting textual searches. Then, we decide to broaden our area of investigation.

The lead in Indonesia also seemed promising, but we lack tangible evidence to confirm this intuition. We choose to scan all of Asia.

Alongside this school uniform, we are trying to identify about ten other objects that often require the same level of attention. However, this expansion to the entire Asian region demands a lot of our energy, which will not be allocated to the other ongoing investigations.

25th July 26th July 27th July 4thAugust

7th August 2023

18thAugust 24th August 25th August 27th August 28th August 28th October

We find similar uniforms in many Asian countries. However, while the clothing style matches, the exact tie pattern still eludes us.

Hong Kong, the Philippines, Thailand, and Singapore are added to our list of priority countries and territories. We are only a small group, and the number of areas to investigate is becoming increasingly difficult to manage.

Hong Kong ?
The Philippines ?
Thaïlande ?
Singapour ?

25th July 26th July 27th July 4thAugust 7thAugust

18th August 2023

24th August 25th August 27th August 28th August 28th October

Close-up on the tie from the uniform provided by Europol

Our searches focusing on the uniform, tie, and logo are leading nowhere. We have reviewed thousands, sometimes beyond Asia, but without any significant results. Several times, we have pursued leads that seemed to bring us closer to our target uniform, but their study led nowhere.

We continue to focus our efforts on the tie design, looking for the countries using it and its manufacturers. For now, this is the tangible element anchoring our investigation.

25th July 26th July 27th July 4thAugust 7thAugust 18thAugust

24th August 2023

25th August 27th August 28th August 28th October

Our leads seem to be running dry.

We are reaching the point where we feel we have exhausted the research linked to our hypotheses.

Where should we focus our skills and efforts? After examining thousands of logos, uniforms, and school websites, sometimes guided by intuition, with much methodical rigor sometimes, most of us have moved on to other investigations that we also hope to complete.

However, we remain vigilant. We know our ongoing investigations well. We know every detail of these blurry and fragmented images. And sometimes, brilliant insights emerge when we least expect them

« As we all know, there are really only two reasons to stop an investigation: either seeing that the image has been removed from the website by the authorities, meaning that further research is no longer needed or expected, or finding the object »

25th August 2023

Faced with the slowing pace of the investigation, a group member decides to take a look at the problem from another angle.

We collectively sense that this object can be found, but we are obviously not searching in the right places.

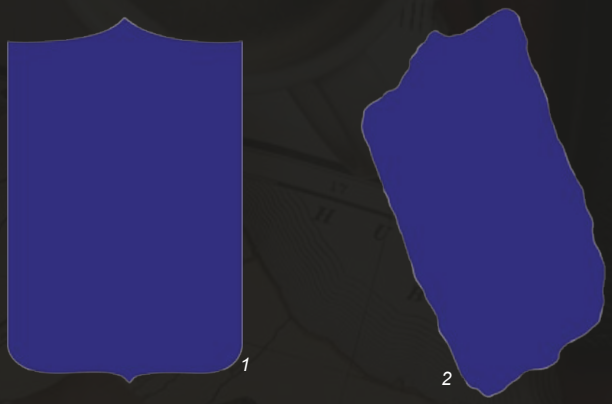
With all the information we have collected, we are beginning to create a map of school crests from Asia and other places in the world. The shapes, colors, and letters, all these details are influenced by local trends and customs.

Two questions are raised, focusing on the most specific characteristics of our target object:

- The shape of the crest does not adhere to the usual heraldry standards. Have we ever seen such a shape before ?

- Two letters are positioned on either side of the crest. Have we ever seen these letters laid out this way ?

At this stage, it is safe to say that we have not found these two elements in any Asian country. We regroup and restart our research based solely on these two criteria, focusing on the rest of the world.



1 Shape of the crest as we understand it
2 Shape of the crest in the initial image

27th August 2023

We have prototyped the crest, and we have a clear representation of its silhouette. Therefore, by searching country by country and asking search engines to show at least a hundred school badges or uniforms, we get an idea of the possibility to find the one that we are interested in.

We find this particular shape in a South American country, far from Asia, where we conducted most of our research...
Then, in the same country, we also find the arrangement of the letters. Once, then twice, then three times.

Finally, we discover the famous symbol of the torch, the one we supposedly most likely noticed on the first day.

In a single day, we find around ten logos associated with this country that fit our criteria. However, they still do not resemble our target crest, which is different in composition and colors.

This is probably why they did not come up in our image searches.

At this stage, nothing is certain yet, but these findings are very encouraging. We are doubling our efforts.

28th August 2023

It is not even 7.00am yet when a group member posts a new series of logos in our discussion channel. He likely chose to wake up earlier that morning to have time for some research before his commitments caught up with him.

The latest results revived the momentum of this investigation, there is a new energy in the group as we want to believe in a positive outcome for this search. Among these results is a crest painted on the facade of a building. The early risers and those available join the Discord channel, and this mural is seen as a close match but the search continues without it attracting enough attention. Yet our target crest is right there, before our eyes, in our own channel discussion.

Four hours later, new comers help us to identify what we were missing so far. The image arrived so quickly after this last methodological change that we are still in doubt. Is this really the right crest?

Have we really found it?

You must be thinking: "How can we pretend to have a clear vision of what we are looking for and pass right by it without even recognizing it?" Well, let us explain. We quickly realized a notable difference in this country between emblems displayed on a building wall or on their own (like a logo displayed as a Facebook page avatar, for example) and emblems worn on uniforms.

Their shapes differed, as did their length-to-width ratios. We had expressed this, and tried to train our eyes to switch from one to the other, but we were just beginning…

Let's go back to our crest painted on the wall. Everything seems to match: general shapes, colors, letters. It's all there. After just over a month of daily research, we have just identified this emblem, only 50 pixels wide, directly pointing to a middle school in a town of 25,000 inhabitants, in a country we know very little about.

But our efforts do not end with this discovery. We are not playing a 'Capture the Flag' game! We now need to verify and consolidate our findings, archive the sources which will allow law enforcement to get to the same conclusions, and make a comprehensive report to make sure the authorities will pay attention.

First, we should exhaust all possibilities for error. We check that it is indeed the same school badge by examining all its variants.

The school uniform, quickly found, is also scrutinized and compared point by point. Types of clothing, colors, everything is checked. We also try to understand why the two-stripes tie is not worn by all the students. We want to provide the maximum amount of useful information in our report.

After an intense 10 hours archiving session, writing, multiple proofreading and corrections, we finally submit the report via Europol's public form.
We are happy. Rarely does an object present at a pedocriminal scene, the last clue to be exploited, lead so precisely to the victim's location.

visuel conclusif

1 Shape of the crest as we understand it
2 Shape of the crest from the original image
3 Shape of the crest we found

28th october 2023

It's been three months since we contributed to this investigation. We hope that Europol has already taken note of our report, verified it, confirmed it, contacted local authorities, and facilitated major progress in this case...
But this time, unlike usual, we concluded our investigation with knowledge of the school attended by the victim. One of us set up an automated information watch for this school. And today, they returned to the Discord channel with news that feels like a thunderclap.

A local news article mentions this institution and an adult associated with it, implicated in a sexual misconduct case involving at least one underage victim.

We unanimously decide to send a quick notice to Europol to inform them. And now you know the drill... Archiving, drafting, multiple proofreading and corrections.

We submit this brief report the same day, and it will be our last connection with Europol concerning the 2500 pixels from this picture.

SPECIAL FEATURE

bellingcat

Key figures about bellingcat

* Eliot Higgins leads Bellingcat
* Bellingcat was founded in 2014
* 27 full-time employees and several contributors
* Over 780,000 followers on X
* 74,000 followers on LinkedIn
* OSINT workshops available to train hundreds of professionals and citizens to Bellingcat's methods
* 35 awards and recognitions since 2015, including the Nijmegen Peace Medal for contributions to peace and human rights

« When I was younger, I was almost pathologically shy to the point that I did not dare leave my house. I was a true geek, passionate about computers and video games. Like many people who are introverted, I spent hours on the computer.

When I am passionate about something, it is all I can think about! I have always been like that. When I was growing up, I was drawn to counterculture, I began to look into the impact of U.S. foreign policy around the world.

With the growing success of social media in 2007 and the arrival of smartphones, we gained access to technologies which allowed us to take photos and share them instantly with the entire world. It was absolutely revolutionary »

Eliot Higgins

Remarks from the documentary
Bellingcat: Truth in a Post-Truth World
(With bellingcat's permission)

Bellingcat is an independent international group of researchers, investigators, and citizen journalists using both open-source investigations and social media to explore a variety of topics, including Mexican drug traffickers, crimes against humanity, tracking the use of chemical weapons, and conflicts worldwide. With staff and contributors across 20 countries around the world, they operate in a unique field where cutting-edge technology, forensic research, journalism, investigations, transparency, and accountability converge.

Here is an example of how Eliot Higgins identified a suspect from the far-right activists rally in Charlottesville, Virginia, via Bellingcat (remarks transcribed with the permission of Bellingcat, from the report entitled "Bellingcat: Les combattants de la liberté" broadcasted on Franco-German channel Arte)

« We have this photo (photo 1) of a man attacking another individual, so we tried to identify who he was. We study photos and videos of white supremacists, we came across this guy (photo 2), several photos show similarities, like his shirt, for example.»

Photo 1

Photo 2

We examined other photos and came across several that appear to show the same person (photo 3). When we compare the photos, we can see that the moles on his neck are exactly the same (photo 4).

Next, we looked into the people around him (photo 5), some of them appear and are named on a Twitter account called "Yes, You're Racist," which provides links to their social media accounts (photo 6).

Photo 3

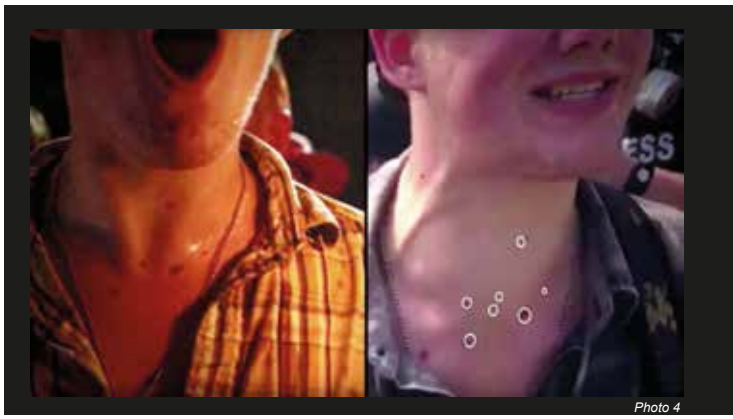


Photo 4

Photo 5

Photo 5

We reviewed their profiles and their followers' and came across the same guy again (photo 7).

On his page, we found more photos, and once again, there were matches, it is clear that the the moles on his neck are identical (photo 8).

It really seems to be him involved in this incident, and we are working to identify the individuals behind this crime. This type of work is increasingly attracting the attention of law enforcement.

Photo 7

Photo 8

BELLINGCAT

The name "Bellingcat" comes from the English idiom "belling the cat," based on a fable in which a group of mice agree that the best way to protect themselves from the approaching cat is to place a bell around its neck to warn of its approach in the future. However, they ultimately fail as no mice volunteered to do the job.

Do you know BlockInt ?

BLOCKINT : When OSINT meets the Blockchain

-
Jonathan Riss
Jonathan Spedale

BlockINT (Blockchain Intelligence) is a field that combines OSINT technique with the analysis of transactions and data on blockchains in order to extract valuable information.

Open Source Intelligence (OSINT) involves collecting information from accessible sources.
In the meantime, blockchain is a decentralized and fully transparent technology that has revolutionized various sectors (finance, supply chain, etc.) by providing an immutable ledger of transactions.

The combination of these two domains has naturally led to a new area of investigation: BlockINT. It leverages OSINT techniques and methods to analyze available blockchain data, offering new perspectives for research, security, and transactional compliance.

What is the Blockchain ?

The Blockchain technology enables data to be stored in a totally decentralized way. Unlike centralized systems where a single authority controls the data, the blockchain operates on a distributed model. This decentralization eliminates the need for intermediaries, thereby reducing costs and increasing transaction speeds. Each transaction is recorded in a block, which is then linked to previous blocks, forming an unalterable chain.

The different types of Blockchain

Public blockchains : accessible to everyone (e.g. Bitcoin)

Private blockchains : for specific users only (Hyperledger)

Hybrid blockchains : which combine elements from the two categories mentioned above

Blockchain main characteristics

Decentralization : No single party controls the entire network.

Immutability : The data is unalterable after it has been recorded.

Consensus : System ensuring participants consent on the transaction's validity

Future prospects for BlockINT

BlockINT is a rapidly growing field, with many technological advancements on the horizon. Progress in artificial intelligence and machine learning promises to enhance on-chain analytical capabilities. This area could play a crucial role in various sectors, like finance, cybersecurity, and more. Career opportunities in this field are increasing, offering interesting prospects for researchers and security professionals.

The rise of privacy solutions such as Zero-Knowledge Proofs (ZKP) and confidential blockchains (Monero or Zcash) presents new challenges for industry specialists.

Image - blockchain example

OSINT & Blockchain: Concepts and Convergence

OSINT is based on the extraction of information from open sources: social media, forums, public databases, and all other freely accessible resources on the internet.
When applied to blockchain, it involves the collection and analysis of data publicly available on networks.

This way, it is possible to gain a detailed view of the movement of funds, wallet addresses, connections between different entities, and even messages (photo 1).

By using clustering techniques and specific analyses, specialists can detect unusual financial flows between different blockchains or identify addresses acting as "mixers" to anonymize transactions.

However, this does not come without its share of difficulties. The pseudonymity of wallet addresses makes user identification very challenging. Additionally, the increasing volume of data and the growing complexity of transactions require advanced techniques and powerful tools to be effectively exploited.

Photo 1

Etherscan.io

Metasleuth.io

Sentio.xyz

Techniques & tools

BlockINT uses various tools and techniques to extract relevant information. These include “clustering,” which allows you to group addresses belonging to the same user to track transaction flows. This is particularly useful when attempting to track transactions associated with illicit activities (scams, ransomware, etc.).

“**Bridge tracing**” is the art of tracing funds transiting between two different blockchains. Transferring assets between multiple networks is a process often used to try to cover the tracks and make the funds more difficult to trace. This tracing technique is complex, requiring expertise in interoperability and a deep understanding of the protocols specific to each blockchain.

Block explorers’ tools such as Etherscan.io or btcscan.org are popular and free tools that allow for the analysis of on-chain data. These platforms enable users to visualize and examine transactions in real-time.

Other platforms like metasleuth.io or arkhamintelligence.com offer the ability to monitor wallets, detect anomalies, and prevent suspicious activities.

Even more specialized solutions, such as Phalcon or Sentio.xyz, go further by allowing users to visualize smart contracts, simulate, and test their various functions, thereby providing an even more granular level of analysis.

Applications

BlockINT finds applications in various fields. In terms of security and compliance, it helps financial institutions adhere to **KYC** (Know Your Customer) and **AML** (Anti-Money Laundering) regulations. It assists in monitoring suspicious transactions, identifying money laundering patterns, and preventing fraud.
Law enforcement agencies use it to conduct criminal and financial investigations by tracking transactions related to illegal activities. For example, in the well-known Silk Road case, investigators were able to trace Bitcoin transactions to identify and arrest the founder of the website.

In academic research, it allows the study of economic behaviors and market dynamics. Researchers can analyze investment patterns across different wallet addresses.

Finally, in supply chain, it ensures product traceability and enhances transparency. This is particularly important for industries where counterfeiting and fraud are major issues, such as the pharmaceutical or food sectors.

By tracking each step of the process through the blockchain, companies can guarantee the authenticity and quality of the products they ship.

Digital investigation techniques

Phones, hard drives, GPS devices, credit cards... All these devices reveal information about their users. Digital forensics has become an essential pillar in criminal investigations, requiring the creation of an organized task-force network of investigators and skilled technicians. Here are a few examples.

Phone Tapping

IMSI-catcher (International Mobile Subscriber Identity) An IMSI-catcher is a device that mimics a cell tower and forces mobile phones within a given area to connect to it. Once connected, it can intercept calls, SMS messages, and sometimes even track the location of a phone. This technology enables the identification of the device or the person using the network.

Legal Wiretapping With judicial authorization, law enforcement agencies can request telephone operators to intercept specific communications. This process involves collaborating with service providers to capture metadata (time, duration, location) as well as the content of the communications.

Wiretapping on Instant Messaging Services With the rise of encrypted messaging apps (such as WhatsApp, Signal), more advanced techniques are often required, such as monitoring communications at the device level (hacking the phone to access messages before or after encryption).

Network Surveillance

Packet Sniffing This is a method of intercepting data on a network by capturing and analyzing data packets. Tools like Wireshark allow for monitoring and intercepting network traffic over a specific period, making it easier to reconstruct communications.

Man-in-the-middle (MITM) In an MITM attack, the attacker positions themselves between two communicating entities (e.g., a client and a server), often without their knowledge, to intercept or alter the exchanged communications. This technique can be used to read supposedly encrypted data if the encryption is poorly implemented.

Router or Server Intrusion It is also possible to take control of network devices, such as routers or DNS servers, to capture traffic.

Forensic Analysis

Disk Imaging One of the initial steps is to clone hard drives, SSDs, or memory from suspect devices for examination in a controlled environment. This preserves an exact bit-by-bit copy of the data without altering the originals. Common tools used include FTK Imager and EnCase.

File System Analysis Once the disk image is captured, the next step involves analyzing files, metadata (e.g. creation/modification dates), operating systems, and logs to understand the user's activities. Software like Autopsy or X-Ways Forensics is commonly used.

Data Recovery In some cases, deleted data is not fully erased from the disk. Advanced recovery techniques can often retrieve this information.

Browser Artifact Analysis By examining cache files, history, and browser cookies, investigators can trace a suspect's online activity, such as their internet searches and websites visited.

RAM (Random Access Memory) Analysis RAM contains temporary and volatile information that can be crucial, including encryption keys, active files, or malicious processes. RAM analysis can be performed with tools like Volatility or Rekall.

Digital Tracing and Geolocation

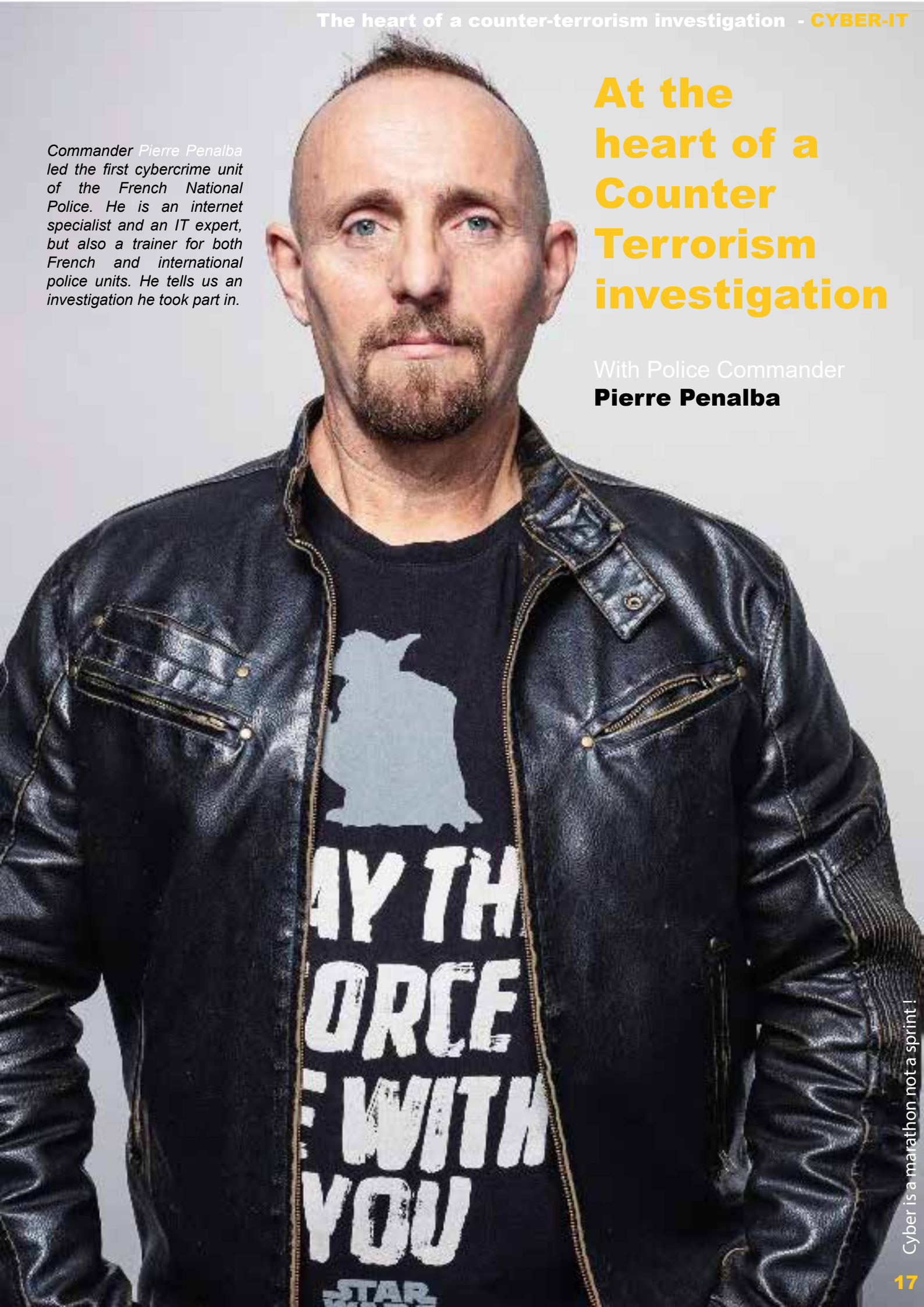
IP Address and Geographical Tracing Identifying the IP address used by a suspect can provide geographic information or at least trace their ISP (Internet Service Provider). Collaboration with the ISP can often lead to identifying the user behind the IP address via connection logs.

GPS Tracking Geolocation via GPS services embedded in phones or laptops can provide precise information about a suspect's movements. Many malware programs are also designed to collect and transmit such location data remotely.

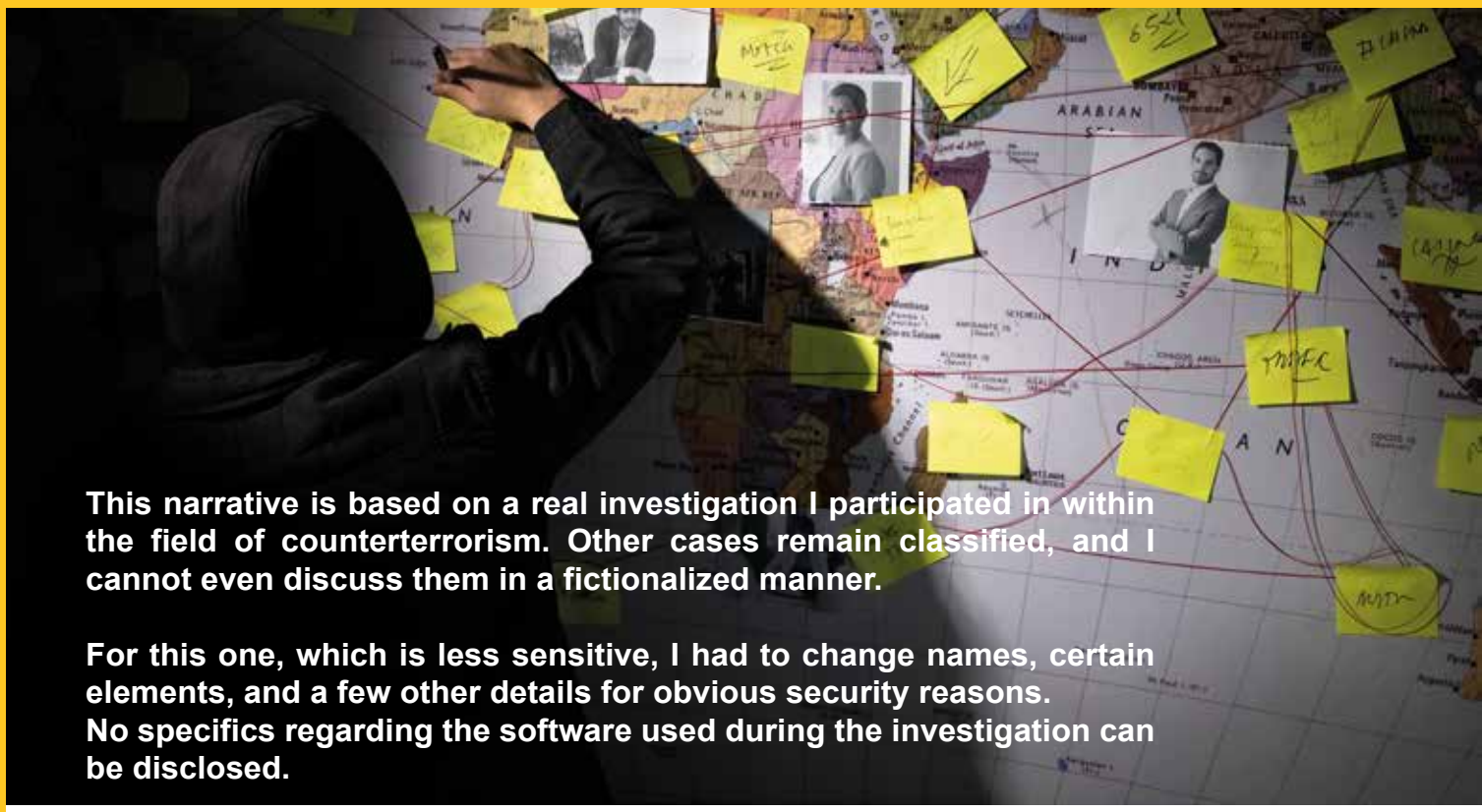
At the heart of a Counter Terrorism investigation

With Police Commander
Pierre Penalba

Commander Pierre Penalba led the first cybercrime unit of the French National Police. He is an internet specialist and an IT expert, but also a trainer for both French and international police units. He tells us an investigation he took part in.



AT HEART...



This narrative is based on a real investigation I participated in within the field of counterterrorism. Other cases remain classified, and I cannot even discuss them in a fictionalized manner.

For this one, which is less sensitive, I had to change names, certain elements, and a few other details for obvious security reasons.
No specifics regarding the software used during the investigation can be disclosed.

2022

A ***note blanche**** has just been received by our unit.

(It is a serious piece of information verified by a government service, but it cannot be referenced as the official "source", it is neither cited nor mentioned in the note.)

The document informs us that a terrorist act is being planned within our jurisdiction.

There aren't many additional details, just a few screenshots of conversations on an encrypted messaging app and a profile communicating with a jihadist originally from our region who had left to fight in Syria.

I suppose that you would like to know how and who obtained this information...
So would I…
The only thing I'm certain of at this moment is that it's credible.

Now, an encrypted messaging app also means there is no possibility of legal identification...
Speaking of which, yes, it is secure in a way, but not really, if you know where to look...

We got one clue: an identity, the young jihadist's who had left France. I will call him Akmad.

The exchanges, primarily in French, suggested that Akmad and his contact were likely close

So began a painstaking effort, using all the OSINT techniques to try to reconstruct Akmad's life and contacts. It was a crazy amount of work. It took us dozens of hours to analyze his social media activity (professional and other sources) over the last few years.

Given the sensitivity of the case, we did not limit ourselves to cyberspace, we also went out to physically monitor relatives and friends, conducting discreet neighborhood inquiries and gathering intelligence, etc. As I mentioned earlier, everyone tends to make progress, especially those with plans for terrorist attacks, believe me. They do not connect from home using their computers or phones, no, they know better.

They use disposable phones on public Wi-Fi networks, change regularly, and trust no one. Sometimes they use bootable, encrypted drives to run VMs with VPNs. In short, they take precautions.

In this case, we had a significant advantage: the closeness of the two young men before Akmad's departure. Our list of suspects quickly narrowed down to a few names. Of course, we put them under surveillance for phone and data monitoring.

We had two Wi-Fi networks to monitor and three phones. We had "gained" access to both Wi-Fi networks (those who say they "hack" Wi-Fi networks… well, never mind…)

***Note blanche** : a brief, typically one-page note, unsigned, usually originating from an intelligence service and written for high-ranking government or administrative officials in France.

OF THE INVESTIGATION...

Image of illustration

The technologies and software allowed us to capture all the traffic, but encryption was a real problem. However, when you know that someone is using an encrypted messaging service, it's easier to monitor the flows and determine if someone is using it...

We do not know what is inside, but we can see the encrypted data passing through. The suspects had intense data activity, but almost nothing with encryption, and even less on the messaging service that interested us.

By chance, one evening, someone connected to the messaging service on one of the monitored Wi-Fi networks. We immediately retrieved the "MAC addresses" of the devices connected to the router, and to our surprise, it was an unknown phone!

Just for your information, a MAC address is extremely useful, we can often trace a lot of elements related to the manufacturer. Oh, yes, we also had physical surveillance that allowed us to cross-check this information and identify a new suspect. The next step was to find his phone.

I used roaming techniques and the 3G/4G antennas in the area to find occurrences that helped to identify the phone number linked to our new suspect's movements.

This took us hours, not just two minutes like we see in TV shows...

It was a disposable number, but nothing prevented us from listening in and monitoring it.

Finally, we were able to put a name to the profile of the wannabe terrorist: Samir.

He was not a childhood friend, but rather an acquaintance who was part of a group led by an ultra-radical preacher who had trained them. They had converted at the same time, which brought them closer, turning them into "brothers."

With his precise location, a specialized police unit set up listening and surveillance devices.

I am not allowed to reveal too much, but basically, we were capturing his data traffic in real time, his conversations, of course, but there was also physical surveillance. I felt like I was constantly looking over his shoulder.

The conversations between the two men were completely mind-blowing, discussing the best ways to cause the most deaths, and techniques to escape from the "kuffars" (non-believers).

We had to document the project in detail, but the most stressful part was that we had to let him start his attack's preparations before we could arrest him, otherwise, legally, it would only remain a project, something virtual, and that is not the same as having actual proofs of the project's preparation or the beginning of its execution...

We also wanted to identify any possible accomplices.
"Fortunately" for us, preparing explosives is not a simple task, especially when trying to hide it from those around you.

Samir had his own premises but was still living with his family, the "kuffars," in his eyes...
He began to acquire the basic components, all while being encouraged and guided by Akmad.
But everything spiraled out of control one evening when Akmad announced to Samir that he was finally going to become a martyr!
He had just learned that the next day he would be driving a car bomb into the midst of a base of infidels!

One of them exclaimed with joy that he was going to commit suicide the next day while killing as many people as possible, and the other replied, "You are so lucky!".

Samir then complained about not being ready, saying that he, too, wanted to go out as a martyr!
Excited, Akmad then explained to Samir that all he needed was a knife to kill plenty of infidels, he just had to go out and cause as many deaths as possible !

Samir began to articulate his murderous project out loud, explaining that he would start with his family, those so-called kuffars, encouraged by an almost hysterical Akmad who assured him that this was a way to save them since he could then take them all out of hell (???)

Honestly, witnessing a scene like this, I briefly thought I was having a nightmare.

There was no time to hesitate.

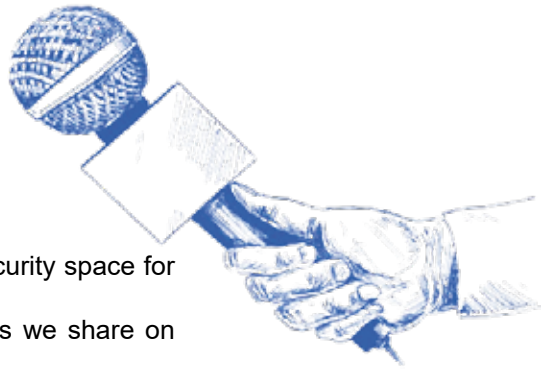
Everyone was ready to go and arrest Samir.
As for Akmad, an urgent white note was sent back to inform about the imminent attack somewhere out there.

Samir was arrested while he was carefully sharpening a gigantic butcher's knife, along with the elements to make his future bomb.
He is going to be sleeping in prison for a very, very long time.
Akmad has disappeared from the networks and messaging services.

This investigation, one among many others, would not have succeeded without the technical expertise, ingenuity, and dedication of the men and women who put the interests of others before their own every day, prioritizing others over their comfort and personal life. I have been proud to work with you. I want to acknowledge you today. Thank you for all that you do.

Interviews - They do cyber and IT

We know them through their daily publications but who are they really ?



As usual, Cyber-IT connected with various professionals from the IT & Cybersecurity space for our Q&A sessions. In this third edition, we present a new set of interviews.
The magazine's interviews are more in-depth compared to the shorter versions we share on LinkedIn. This is due to social media's character limits policy.

TRISTANT MANZANO
CEO of Security Data Network

Hi Tristan, how are you? Can you tell us a bit about yourself ?

"Hello Arnaud, thank you very much !

I am Tristan Manzano, CEO of Security Data Network and a cybersecurity consultant."

What was your career path ?

"I started in IT at the age of 11 and quickly realized that I was passionate about it, so I spent entire days on the computer.

I completed a high school diploma specialized in Network & Systems at 20, then continued with a BTS (Advanced Technician's Certificate) in "Computer Networks and Telecommunications," followed by a Bachelor's degree (bac+4) in "Systems and Network Engineering Management." Then I started my own company and began to complete certifications."

What are your day-to-day tasks ?

"My tasks include: managing the company, run penetration tests, red teaming, performing security audits, and providing training at engineering schools."

What does a typical day look like for you ?

"I usually start with technology watch, reading my emails and other messages, then I begin or follow-up on ongoing projects. By the end of the day, I get prepared for the next day."

What do you like/dislike about your job ?

"IT in general !

I truly enjoy all of it, from systems and networks to programming. Cybersecurity is really the next step because it allows me to grasp and enjoy all aspects of IT."

One last word ?

"Happy Hacking ! 😁"

SDN SECURITY DATA NETWORK

NATHALIE GRANIER
Researcher in cyber threat intelligence and human behavior

Hello Nathalie, can you tell us a bit about yourself ?

"A girl from the southwest of France, more specifically from “Ovalie” (i.e. French rugby region!) 😉 an epicurean, a psychologist for a few decades, working in cybersecurity for the past 8 years."

What is your background ?

"I have worked as a psychologist in various organizations. I am a psychologist, specialized in social and cognitive science.
I got a Master’s degree in psychology, which I supplemented with various specialized training programs. I also have a diploma in Human Resources and a Master’s degree in consulting.

Therefore, I have held positions in HR, as a consultant, or as a psychologist, and in Cybersecurity: my various positions covered delivery, consulting, cyber content, crisis management, and Threat Intelligence analysis. "

And what are your responsibilities ?

"I do :
Consulting :
- Cyber expertise insights
- Market technology and economic monitoring
- I attend and participate in trade shows and conferences
- Manage technical studies and analysis of competition management and organization
- Consulting services
- Technical solutions implementation

I work in cybersecurity, in CTI (Cyber Threat Intelligence), I am responsible for the CTI framework.

- I analyze threats specifically targeting clients’ environments
- Open sources data collection and analysis for third parties and cyber stakeholders
- Threat investigations: clients support and assistance
- Provide technical reference to clients
- Continuous service improvement."

What does a typical day look like for you ?

"No day is the same, and that is a good thing.

You need to be ready for the unexpected, change necessitates flexibility and curiosity. There are no fixed hours, again, this is convenient for me because I am insomniac.

My "calm" days, or even my weeks, will alternate depending on the various functions mentioned above. And when I am not doing all that, I am lucky enough to take part in conferences, webinars, round tables, and I write articles always related to cyber and psychology."

What do you really enjoy about your work ?

"The unexpected, no routines !

The necessity to be curious and learning continuously. Life in cybersecurity is a constant challenge, and I love that! Plus, I can combine it with psychology. Learning to decode human behavior behind a screen, understanding why we do this, and how a screen can disrupt the rules."

A final word ?

"If you are curious, flexible, eager to learn, and to share: Go for it, this job is for you!
" One must be enthusiastic about their profession to excel in it." Denis Diderot* … while always keeping your humility, I would add…

*(*Denis Diderot is a French writer and philosopher from the 1700’s)*"

ANOZR WAY
PEOPLE-CENTRIC CYBER PROTECTION

DR GUILLAUME CELOSIA
Industrial Chief Information Security Officer

In a nutshell, who are you ?

"Hello! I'm an Industrial CISO (by day) and cybersecurity enthusiast (by day and night)."

What about your background ?

"A rather "classic" educational path at first (with a major in ubiquitous computing systems security) ... and then, the tragedy: passion took over! To satisfy it, there was only one solution: getting a PhD.

It's an adventure I can only recommend wholeheartedly for the countless learning possibilities it provides.

My professional experience: I started with technical skills (to understand), then moved into governance (to master the technical approach). A few communication skills were acquired after a stint in consulting. We mix it all, and there you have it !"

What are your day-to-day responsibilities ?

"Audits, governance, cyber awareness, training, IT architecture, cyber watch, security dashboard management, vendor reviews, etc. As you see, my daily work is pretty diverse... but it all leads towards a single goal: to protect my industrial perimeter from cyber-attackers !"

What does a typical day look like for you ?

"Are you sure you really want to know ?! Alright, but you might be disappointed: I wake up - eat - calls/emails - eat - emails/calls - eat - "sleep" - repeat! In the end, isn't the life of a CISO just a beautiful culinary tale ?"

What do you like/dislike about your job ?

"Let's be honest, the IT side of Cybersecurity is already quite complex... but in an industrial environment/OT (Operational technology) side, it is on another level !
It is a real paradox, but that is probably what I enjoy the most.

As for what I dislike, without a doubt: the AI-powered blockchain nonsense !"

Perfect! Thank you, any final word you would like to share ?

"OIt can't say it enough: cybersecurity is everyone's business! Thank you for this opportunity and for publishing this interview !"

STEPHANE FERRER
DPO - GDPR Compliance and Founder of RGPD-SF

Hi Stéphane, nice to meet you, tell us who you are ?

"Mutual pleasure, Arnaud! My clients think I am terribly paranoid, but others see me as someone who translates obscure and frightening (even clearly boring) concepts into simple words."

Can you tell us a bit more about your background ?

"My background is, like many others, atypical. I have a scientific profile (environmental engineering), and then the twists of life led me to shift from the 'bio' environment to Windows'.

Ultimately, I found the right balance in the DPO Role: human, IT, legal, crisis."

What are your day-to-day responsibilities ?

"I have several responsibilities, but I would say the main ones are counseling, implementation, and raising awareness.

However, the first mission I set for myself is to avoid falling into a routine, and fortunately, today that mission is accomplished."

What does a typical day look like for you ?

"Since I have also been an IT manager at ISM LES MARISTES School for 25 years, I am immediately solicited by users, both teachers and students, upon my arrival.

I take care of them and show them the risks associated with their practices. I also manage 'GDPR by Design' projects for governance. Additionally, I oversee GDPR compliance for my clients.

I rarely get bored."

What do you like/dislike about your job ?

"What I enjoy is helping people and being able to provide concrete and understandable answers to them !

What I find less enjoyable is being seen as a hindrance (not to say a nuisance). However, my vision leads me to believe that it is my responsibility to change their minds with the right arguments."

Any final word ?

"Beyond saying a final word, I prefer to mention a motto: GDPR is about securing to protect, not blindly submitting to yet another regulation."

Institution Sainte-Marie
83500 La Seyne sur mer

VALERY RIEß-MARCHIVE
EDITOR-IN-CHIEF, LeMagIT

Nice to meet you Valerie, tell us, who are you ?

"I am the editor-in-chief of MagIT and one of its co-founders. Additionally, I am also a collector of cyberattacks (including ransomware) for which I strive to maintain a comprehensive inventory as since September 2020. This includes information from claims made by cybercriminals as well as reports published in the press, worldwide. Over the past year, I have been working to make this collection more complete, precise, and transparent. This effort has allowed us to create our weekly cybersecurity newsletter and a regularly updated inventory on my GitHub feed.

For this project, I also focus on 'correcting' cybercriminals' claims' chronology to prevent them from having too much freedom of action in their marketing efforts. Lastly, I created a negotiation guideline collection that has been updated, anonymized, and standardized as a JSON file, available on ransomch.at and ransomware.live ."

Could you please explain your background ?

" I completed an initial training program in computer science at the University of Versailles Saint-Quentin-en-Yvelines (UVSQ) in France. I experienced the internet before the web and started coding during my teenage years. During my studies, I discovered the IT press as a freelance contributor, and I stayed in that field. I worked in Mac press, professional IT press, consumer IT press, and I wrote books about Apple products. Then in 2008, I co-founded LeMagIT with a group of colleagues and friends. It was around 2011 that I pivoted toward cybersecurity, initially while following market trends and product developments. In 2019, I really began to monitor the threat landscape, attentively."

Are there any things you like/dislike about your job ?

" While staying within the realm of journalism, I changed careers multiple times. I specialized in Mac, then mobile telephony, then enterprise IT, then outsourcing to India, and then cybersecurity... with some interest in threat intelligence. This versatility, while largely remaining in the same field, is significant. Some communication practices, especially in times of crisis, can be a bit alarming, but I have observed real progress over the years. And that is refreshing."

What are your day-to-day responsibilities ?

"The first of my daily missions is to allow my colleagues to work steadily. Le MagIT has a remarkable, professional, and rigorous team. It is a privilege to work with François, Philippe, Yann, Gaétan, Pascale, and our boss, David. I also want to highlight our freelance contributors; I manage some of them.

I am also here to support anyone who needs guidance or to facilitate communication with a grumpy press officer.
I also keep track of cyber incident news from around the world to contribute to the cyber weekly. I follow cyber news to find ideas for IT projects, advice, or even opinion pieces and I also write all of this. Because writing is certainly part of the job.

In my case, writing also involves coding in Python to create new tools, especially for reporting, for the monthly meteoransom bulletin, but also to evolve and maintain tools for internal use"

Do you have a typical day-to-day ?

"My typical day starts with Microsoft Teams to discuss with my colleagues about the day's edition. It also involves an RSS feed reader and deleting an impressive number of messages.
In addition to this, I manage my daily phone calls (and DMs), along with various meetings and interviews, not to mention webinars (either as an attendee or as a guest speaker).
I also spend a lot of time monitoring a few social media platforms, so I can keep an eye on certain cybersecurity researchers' work or follow-up on conversations that might spark new ideas for some articles or press coverage.
Every day, I also dedicate some time to look for ransomware samples on the main sandboxes.
With all of this, I still need to find time to write. As a result, it's not uncommon for my day to stretch out a bit…
"

Thank you, Valeri, any last word you would like to share ?

"I will repeat myself again, but I believe we do not even begin to grasp how serious and pervasive the threat is. I am convinced that there are many, many potential victims of cyberattacks who do not know they could be targeted. Some may be fortunate enough to escape it, but not all, unfortunately.
And, unfortunately, the vast majority are absolutely unprepared for it."

ETIENNE CAPGRAS
Cybersecurity Content Manager for OpenClassroom

OPENCLASSROOMS

Hello Etienne, thank you for answering my questions. So, who are you ?

"Hello Arnaud, it's a pleasure to discuss with you. I am Etienne Capgras, the head of cybersecurity training at OpenClassrooms. I joined the company three years ago."

Can you tell me a bit more about your academic background ?

"I would say I have a typical background. In 2010, I graduated from the INSA engineering school in Toulouse - France, and began my career at Wavestone, where I worked from 2010 to 2021. My initial assignments involved penetration testing and audits in various sectors, such as banking, healthcare, and transportation.
I then assisted several operators of vital importance (OIV) with their compliance with the LPM (French Military Programming Law): risk assessments, architecture, program management, and liaising with ANSSI (French Cybersecurity Agency), which gave me a significant expertise on the subject.

In parallel, I had the opportunity and responsibility to mentor about thirty consultants in their long-term career development. Ultimately, I joined OpenClassrooms at the end of 2021 to develop the training catalog in cybersecurity and IT."

What are your day-to-day responsibilities ?

"I joined OpenClassrooms to develop the cybersecurity training catalog.
I need to ensure that we train people for the right job positions (those in demand), in the right way, and with the right educators. Another aspect of my role is to promote our training programs to companies and potential candidates: it is pointless to develop relevant content if it is not utilized properly.

The skilled professionals' shortage in cybersecurity has impacted me and it is still a concern: there is an incapacity to secure IT systems properly, many professionals are burning out, we notice a rise of incompetent players on the cybersecurity job market yet these profiles are constantly in-demand because of the skills shortage. We need to act quickly!
So you could say my mission is to make cybersecurity careers accessible to everyone, for everyone's benefit :)"

What does a typical work day look like for you ?

"There aren't any! We do some market analysis to identify and characterize in-demand job positions. This involves numerous meetings with industry professionals to understand their practices, expectations, and specific needs, as well as discussions with our candidates, students, and partners like Root-Me and CompTIA.

Since 2023, I have also been a member of a European working group led by ENISA (European Union Agency for Cybersecurity) focused on modeling cybersecurity skills. And, of course, all aspects related to creating or updating our content: develop new courses, validating and updating the curriculum, and expert's recruitment..."

What do you like/dislike about your job ?

"What I enjoy the most is the impact I can have through OpenClassrooms, it is really something I can be proud of! All our courses are available for free for the widest use possible and our degree programs aim to make certain professions more accessible. And in all of this I am surrounded by passionate and engaging colleagues and experts! What more could I ask for ?

However, one should have a long-term vision. You must know that between the moment we think about a new training program and the first graduation of this program, it typically takes around two, sometimes even three years: designing, launching, enrolling, the first students starting, their progress, graduation, and finally, their entry into the job market. The key word here is patience !
"

Thank you, Etienne, any last word you would like to share ?

"We are at a pivotal moment where the cybersecurity ecosystem recognizes the need to recruit more broadly and quickly, yet it is not succeeding enough in doing so. There is a mindset shift happening we went from strictly degree-based recruiting to skills-based hiring, and this is very encouraging news !

It's up to us to turn this opportunity into a success !"

New Section

THE EXPERTS' HUB

Weak signals detection and interpretation

By NABOU JAMRA Hiba & Mathieu Pichon

In this chapter, we will introduce the concept of weak signals. This concept is not precisely defined because authors from different disciplines use various terms to refer to it, and some even do not define it at all, assuming it is a well-known notion. Another way to define a weak signal is to clarify its characteristics by highlighting specific features that are unique to it.

Nevertheless, we will see that the various works on weak signals point to four key characteristics: although they are informal, rare, and difficult to interpret, they are indicative of forthcoming events.

Weak signals : a versatile concept

Igor Ansoff's article, "Managing Strategic Surprise by Response to Weak Signals", remains the key reference in the field of weak signal research. For the first time, the concept of weak signals is identified within the domain of Management Sciences.

Ansoff defines weak signals as "the first symptoms of strategic discontinuities that act as a form of early warning information, of low intensity, which may indicate a trend or significant event." This article emphasizes the importance for a company to detect nearly imperceptible information to either avoid threats or capitalize on opportunities.

The publication of this article came after the first oil shock of 1973, when political instability clearly showed that the strategic plans established during the post-war boom were no longer viable. Companies could no longer rely solely on extrapolating from past data to avoid being taken by surprise by changes in their environment, they realized they had to anticipate sudden events.

Ansoff's definition is based on the utility of a weak signal, identifying it as an element with anticipatory characteristics; however, this definition lacks precision and is more of a metaphor. Subsequently, many authors have built upon this work to clarify the concept.

Over the past fifty years, the definition of a weak signal has evolved.

Before 1980, the notion of a weak signal referred to emerging phenomena that could impact the future. In the 1990s, definitions began to focus on poorly defined sources and their impacts. During the 1990s, new adjectives emerged to describe the reasons these signals are so difficult to detect: small, dynamic, and peripheral. From the 2000s, definitions began to reference indicators of a phenomenon (such as a trend) rather than the phenomena themselves.

« A perception of strategic phenomena detected in the environment or created during interpretation, far removed from the receiver's frame of reference »

Van Veen et Ort

The concept of weak signals has developed across various fields, such as signal processing, information theory, corporate strategy, crisis management, and industrial risk prevention. Due to this diversity of domains, it has generated a rich lexical field. Several terms have emerged, such as “premonition”; in crisis management, we find terms like “alarm signal,” “warning signal,” “anomalous signal,” or simply “anomaly.” In the field of risk prevention, terms like “early signal,” “early alert,” “premature signal” are used interchangeably without distinction of meaning. In these two latter fields, weak signals are viewed as warning signals since they are studied from the threat’s perspective.

A signal is considered weak because it is difficult to detect, often buried under a multitude of data that is frequently irrelevant. However, such a signal is even weaker when it can indicate something very significant if industry experts are able to perceive and interpret it. Several authors have highlighted the specific characteristics of a weak signal, which can be summarized as follows:

Fragmented : We do not have complete information about the event to be anticipated, we only have a small number of signals to process. Based on their own interpretation, industry experts must be willing to make decisions. We also find adjectives such as incomplete, imprecise, and vague.

Apparent weak signification : There is no cause-and-effect relationship, the weak signal appears to be unclear or ambiguous, lacking meaning and requiring interpretation from industry experts.

Weak pertinence : It is scattered among a multitude of irrelevant data, and many people overlook this information, it becomes mostly unseen.

Weak signal life cycle

Weak signals are described as ambiguous indicators of potential future disruptions, requiring several filters to be processed before a decision can be made.

In the 1970s, Ansoff suggested that weak signals must pass through three filters:

Surveillance Filter : This refers to the ability of the weak signal to be detected amidst all other information and data perceived by someone.

Mentality Filter : This is the ability of the signal, once detected, to be recognized as relevant in the current situation. This filter is influenced by numerous cognitive biases -preventing decision-making. Biases such as the normalcy bias, confirmation bias, optimism bias, etc.it explains why these pieces of information may not be retained. These biases are individual, but organizational factors can also contribute to explain why weak signals get ignored.

Power Filter : This has to do with decision-making once the signal is detected and its relevance is acknowledged. Decision-makers may choose not to prioritize the signal despite the associated risk.

More recently, a fourth filter, the Transmission Filter has been added. This filter addresses the flow of information within an organization and is located between the Mentality Filter and the Power Filter. It acknowledges that those who first detect and evaluate the signal's meaning and relevance are typically not the ones with decision-making authority.

To conclude these various definitions, it's important to note that Ansoff was the first to define weak signals as the initial, unconfirmed signs of potential change that could later become indicators of opportunity or threat. This general definition has been adopted by other researchers who see weak signals as predictive raw material. They describe weak signals as fragmented, rare, and barely visible data today, which may conceal a trend.

Other scholars, such as Seidl and Rossel, suggest a perspective where weak signals are viewed as a 'socio-cognitive construction of reality,' helping experts make sense of their environment and act meaningfully upon it.

We consider a weak signal to be an insignificant piece of data whose interpretation by experts can trigger an alert. These alert signals that an event with potential opportunities or threats may occur.

Case study in an information system (By Mathieu Pichon)

Imagine you are walking at night and notice a man staggering and making strange movements. Instinctively, your body feels a weak signal suggesting that this man is suspicious, and even potentially dangerous.
In cybersecurity, detecting an attacker once they have infiltrated the information system (IS) is often challenging. The majority of weak signal detection relies upon the ability to spot the slightest mistake the attacker might make after being implanted.

Detecting weak signals is primarily based on research and development. The goal is to analyze real attacks and observe which of the IS passive behaviors are triggered. This could sometimes be represented by a simple event ID or by a consistent number of temporary files appearing in the same way and in the same quantity. To ensure accurate weak signal detection, the detection rule based on the correlation of these events should not generate more than 10% of false positives.

To illustrate this, let's return to a metaphor: imagine I program an AI to alert me of a potential burglary through my house' garden camera whenever several suspicious events occur. If my detection rule relies solely on it being nighttime and the person wearing black clothes, I might detect a teenager in a black hoodie who is simply retrieving a ball that landed in my garden. Although this teenager has no reason to be there, and no malicious intent, my response would differ significantly from how I would react to a man standing at 5 feet 11 inches tall with harmful intentions.

To avoid false positives, I would therefore add additional criteria, such as the person's height, their behavior, and what they are doing in the garden.

Let's consider a concrete example: our initial data source is the log perimeter where the attack takes place. Imagine an instance of dumping credentials from an Active Directory (AD). In this scenario, accessing an object triggers an event ID. However, my detection rule cannot rely solely on this information. The dump occurs on a rogue machine remotely, rather than locally, which means I can't depend on known commands.

I will conduct my own dump and analyze the weak signals emerging within the system. I will then check if these signals are recurrent with each dump and select the most relevant ones to add into my pre-production rule. While this process is demanding and takes a long time, it is highly effective thanks to its relevance, and the insights we get are invaluable."

FOR MORE INFORMATION ON THIS TOPIC

You can read the doctoral thesis by Hiba Abou Jamra, ***available online for free***.

One Month to get #CyberEngagés

The most important Cyber awareness month is back !

Launched in 2012, the European Cybersecurity Month (ECSM) is an initiative of the European Union Agency for Cybersecurity (ENISA). The goal is to raise awareness among EU countries about cyber threats and their prevention. In France, this event is known as "Cyber-Moi/s" and is organized by the teams at Cybermalveillance.gouv.fr.

In response to the increase of social engineering fraud, where cybercriminals manipulate victims to obtain money or personal data, ENISA chose this topic as the main theme for CyberMoi/s 2024, while also focusing on the impact of artificial intelligence on young people.

During the whole month of October 2024, various activities will be organized in France and across Europe around cybersecurity: events launch, awareness-raising sessions, video campaigns, and more.

As in previous years, a wide range of public, private, and non-profit stakeholders will come together to provide an educational program promoting a common cybersecurity culture in Europe.

CyberMoi/s Highlights

Many initiatives will take place in October:

CyberMoi/s Launch on October 1st, 2024

- Launch event at the French Assemblée Nationale
- Conferences for all
- Cyber citizen campaign : #CyberEngagés - stronger together
- Share a cybersecurity tip on social media to help people from your community
- Joint effort starting October 1st, 2024
- Open to all, public and professionals
- Use the hashtag #CyberEngagés
- Visuals available on CyberMoi/s Website starting October 1st
- CyberMoi/s Agenda (available in September)
- Get information about Cybersecurity awareness activities organized across the country
- Are you or your organization hosting an event? Get it registered in the agenda at CyberMoi/s site

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Example : How to raise awareness in your organization

“Quishing" : QR Code Phishing

In 2024, phishing remains the main cyber threat. Within the various forms of phishing identified by ANSSI (French Cybersecurity Agency), there is "quishing" a phishing technique using QR codes

QR Codes: Similar to barcodes, are encoded images containing information like websites links or apps to Download. Their popularity increased in recent years due to their convenience, allowing users to avoid manually entering links on mobile devices.

QR Code : A New Opportunity for Cybercriminals ?

Like any technological innovation, the rise of QR codes quickly caught the attention of cybercriminals. In recent years, fraudulent QR codes have regularly made headlines in national news for phishing schemes. Among the most common cases, there is fake parking ticket notices sent to homes or placed on the windshields of parked cars in several cities across France. These fake notices prompt recipients to scan a QR code for more information or to pay a fine, redirecting them to malicious websites.

Victims, believing they are settling their fines, end up recklessly providing sensitive information to cybercriminals: credit card data or other personal information.

Another common example is the fake delivery notification from the post office left in mailboxes. Recipients, believe they missed an important delivery, scan the QR code to reschedule the delivery or pick-up their package. Unfortunately, these QR codes often lead to fraudulent websites, cleverly designed to steal personal or financial information from their victims. This method exploits users' trust in postal services, making the attack all the more effective.

Cybercriminals have also targeted parking meters and electric vehicle charging stations by placing fake QR codes on them. Users who scan these codes, thinking they will pay for parking or charge their vehicle, are redirected to malicious websites. These sites may either attempt to steal payment information or install malware on users' devices. This form of attack is particularly insidious because it exploits trusted public infrastructures, making users less suspicious.

Fake Office365 login confirmation QR codes fraud scheme have also been reported within the workplace. These codes, sent by email under the pretext of security verifications, prompt users to scan them to confirm their login details, redirecting them to phishing pages where their credentials are stolen. Once in possession of this information, cybercriminals can access the victims' professional accounts, compromise sensitive company data and facilitate further attacks, such as intellectual property theft or ransom demands.

These fraudulent QR codes, known as "quishing" have been multiplying at an alarming rate.

The evolution of quishing tactics shows an increasing sophistication among cybercriminals seeking to exploit users' digital habits. Quishing campaigns can be highly targeted, focusing on specific individuals or companies to maximize the impact and financial gains of their attacks.

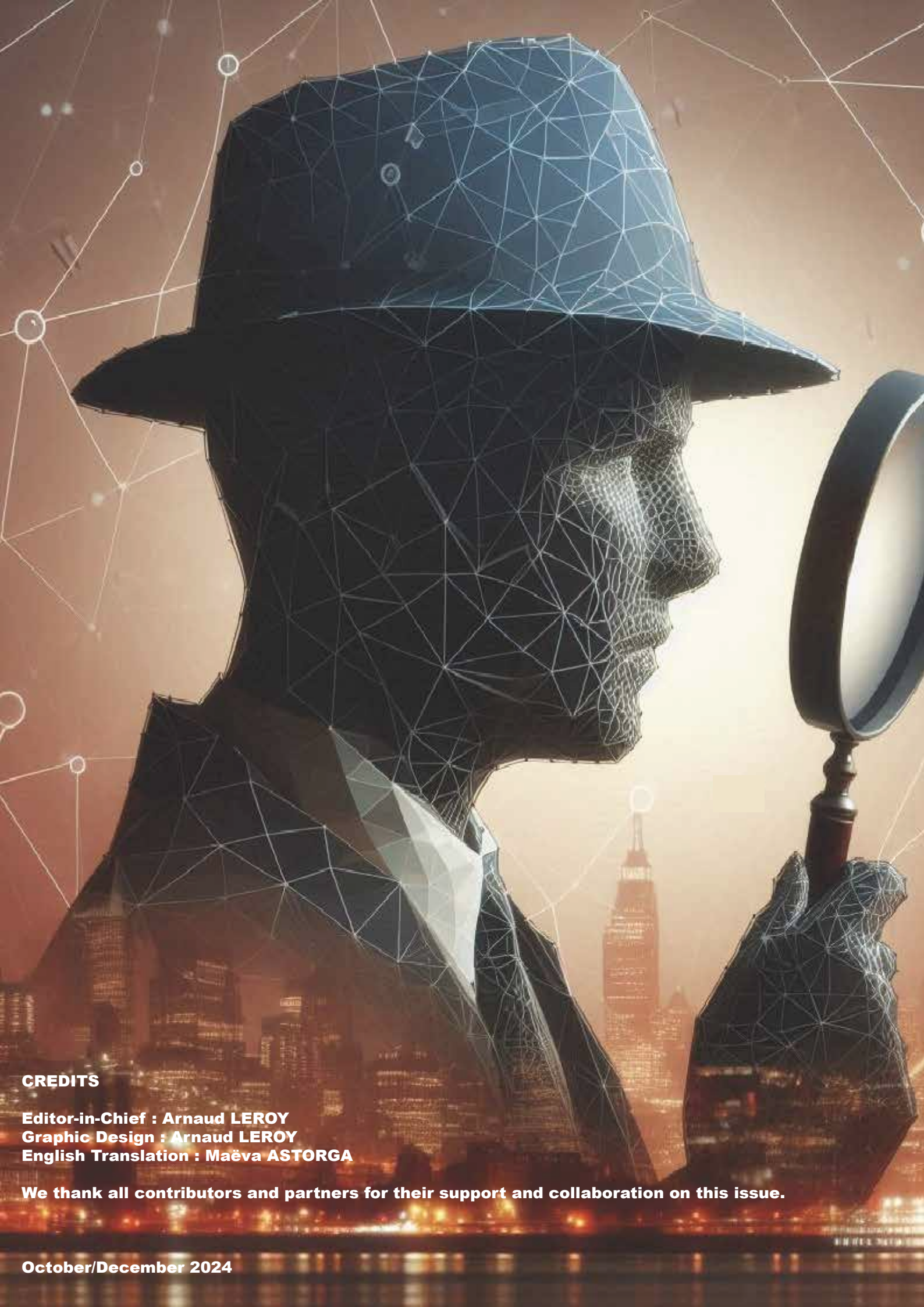
Our Recommendations

To protect yourself effectively against quishing, it is crucial to follow several cybersecurity tips and guidelines. First of all, verify the source of the QR code before scanning anything, make sure that it comes from a reliable and known source, and be particularly vigilant with codes received via unexpected emails or text messages.

Use reputable QR code scanner applications that offer security features such as URL analysis, to detect suspicious sites and link previews before opening a page.

Before providing sensitive information after scanning a QR code, carefully examine the URL to verify its legitimacy, ensuring it begins with "https://" and looking for signs of phishing, such as spelling mistakes or suspicious domain names.

En savoir plus !



CREDITS

Editor-in-Chief : Arnaud LEROY
Graphic Design : Arnaud LEROY
English Translation : Maëva ASTORGA

We thank all contributors and partners for their support and collaboration on this issue.

October/December 2024