How AI is supporting cybersecurity

Summary:
As in many other sectors, artificial intelligence (AI) is a game changer in cybersecurity. In an increasingly connected and digital world, cyberprotection needs a powerful tool such as AI, able to learn from new behaviours, adapt to an ever-changing environment and be customised to clients’ needs. Thales IT security expert Olivier Bettan explains how AI can be used for protecting a business from cyberattacks and the different approaches Thales is working on.

“Welcome to our series of Thales podcasts on Artificial Intelligence.
With us to discuss the subject of AI in cybersecurity at Thales is IT security expert Olivier Bettan.

Welcome Olivier and thank you for explaining to us today how AI is supporting cybersecurity and how it can help protect a business from hackers.

Questions:

1) Olivier, we live in a world that’s more connected than ever, which leads to a growing need for cybersecurity. What is AI bringing to cyberprotection, and how is it doing so?

   Al helps us better detect cyberattacks, reduce the number of false positives — in other words, anything mistakenly identified as a threat — and AI also generates more readily understandable and actionable results.

   AI also helps us to detect advanced persistent threats, which are becoming ever more sophisticated, and also to respond faster.

   With AI doing all this, humans are be able to focus on high value-added tasks in a sector where the right talent is hard to find and demand is growing all the time.

2) So, AI has an important role to play in detecting cyber threats and attacks.

   Exactly!

   Attacks are becoming increasingly sophisticated. They’re evolving all the time and can also use AI themselves to select their targets, optimise their intrusion capabilities, determine the best vulnerabilities to exploit and, as far as possible, stay under the radar of detection systems.

   On the defence side, it’s absolutely vital that we know and understand these new techniques. Thus we can develop appropriate and effective detection solutions.

3) We’ve all seen Hollywood movies where AI takes control. Is that a real risk?

   We’re still a long way from artificial general intelligence which would no longer be controlled by human decisions. Currently, each AI system deals with a specific issue.

   And by their very nature, systems with built-in AI are designed to function with a certain degree of autonomy. Yet it’s really important for these systems to be robust and reliable, and
they need to assist their human operator in a completely transparent way to avoid the "black box" effect.

4) **But, can we trust AI in the cybersecurity world?**

The French defence procurement agency recently published a set of best practices for the supervision, or control, of AI systems that have a high degree of decision-making autonomy. As long as we can restrict the actions of an AI system to what we deem acceptable, the problem of the machines taking over can’t arise. Otherwise, defining built-in laws into AI systems — like the Three Laws of Robotics in Isaac Asimov’s novels — would involve a degree of interpretation that would be prone to error.

5) **Is it fair to say that AI is helping detect information and behaviours that were not detected before?**

Yes. Combined with Big Data, unsupervised AI can help us counter unknown threats — unlike conventional cybersecurity systems based on known threats and signatures.

It does this by rapidly detecting unusual situations and flagging behaviours that don’t correspond to what we would expect in a given situation.

⇒ AI provides a constant stream of evidence, that forensic investigators can usefully navigate through and analyse.

6) **In very concrete terms, how are you working on cybersecurity powered by AI?**

When we work on a project, our cybersecurity specialists and AI experts first choose the type of model to be used. It depends on the operational information available and the detection problem they need to solve. They can use a supervised or an unsupervised approach.

Next, they decide on the lifecycle of the AI used for detection.

The AI model could be trained once and for all before being deployed. This would be the case if the behaviour is periodic or for certification purpose.

AI can also help us with prevention or for decision support. In the case of a massive attack, when there is no time to talk to operators, we let AI do its job.

Where the effect of AI decision present a critical risk, we ask operators for their opinion.

7) **Can the AI model be trained several times or is it something we can just do once?**

The AI could be periodically retrained, for example in the case of expected environment changes.

Alternatively, it could learn on a continuous basis, for example when the behaviour to be characterised is evolving.

In cybersecurity, the second scenario prevails.
8) **You mentioned earlier a supervised approach for the AI model. Could you explain what it is?**

Yes. A supervised learning approach involves building a predictive model on the basis of raw data or labelled results.

Specifically, for a classification algorithm, this means predicting which category an object will fall into (using support vector machine, decision trees, neural networks, etc.).

9) **How do you apply this to cybersecurity?**

In cybersecurity, we configure our supervision systems so they respond to behaviors placed in specific attack classes by our AI models.

The supervised approach has the advantage of generating a response in line with our Thales TrUE AI standard – TrUE standing for “Trustable”, “Understandable” and “Ethical”.

Classes can also be defined by the customer, depending on their own objectives, the issues they face, the cyberthreat environment or their information system.

10) **And what about an unsupervised approach?**

The difference with the supervised approach is that it enables us to discover an internal representation, or a structure, solely on the basis of unlabelled raw data.

To deal with unknown attacks, we need an unsupervised approach.

Here, we expect AI to autonomously group the data we feed into it. But AI doesn’t assign meaning to these automatically defined groups. Only operators can attach a semantic to them, limit their number and determine which are of interest.

11) **Are there any kind of mixed approaches?**

There are indeed intermediate approaches, such as semi-supervised learning, or active learning, which allow operators to provide the AI system with feedback on the relevance of its responses.

For all the approaches I’ve mentioned – supervised, unsupervised or intermediate - we definitely need to be able to explain to user why the AI system made the decisions it did especially to ensure AI adoption.

12) **How is AI able to work in situations where there’s no data?**

This is where learning-based AI reaches its limits. When there’s little or no data, different approaches are possible.

You can generate synthetic data to supplement the data that the AI system will process. The difficulty here is ensuring that this data is sufficiently representative of reality. In particular, it’s important to ensure that all the simulated behaviours in the scenario are consistent.

Another approach is to reduce the scale of the learning problem by injecting more operational knowledge.

13) **How will AI react in the event of multiple and simultaneous attacks?**
In cybersecurity, the issues aren’t the same as with a driverless car, for example. Decisions are made in line with the level of risks established by the Thales team and our customers. We define a hierarchy, specifying what has the most value, the functions that absolutely must continue to operate, etc.

In the case of a simultaneous attack, decisions will be made in accordance with the potential loss or damage in terms of image, value, financial impact, ...

Nonetheless, it’s very difficult to predict the knock-on effects that could result. In the longer term, a decision can have unexpected consequences, which can be even more devastating.

AI is also used for this — to triage alerts and rank them in order of importance. At Thales, we’ve developed a solution called Cybels Analytics to help our customers in this area.

**14) Could you say a few words about this solution?**

Cybels Analytics combines the expertise of our AI and Big Data specialists, data scientists, and our cybersecurity experts.

It’s a complete solution that adapts to the situation of each customer and to the target environments.

It offers advanced detection and hunting capabilities to identify the most complex attacks.

It incorporates Big Data technologies and personalised AI algorithms, as well as Cyber Threat Intelligence databases, which further improve its detection and analysis capabilities. Cybels Analytics is coupled with a file analysis centre, which detects the most complex malicious code.

**15) More generally, what is Thales able to bring to AI-based cybersecurity solutions?**

There’s a huge shortage of cybersecurity experts, and Thales can help fill the gap.

Customers also come to us for our expertise and for access to the outside sources of intelligence we can provide. We help them expand their knowledge.

Thales has a broad diversity of business activities and complementary expertise in cybersecurity and AI.

We have a good grasp of the issues and we know what our customers need.

We have 30 years of experience in the AI community, and we know a lot about the models and operating procedures involved

We also keep a very close eye on developments so that we can configure our solutions as effectively as possible.

**Conclusion:**

It’s on Thales’s expertise that applies AI to cybersecurity that we’re going to end our interesting discussion. Thank you Olivier and thanks to our listeners. We look forward to having you with us on the next podcast in our series on artificial intelligence. We’ll be talking about AI in biometric recognition, ethics and space. We hope you’ll all join us.