Interview

IRINA
Rybalchenko
✕ @PeriodicAND

The ANC-AD is responsible for planning, coordinating and managing the cybersecurity of the country's networks and information systems, both nationally and globally. We spoke to Jordi Ubach, head of the national cyber security agency, about the current importance of computer security, types of cyber attacks, and advantages and disadvantages of the explosive development of AI.

–What is the primary function of the agency?
–The agency was created in 2021 by an executive order published in BOPA. The 2022 law established a number of objectives. Our daily life is essentially the cybersecurity of the country. The agency's charge is to verify the correct application of the law, which has a number of obligations and limitations. We provide support, and are the single point of contact, for any type of incident. We do not work from inside the company - we fulfil this task from outside.

The agency is a government-dependent body.

–How important is cyber security in today's business?
–Increasingly, more and more companies consider IT security very important. Many companies no longer see security as a burden, but as another company asset.

–But can we say that the education of entrepreneurs in this area is sufficient?
–Generally, people don't have sufficient cybersecurity knowledge, and it is difficult to find qualified personnel. That's why we try to get closer to the people by organising seminars and social campaigns and arranging classes in schools and at the University of Andorra.

–How often are cyberattacks carried out?
–Across Europe there are about thirty thousand cyber attacks per hour. With the right preventive measures in place, a high percentage cannot reach their target, so there are actually very few successful

I.R.

Jordi Ubach
Cybersecurity specialist

«The main profession of the future - cybersecurity specialist»

«People receive links via email, WhatsApp or Instagram, click on them and don't even realise that they are accessing their data at that moment»

cyberattacks.

–In the case of a successful cyberattack that results in, for example, data loss or website lockdown, how long would it take for a company to mitigate the effects?
–Cyberattacks don't happen all at once. Unless it is global and generic, an attack on a company usually starts with a prior period of getting inside the company's infrastructure. This is about 270 days, the time needed to investigate the company's defences.

If the company has backups of all data systems, the systems can be restored within 24 hours. If there are no backups, it will take a long time to restore the systems, and they may lose data. There can also be economic and reputational losses.

Andorran companies do not suffer from serious attacks; here we are talking about medium level attacks. In the context of Europe, 70% of attacks target SMEs (a category of companies with less than 250 employees). In Andorra, in terms of cyber secrecy and, especially, the application of the law, we are in our embryonic stage compared to other countries where laws or regulations have been in place for years. But we are on the right path!

–How can businesses and individuals protect themselves?
–Don't use public Wi-Fi! Obviously, when a service is free, we all want to access it, and then we have problems, because we make it easy to access our data.

Always read the security policy before accepting online services. Public Wi-Fi networks are unsafe, because we don't know who owns them.

Our computer is safer because

►► In the future many jobs will be focused on controlling the tasks performed by the AI

Windows includes an anti-virus package, but our mobile phones don't support it. A licence for the same antivirus can be used on three different devices and costs about 10-12 euros a year.

People receive links via email, WhatsApp or Instagram, click on them and don't even realise that they are accessing their data at that moment.

We often think, «Who needs my data»? Well, the truth is, there will always be someone who wants it.

ANC-AD, in its 2022 annual report, showed how over 4,000 mobile devices were affected by malware (RedLine), which is a malicious programme that captures all the data we have: our passwords, emails, messages and personal photos.

–How has the type of cyber threats in the country's economic sector changed?
–The types of threats are the same, including fraud, data theft and extortion. It used to be calls and direct contact, now it's all moved to the digital world. We all tend to be good people. But we need to be careful with all these things!

–Is there any problem with the quality of professionals in this field?
–By 2025, Europe will have a shortage of 2,000,000 professionals in cybersecurity and the defence of the entire digital infrastructure. Given the rapidity with which the digital world is evolving, and given the relevance of AI and the expansion of the perimeter of companies (remote work,

«Across Europe there are about thirty thousand cyber attacks per hour»
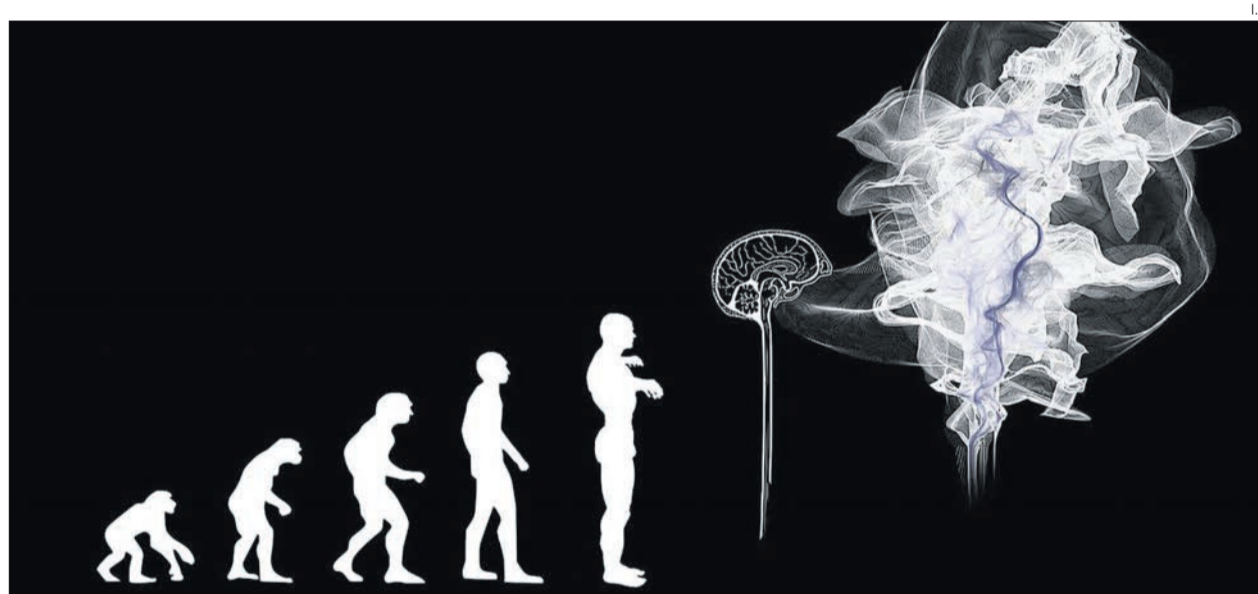
freelancing, etc.), we can assume that this will be the main profession of the future.

–What are your predictions for the development of technology and new computer security trends?
–The trends for 2024-2025 at the European level will be an increase in attacks, but more directed at individuals and companies - above all, at the supply chain.

–It would be interesting to know your opinion on the presence of AI in modern society....
–If we weigh the pros and cons, the result is positive, because AI allows us to develop more powerful tools that can detect any threat; therefore, the benefits, in terms of global security, are greater. But it's like a sharp knife that can be used to cut something - or for other, much worse things.

–I recently read the news that fake accounts on social media have already created their own language, and we, humans, have lost control for a moment. The world that science fiction writers have talked about is just around the corner, and it's getting dangerous. Wouldn't you agree?
–Europe is very concerned about the ethical side: what needs to be regulated and what will be beneficial? Will there be job losses? Yes! Will there be a new industrial revolution? Yes! Some occupations will have to reinvent themselves; make changes. Basically, many jobs will be focused on controlling the tasks performed by this AI. ≡