bilingual edition

ptsoc{news}

Primeiro semestre 2026 | First half of 2026

#19

New Legal Framework for Cybersecurity

New .pt registration rules

Autonomous cybercrime and DNS abuse

The impact of AI on DNS abuse

Evaluation of national digital resilience

Credits

This publication is produced by .pt

19th Edition | First half of 2026

Edited and designed by: Casa dos Bits – Edições Lda

Luisa Ribeiro Lopes
Chair Of The Board Of Directors at .PT

Strengthening the community connection with PTSOC News

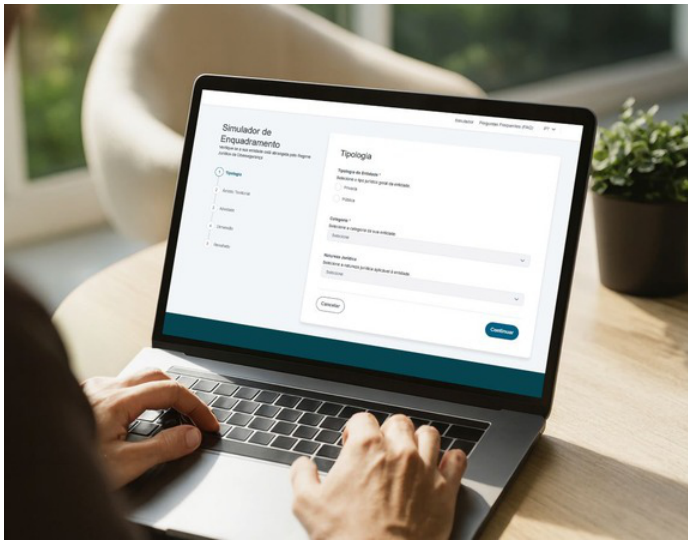
PTSOC News is now entering a new phase, marked by a design and content review. This evolution reflects the commitment to making the magazine a source of reference technical information and an active point of contact between .pt and the cybersecurity community. The goal is to strengthen proximity, promote knowledge sharing, and consolidate a collaborative network that contributes to a safer and more resilient digital space.

More than a visual update, this new phase reflects a strategic vision: to position PTSOC News as an information and cooperation hub, capable of keeping up with the growing challenges of digital security and supporting professionals and organizations in adopting best practices.

This reinforcement gains special relevance at a time when the new Cybersecurity Legal Regime — which transposes the European NIS2 directive — imposes new responsibilities and requirements on many covered entities. We want to continue contributing to the empowerment and awareness of the national ecosystem, reinforcing .pt as a domain of trust and excellence, and for this we count on the commitment of the entire community.

Índex

Cybersecurity Legal Framework



The new lifeline for companies and the country's digital resilience

The legal framework is ready for the application of the Cybersecurity Legal Regime, which transposes the NIS2 directive, with new challenges and obligations for a larger number of entities and deadlines to meet.

The topic of cybersecurity has definitively become part of the agenda of organizations of different sectors and sizes, and with the entry into force of the Cybersecurity Legal Framework, which transposes the European NIS2 directive, there is also a new phase with challenges for the entire ecosystem. Around six thousand entities are now subject to more demanding rules, reinforced responsibilities and tight deadlines, a number that is growing exponentially compared to the previous legal framework. Never before have so many public and private entities been required to comply with formal digital security requirements, with measures that are increasingly demanding, in a context where threats are becoming more global and sophisticated with the help of Artificial Intelligence.

"Cybersecurity is an investment, and that means it brings added value and improves the functioning of institutions and companies, increases the quality of products and services, and ensures the quality of life of people."

Lino Santos, Coordinator of the CNCS

The new regime was published in December 2025, officially came into effect on April 3, 2026, and has just been operationalized with the publication of the Regulation and the MyCiber registration platform of the National Cybersecurity Center (CNCS), which assumes the role of competent cybersecurity authority. But the path was already being prepared for strengthening the resilience of national information systems networks, with the stated objective of creating a safer and more resilient ecosystem, prepared to protect companies, people, and the rule of law itself.

"With the cybersecurity legal regime, what we want is more trust, more resilience, and more responsibility in cybersecurity," argued Lino Santos, Coordinator of the CNCS, during the C-Days 2026 conference.

Registration on MyCiber platform: Timeline and compliance steps

On the same day the new Legal Regime of Cybersecurity came into force, Portugal's National Cybersecurity Centre (CNCS) launched the MyCiber platform online - the official portal where organizations must register and maintain contact with national cybersecurity authorities. **The platform is now a central compliance step, as entities are required to register within the legal deadlines: 30 days for companies created after December 4, 2025, the date the legal framework was published, and 60 days for those established before that.**

After being notified that they have been qualified as essential or important, organizations have 20 days to communicate the name of the cybersecurity manager and permanent point of contact. And there are more deadlines to be noted on the agenda: by January 31, 2027, or 6 months after the notification of final qualification, whichever comes first, the List of Assets of essential, important and relevant public entities must be submitted.

Also note that, **within two years, in June 2028, essential entities must begin submitting an annual report and implementing cybersecurity measures, an obligation that also covers important and public entities.**

Non-compliance with the registration obligation results in the imposition of sanctions. The applicable fines are set based on the nature of the entity and the severity of the infringement.

Cross-cutting impact across 17 identified sectors

In addition to traditionally critical sectors, such as energy, transport, or health, the regime now includes companies from "important" sectors, essential suppliers, and a significant part of the digital supply chain. The impact is felt by large operators but also by SMEs that have never been involved in a cybersecurity regulatory framework.

The challenge here is deeper. Many companies start from low levels, without dedicated teams, structured processes, or internal policies. Others rely heavily on external suppliers, which increases complexity. And there is still a literacy deficit that translates into late or reactive decisions in incident preparation and response.

The responsibility of senior management in organizations is one of the changes in the new regime. NIS2 makes it clear that administrators and directors now have formal duties to oversee policies, approve measures, ensure resources, and monitor risks. The logic is simple: cybersecurity ceases to be a "technical" issue and becomes a governance issue.

Hackers vs. Crackers: What are the essential differences?

HACKERS
Ethical / White Hat

Goal: Improve security by identifying vulnerabilities before malicious actors can exploit them.
Approach: Operate with authorization, following rules, standards and legal frameworks.
Contribution: Strengthen systems, support companies and public entities, and help prevent incidents
Motivation: Ethics, research, protection and enhancing digital resilience.

CRACKERS
Malicious / Black Hat

Goal: Exploit vulnerabilities for theft, fraud, sabotage or extortion.
Approach: Act without authorization, breaking into systems and violating laws.
Impact: Cause financial losses, service disruption, data breaches and blackmail.
Motivation: Profit, digital vandalism, espionage or organized criminal objectives.

The consequences of non-compliance can be serious. The system stipulates high fines, proportional to the size of the organization, and penalizes negligence, although the Government has made it clear that it sought to implement a "balanced and proportionate" system, seeking to avoid "excessive contextual costs."

Lino Santos also argues that the CNCS wants to be a partner of the ecosystem, not just an inspector, working closely with the entities, sharing good practices and lessons learned, and listening to the organizations in their difficulties and achievements. The strategy involves empowering, supporting, and creating conditions for organizations to evolve.

Planning and improving maturity

For the organizations covered, the question is inevitable: what needs to be done now? The first step is to conduct a diagnosis and confirm eligibility under MyCiber, identify critical functions, and appoint a cybersecurity manager. Then, it is necessary to assess risks, implement technical and organizational measures, review contracts with suppliers, define incident detection and response processes, and prepare documentation for future audits. Training, from management to operational teams, is a mandatory part of this path, even with the lack of cybersecurity specialists, who are among the most sought after and may not be sufficient to meet the demand.

Ethical hackers get stronger legal protection

The regulation of ethical hacking is one of the major innovations introduced by the new Cybersecurity Legal Framework and represents a distinctive approach in Portugal's transposition of the NIS2 Directive. **The idea is to protect hackers who assess systems and platforms to identify vulnerabilities that can be reported to organisations and resolved before they are exploited by malicious actors.**
Under the new legislation, white hat hackers are granted legal protection when testing systems, applications or networks, provided they have explicit authorisation to do so. However, **they must not act with the intention of obtaining economic advantage, although they may be remunerated as part of their professional activity.**
Excluded from this protection are actions such as service interruption, system damage, deletion or copying of data, DDoS attacks, phishing or credential theft, all of which continue to be treated as criminal offences.

Simulator as a starting point for meeting obligations

Even before the publication of the Regulation and the launch of the MyCiber, the **National Cybersecurity Centre made available an online simulator that allows companies and public organisations to test whether they fall within the scope of the new regime.**

This is a first step to support the adaptation process, although the tool is not binding and does not cover certain specific cases. The result is merely indicative and is not subject to formal assessment, meaning that its use does not replace the mandatory registration of entities, which begins after the Regulation is published.

Who is covered by the Cybersecurity Legal Framework?

The new framework resulting from the transposition of NIS2 significantly expands the range of entities subject to cybersecurity obligations, now encompassing 17 sectors as well as Public Administration. The legislation differentiates between "sectors of critical importance" and "other critical sectors", and further classifies entities as essential, important, or relevant public entities.

Sectors of critical importance

energy; transport; banking; financial market infrastructures; healthcare; water management (drinking and wastewater); digital infrastructure; ICT service management; and space.

Other critical sectors

postal and courier services; waste management; production, manufacturing and distribution of chemicals; production, processing and distribution of food products; manufacturing industry; provision of digital services; and research.

The coming months will be decisive. With the new measures coming into effect within 24 months, organizations must accelerate their cybersecurity maturity by applying risk analysis and security policies, incident handling, and basic cyber hygiene and training practices. At C-Days, the CNCS coordinator warned that "these are not 24 months to leave everything to the last minute. It is a time to build and implement, a time to plan and grow in maturity gradually, and not leave everything to the last minute."

The challenge is not only technical but also cultural. The framework redefines responsibilities, raises demands, and forces a new way of thinking about digital risk. But it also opens up space for a more robust, better prepared, and more competitive ecosystem.

New .pt Registration Rules:

An evolution to strengthen trust and security in the portuguese digital space

Marta Moreira Dias
Member of the Board of Directors of .PT

The transformation of the digital environment and new legal and regulatory requirements, including the Legal Regime for Cybersecurity, are behind the evolution of the .pt Registration rules that will come into effect on July 1, 2026.

The Portuguese top-level domain (.pt) has registered sustained growth over the last few years, establishing itself as one of the best-performing European ccTLDs (country code Top-Level Domains). At the same time, it maintains very low levels of litigation, a residual number of complaints, and an extremely low rate of domain removal due to non-compliance with registration rules. This context demonstrates the maturity of the .pt ecosystem and the adequacy of the rules currently in force.

This is also why the revision of the Registration Rules, scheduled to come into effect on July 1, 2026, does not arise as a response to structural problems or flaws in the existing model. On the contrary, it is a natural and preventive evolution, intended to keep pace with the transformation of the digital environment, incorporate new legal and regulatory requirements, and respond to suggestions submitted by registrars, end consumers, stakeholders, and other market players.

Why was it necessary to revise the 2021 rules?

Since the last revision, carried out in 2021, the European and national legislative and regulatory framework has undergone significant changes. Among the main factors that justified the update of the Registration Rules are the entry into force of new legal instruments, such as the Digital Services Act, the Legal Regime for Cybersecurity, the Geographical Indications Regulation, and various national regulations that impact the management and use of digital identifiers.

The review also sought to reflect the experience accumulated by .PT in managing the national domain, incorporate operational improvements suggested by registrars, and align procedures with internal initiatives and processes developed in the meantime. These new rules therefore adequately reflect the increased demands for security, reliability, and accountability placed on the entity managing the national domain.

The central objective was to ensure that the rules remain clear, up-to-date, proportionate, and adequate to the challenges of an increasingly demanding digital ecosystem, without compromising the simplicity and efficiency that have characterized the .pt registration model.

Security and cybersecurity: a central axis of the review

Among the factors justifying the update of the .pt Registration Rules, the strengthening of security and cybersecurity requirements applicable to critical Internet infrastructures is particularly relevant.

As the entity responsible for managing the top-level domain corresponding to Portugal, the DNS.pt Association plays an essential role in preserving the stability, resilience, availability, and trust of the national digital ecosystem.

The management of the .pt ccTLD involves responsibilities that transcend the mere registration of domain names, also encompassing the adoption of preventive and reactive mechanisms aimed at mitigating risks and service compromise and other threats that may affect the security of users and the Portuguese Internet itself.

In this context, the entry into force of the new Legal Regime for Cybersecurity is particularly relevant. By formally recognizing .pt as an essential entity, the legislator has concretized and clarified a set of obligations already inherent in the management of a critical digital infrastructure, establishing a more robust framework of responsibilities regarding risk management, security governance, incident prevention, monitoring, reporting, and institutional cooperation.

The revision of the Registration Rules therefore also serves as an instrument for aligning with this new legal framework, ensuring that the terms and conditions applicable to the registration and maintenance of .pt domain names adequately reflect the increased demands for security, reliability, and accountability placed on the managing entity of the national domain.

It is also important to emphasize that this new regulatory framework is not limited to the DNS.pt Association. On the contrary, it promotes a more comprehensive and integrated approach to the security of the .pt ecosystem, clearly extending certain obligations and responsibilities to the various actors in the value chain, particularly registrars.

The security of the .pt digital space increasingly depends on the ability of all those involved to act in a coordinated manner, sharing responsibilities, best practices, and procedures that contribute to the prevention and mitigation of risks.

An update focused on the future

The new .pt Registration Rules represent a thoughtful evolution aligned with the current reality of the digital ecosystem. They do not alter the fundamental principles that contributed to the success of the national domain, but introduce improvements that reinforce security, the quality of registered information, legal compliance, and operational efficiency. This is our commitment, only achievable with the effort of all.

The main changes introduced in the .pt domain registration

Strengthening of data validation and verification mechanisms

One of the most relevant changes is the creation of a specific article dedicated to the validation and verification of data associated with domain name holders. It is now expressly stipulated that data verification is a condition for the registration of .pt domains, for the transfer of ownership, and for changes to essential contact information, such as email address or telephone number. The concepts of "validation" and "verification" have also been introduced into the Registration Rules glossary.

Adjustment of procedural deadlines

The new rules also introduce changes to the deadlines applicable to verification procedures. The deadline for confirmations, corrections, or additions to the data provided is extended from 5 to 10 days, providing greater flexibility for holders and registrars. Additionally, the deadline for analysing domain compliance is suspended while these requests for clarification or documentation are in progress.

Harmonization of registration conditions

Another important novelty is the application of the same registration conditions to .pt and .com.pt domains, simplifying the regulatory framework and promoting greater consistency between the different categories of domain names.

Clarification of the payment regime

The revised rules also establish that all registered domains will be charged, even when they are subsequently removed for not meeting the admissibility conditions stipulated in the rules. The future introduction of a fee applicable to the pending delete period for domains renewed at this stage of the lifecycle is also foreseen, with implementation occurring in a deferred manner.

New instruments for dispute resolution and legal compliance

The revision introduces the possibility of resorting to mediation within the framework of alternative dispute resolution mechanisms related to domain names. On the other hand, the possibility of blocking or redirecting domain names upon notification by a legally competent authority is now foreseen, allowing for a more effective response to situations requiring urgent intervention or compliance with legal requirements.

WHOIS Service Update

The changes also reflect the evolving requirements regarding the protection of personal data, addressed in conjunction with the aforementioned Cybersecurity Legal Regime. In the future, personal data will no longer be published in the WHOIS directory, and it will no longer be necessary to collect consent for this publication.
For legal entities, the name and address will continue to be available, while contact mechanisms will remain.

Autonomous cybercrime and DNS abuse

Trends shape the future of digital attacks

The IOCTA 2026 report describes a rapidly changing scenario where cybercrime becomes more autonomous, more invisible, and more difficult to stop.

Europol warns that, in the coming years, the ability of authorities to respond will depend on the adoption of advanced technologies, lawful access to critical data, and much closer collaboration with the private sector.

One of the most disruptive trends is the emergence of autonomous cybercrime. Criminal groups already use agentive AI systems capable of executing complete attack flows, from information gathering to intrusion, exfiltration, and monetization, with minimal human intervention. As these tools become more accessible, attackers are able to distance themselves from operations, reducing the risk of identification and transforming cybercrime into an increasingly intangible threat.

The report also highlights the evolution of hybrid threats, where state-sponsored actors and cybercrime groups collaborate fluidly. DDoS attacks continue to be used to undermine public trust and generate political instability, while hacker coalitions combine intrusions, data theft, and fraud schemes. The result is a dynamic attack ecosystem, where boundaries between espionage, sabotage, and financial crime become increasingly blurred.

At the heart of this new reality is DNS abuse, which IOCTA identifies as one of the most exploited critical infrastructures for online attacks and fraud. DNS acts as a bridge between criminal infrastructure and victims, allowing offenders to launch phishing campaigns, distribute malware, or control botnets through temporary domains. Criminals exploit the absence of automatic reporting mechanisms and the slowness of international judicial requests. By the time a malicious domain is finally blocked, the attack has often already reached scale.

DNS is similarly essential for ransomware and C2 operations, with botnets using residential proxies to mask traffic and mimic legitimate users. This technique makes detection difficult and dismantling criminal infrastructure significantly more complex.

The IOCTA 2026 reinforces that the future of cybercrime will be marked by distributed infrastructure, opaque cryptocurrencies, fragmented markets, and autonomous AI. To reduce the "speed gap" between attackers and authorities, Europol advocates a response based on technological innovation, lawful access to essential data, and continuous international cooperation. Without this adaptation, cybercrime will continue to gain ground.

The impact of Artificial Intelligence on DNS abuse

José Casinha
Member of the Board of Directors of .PT

AI has not changed the nature of DNS abuse attacks, but there has been an increase in scale, speed, and sophistication. The impact of autonomous agents is still uncertain, and a defensive response requires sustained, evidence-based adaptation.

The two major categories of Artificial Intelligence technologies, LLMs and autonomous agents, interact with DNS abuse in fundamentally distinct ways, and any serious analysis must treat them separately. The current state of abuse is dominated by LLM-assisted workflows; abuse driven by autonomous agents remains a short- to medium-term concern, not a documented present reality.

One of the most important findings when examining the role of AI in DNS abuse is that the fundamental attack vectors have not changed. Phishing, domain spoofing, malicious records, infrastructure-based campaigns, and SEO manipulation are not new phenomena—they have been operational tools of cybercriminals for over a decade. What AI has changed is not the nature of these attacks, but the economics and efficiency with which they can be executed.

This distinction is extremely relevant. It means that existing defensive frameworks, policy instruments, and detection approaches remain conceptually valid. The challenge is not to design responses for entirely new threat categories, but to ensure that existing responses can operate at the speed and scale that AI-assisted attacks now demand.

How AI is influencing the attack landscape

Perhaps the most consequential effect of AI on DNS abuse in the short term is the democratization of capabilities, that is, we are seeing a clear reduction in barriers to entry. Tasks that previously required significant technical knowledge are now accessible to actors with far fewer skills.

This is not just a quantitative change. It is a structural transformation in who can conduct sophisticated abuses.

Beyond content, AI tools — particularly autonomous agents — have the potential to transform how infrastructure supporting abuse attacks is created and managed. Domains can be registered, hosting environments provisioned, and campaigns reconfigured with reduced human intervention. When infrastructure is detected and eventually disabled, replacement infrastructure can be automatically created and activated without any human intervention.

This has implications that go beyond operational efficiency. It begins to challenge the economic logic of defensive takedown operations: if the cost of replacing disabled infrastructure approaches zero and the replacement can be automated, the deterrent effect of disruption is substantially weakened.

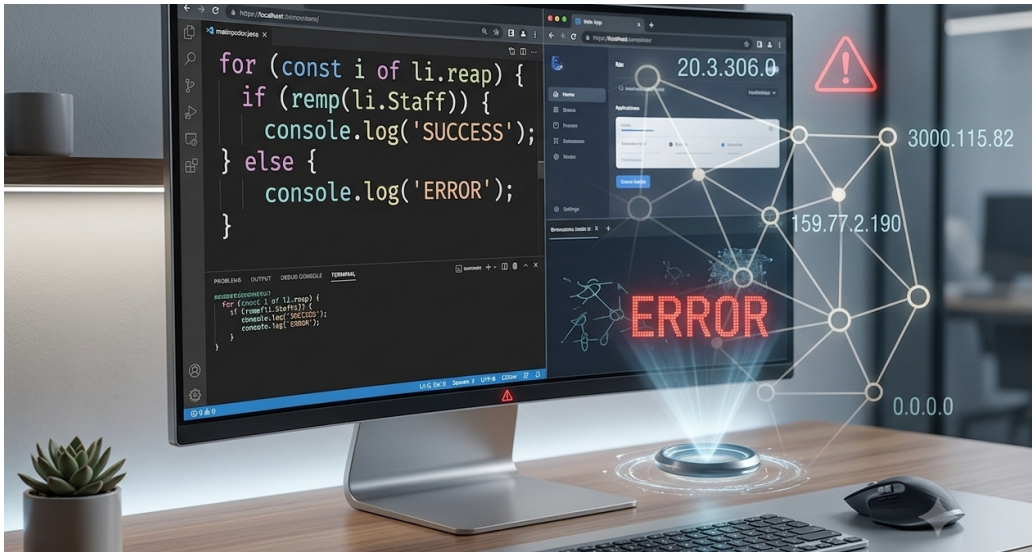
The convergence of scale and personalization with the ability to conduct campaigns that are simultaneously broad and individually tailored represents a qualitative shift in attack capabilities that was virtually unattainable before generative AI.

The role of existing AI in defensive infrastructure

The same capabilities that enable AI-assisted abuse are available for defense activities, with AI defensive applications in the context of DNS abuse playing a key role.

It is important to recognize that AI-powered defenses are not a future aspiration; they are already embedded in parts of the DNS ecosystem. Record risk assessment systems that flag potentially abusive domain registrations before they are completed already incorporate AI-adjacent techniques. The relevant question is not whether to introduce AI into the defensive strategy, but how to extend and improve existing capabilities.

Deploying AI in DNS abuse defensive contexts carries its own risks that require careful management. Hallucination, the generation of confident but incorrect outputs, is a real failure mode of LLMs that is particularly dangerous in high-risk abuse mitigation contexts. A false positive that incorrectly classifies a legitimate domain as malicious can cause real harm; a false negative that fails to detect malicious activity creates ongoing risk.



Perhaps the most consistent observation about DNS abuse in the age of AI is that this type of activity remains fundamentally dependent on human victims. DNS abuse is effective because it can persuade a human to click a link, entering credentials, downloading a file, or authorizing a payment. The attack chain ends with human behaviour, and that is the ultimate goal that gives value to the abuse.

This observation has an important implication: the evolution of AI-assisted DNS abuse will be reactive to how humans themselves change.

This means that all the AI investment on the attack side ultimately serves the purpose of exploiting human cognitive vulnerabilities: limitations in language comprehension, susceptibility to social engineering, the heuristics that guide online decision-making, and the varying levels of digital literacy among different user populations.

As potential victims develop better intuitions for AI-generated content, attackers adapt to produce content that defeats those intuitions. This creates a co-evolutionary dynamic rather than a one-time capability shift.

The only scenario that fundamentally alters this picture is the emergence of machine-to-machine abuse — attacks in which both the victim and the attacker are automated, and the harmful outcome is achieved without a human ever being involved in the cycle. This remains a future possibility and not a present reality, but the trajectory of AI agent development makes it a scenario that forward-looking analysis cannot ignore.

Short-term trajectory

Looking ahead, three developments seem most likely to shape the impact of AI on DNS abuse in the short term.

Increased scale and speed are the most certain short-term consequences. Already demonstrated capabilities — automated domain screening, rapid content generation, programmatic infrastructure management — will continue to improve and become more widely available. Campaigns that currently require significant operational effort will become more accessible and faster to execute.

Increased sophistication is the second trajectory. Not because AI will introduce fundamentally new attack techniques, but because the availability of capable tools for a wider range of actors means that more sophisticated attack patterns will become routine rather than exceptional.

The emerging activity of autonomous agents represents the third and less certain trajectory. As the capabilities of AI agents mature, the possibility of campaigns running with minimal human direction becomes more realistic. The implications for both detection and deterrence are significant.

Conclusion

AI is not revolutionizing DNS abuse in the dramatic way some narratives suggest, nor is it a fringe concern that can be safely postponed. The accurate characterization is that it is an accelerator—a set of capabilities that makes existing attack patterns faster, cheaper, and more accessible, without altering their fundamental nature.

The plots are old. The scale and speed are changing. The abuse economy is shifting in ways that favour actors who previously lacked the resources or skills to operate with sophistication. And the structural conditions—complete automation of the attack lifecycle, machine-to-machine abuse, autonomous infrastructure management—are approaching viability even if they are not yet the norm.

The appropriate response is neither alarm nor indifference, but sustained, evidence-based adaptation: improving detection, strengthening policy frameworks, deploying defensive AI thoughtfully and with adequate oversight, and maintaining community coordination that allows the field to clearly see what is really happening — as opposed to what is feared or assumed.

The human remains, for now, both the target and the essential link in the abuse chain. Understanding that the threat evolves in response to how humans change — how they interact with AI, how their trust calibration adapts, how their digital literacy develops — is perhaps the most important analytical framework for anticipating what comes next.

Cooperation to combat cybercrime

EU ratification of UN cybercrime convention boosts collective capabilities

The European Union's formal adoption and consent to the United Nations Convention against Cybercrime is an important step in harmonizing offenses and strengthening police and judicial cooperation, and accelerates cross-border access to electronic evidence, one of the biggest challenges in criminal investigation.

Digital crime is no longer a technical phenomenon and has become an economic, social and geopolitical problem. Cybersecurity Ventures estimates indicated that, by 2025, cybercrime could cost the global economy more than $10 trillion, with the potential to exceed $12 to $15 trillion. Organizations and citizens face more frequent, faster and more automated attacks, driven by AI tools that reduce costs for attackers and amplify the impact.

Cooperation between various entities and countries is highlighted as a crucial factor in a context of globalized cybercrime, where pressure also increases with technological evolution. In 2024, the United Nations moved forward with a United Nations Convention against Cybercrime that creates a common minimum basis for cooperating, investigating, and responding to attacks that cross borders in seconds, and now the European Union has formalized an accession that had already been approved in December of last year.

The Convention defines a set of digital crimes, establishes rules for the collection and sharing of electronic evidence, and strengthens safeguards for fundamental rights. The EU underlines that this agreement strengthens the EU's capacity to combat cybercrime together with international partners and expands international cooperation among the 112 UN Member States that are not party to the Budapest Convention on Cybercrime.

In this sense, the UN Convention responds to three central needs:

1

Faster and more effective investigations, creating more agile mechanisms to access essential data, always with judicial oversight.

2

Common minimum rules, reducing grey areas and facilitating joint action, especially in coordinated attacks involving multiple jurisdictions.

3

Protection of rights in a hostile digital environment, incorporating principles aligned with the EU Charter of Fundamental Rights.

In a digital ecosystem where an attack can originate from anywhere and target any organization, the European Union recognizes that cooperation is the only strategy to ensure a global fight, reduce risks, accelerate responses, and protect citizens, businesses, and democracies.

IberianQCI:

Portugal and Spain connect Quantum Communications Infrastructures

The goals for the three-year project are ambitious and include contributing to the development of a scalable European quantum communications ecosystem.

The IberianQCI project, led by Indra Space, was officially launched as the Iberian segment of the future European quantum communications network, EuroQCI, created to ensure highly secure connections between the Member States of the European Union and protect critical infrastructure and sensitive information against future threats.

With a planned extent of three years, IberianQCI aims to interconnect the national quantum communications infrastructures of Portugal and Spain, creating an integrated network that is fully interoperable with the European architecture. The initiative adds to the work already developed within the scope of EuroQCI and national projects such as PTQCI (Portuguese Quantum Communication Infrastructure) and DISCRETION, the latter led by Portugal to strengthen the security of military networks.

Funded by the Connecting Europe Facility (CEF), the project is coordinated by Portugal through Indra Space, in collaboration with scientific, technological and industrial entities from both countries. Among the Portuguese partners are Infraestruturas de Portugal, IP Telecom, Instituto de Telecomunicações, Altice Labs and Instituto Superior Técnico. On the Spanish side, the Polytechnic University of Madrid, Telefónica, the Consejo Superior de Investigaciones Científicas (CSIC), the Instituto de Ciências Fotónicas de Barcelona, the Centro de Supercomputación de Galiza and the University of Vigo are participating.

The development of quantum communications is vital to ensuring global cybersecurity in the face of the future capabilities of quantum supercomputers. These communication systems allow for ultra-secure and nearly impenetrable data transmission, serving as a pillar for the protection of critical infrastructure, government data and financial institutions. Unlike traditional networks, quantum connections allow the distribution of tamper-proof cryptographic keys, based on physical principles that make it impossible to intercept them without immediate detection.

Currently, fiber optics limits the transmission of quantum keys to about 100 kilometers, but the use of satellites eliminates this barrier, allowing global coverage with less signal attenuation.

The IberianQCI hybrid architecture combines terrestrial and space components. A cross-border link is planned between Vigo and Valença, using trusted nodes that strengthen connectivity between the two countries and integrate existing national networks. The space component will include three optical stations, in Madrid, Barcelona and southern Portugal, connected to the terrestrial segment in Lisbon. These stations will allow secure communications with the EAGLE-1 demonstrator satellite, in low Earth orbit, and with the future SAGA constellation, ensuring the distribution of quantum keys even between countries without common borders.

Evaluation of national digital resilience: Literacy, good practices and training need to be reinforced

The 7th edition of the Cybersecurity Report in Portugal, under the theme Society, outlines the readiness of Portuguese society to respond to cyber risks, identifying key weaknesses and emphasizing the need to enhance digital skills.

The document complements the Cybersecurity Report in Portugal, theme Risks & Conflicts, which was published in 2025 by the National Cybersecurity Center (CNCS), and seeks to offer an integrated view of the risk landscape in cyberspace of national interest, addressing behaviours, technological maturity and vulnerabilities in a context in which threats evolve quickly.

As individuals and companies increase their use of digital services, exposure to risks also increases, particularly in the areas of social engineering and fraud. The report identifies the main trends in incidents that have affected national infrastructures and confirms that the vast majority continue to be concentrated in the private sector, representing around 78% of the total, but a dangerous tactical mutation is observed in the attackers' targets.

The data reveals a significant worsening in Public Administration, where incidents increased by 67% in the space of one year, between 2023 and 2024. Local administration stands out as one of the most vulnerable targets, with around a quarter of municipal councils reporting active cyberattacks on their ecosystems during 2024 — a clear sign of structural weaknesses.

With regard to the types of attack vectors, the predominance of techniques that exploit human error and psychological manipulation remains. Phishing, smishing and vishing continue to be the preferred entry points for criminal scams, now combined with more sophisticated forms of social engineering. Online scams, account theft and compromise, and ransomware attacks, which paralyze operational services and demand large ransoms, remain among the most frequent threats. The report also highlights the growth of CEO Fraud, false recruitment campaigns and incidents involving infostealers, which accounted for more than 80% of malware activity observed in Q3 2025.

Companies still unprepared to respond to threats

Portugal appears as the fifth country with the lowest percentage of incidents among small businesses (10–49 workers), suggesting that digitalization has been accompanied by some adoption of security measures.

Despite the increase in incidents recorded by CERT.pt in 2024, a comparative analysis with Eurostat data indicates that the percentage of Portuguese companies affected by incidents impacting the availability of ICT services, destruction or modification of data, or disclosure of confidential information, was lower than the European average.

Still, most organizations have not reached high levels of maturity. Advanced firewalls, intrusion detection systems and strict access management policies continue to be primarily a reality for large enterprises, leaving smaller supply chains and partners exposed to indirect risks. Public Administration faces similar challenges: despite progress in digitalization and the adoption of security measures, these prove to be insufficient to prevent incidents with national impact.

Reduce the attack surface and strengthen cyber resilience

The report highlights that, although there is growing recognition of the importance of cybersecurity, this progress has not yet translated into an effective reduction in negative impacts. The perception of risk is high and organizations are reinforcing investment, particularly through hiring specialized services. However, recruiting qualified professionals remains a widespread obstacle, creating weaknesses due to a shortage of internal resources.

The lack of awareness and ongoing training is another critical point.

Most Portuguese companies do not promote regular cybersecurity training actions, nor do they integrate mandatory training for employees. The use of long-range campaigns targeted at the general public also remains small, limiting the dissemination of basic cyber hygiene practices.

Given the vulnerabilities identified, the report recommends strengthening digital literacy and associating it, from an early age, with specific cybersecurity literacy. It also advocates for intensive human resource training, with a special focus on Public Administration, especially at the municipal level, and on small and medium-sized enterprises, which continue to lack a budget dedicated to digital protection. Increasing the reach and effectiveness of public awareness actions is also pointed out as essential to equip citizens with skills that allow them to mitigate fraud and scams before they reach home or business networks.

78%

of incidents occur in private sector companies

+67%

growth in attacks against Public Administration between 2023 and 2024

25%

of local administrations reported detecting cyberattacks in 2024

19th Edition | First half of 2026