New technologies, new threats

Les Assises de la Sécurité et des Systèmes d'Information [1] [the Security and Information Systems conference event], took place in Monaco from 10 to 13 October 2018 and brought together decision makers, CISOs, jurists, and experts in digital transformation and cyber threats, to focus on a range of central and sensitive topics.

The subjects addressed this year were even richer and more varied than before. Amongst the themes set to be discussed at Les Assises were how to secure the Cloud and IoT, the GDPR rules, security "by design", proven codes, new vulnerabilities linked notably to the rise of Artificial Intelligence, and the essential contributions AI is making to cybersecurity. These security-related questions are part and parcel of companies' digital transformation and, as such, they dictate whether any new platform is – or is not – adopted. Running through all of this, it is very much our confidence in digital that is being tested and is at stake here, whatever the relevant technology may be. Digital insecurity impairs trust, which, when it becomes lost, has the effect of suppressing any creation of value, thereby wiping out the attraction and benefits of innovation. The flood of connected objects in both private and public spheres (more than 6 billion objects in 2018, according to Gartner [2]) brings with it fresh vulnerabilities that are immediately exploited by cybercriminals. A connected object sold for just a few dozen euros is, by its very nature, very hard to equip with "by design" protection. Consequently, the object can find itself being "recruited" into a botnet and used as part of a powerful Distributed Denial-of-Service (DDoS) attack. Such attacks have been mounted by armies of connected refridgerators, watering systems and videosurveillance cameras affected by security flaws. Ransomware attacks increased significantly during the 2016-2017 period, with more than 2.5 million recorded cases (2016-2018 Kaspersky report [3]). They have a severe impact on companies, encrypting their data and only sometimes returning it to them, usually in exchange for a ransom to be paid in bitcoins. In 2017, the WannaCry campaign of attacks affected thousands of targets spread out across the five continents, making it one of the major worldwide cyberattacks. After WannaCry, in 2017 and 2018 came the Petya, NotPetya, GoldenEye, and Bad Rabbit ransomware, inflicting heavy financial losses on those companies that fell victim to these waves of attacks.

Clearly, Cloud Computing is confronted with new threats which, if not taken into account, can undermine customer confidence. Artificial Intelligence, and in particular machine learning, are indeed providing new ways to secure Information Systems. However, paradoxically, AI also brings with it new vulnerabilities.

AI used for cybersecurity: an area of competitive French know-how

As expected, Artificial Intelligence is transforming cybersecurity practices by providing new solutions to tackle advanced, furtive, digital threats. Such threats often remain "under the radar" of classic defence systems, such as antiviruses, firewalls, and SIEM (Security Information and Event Management) that are based on signature analysis, rules engines, and human expertise. AI makes it possible to detect certain threats way upstream of the attack by taking account of all events occurring in the information system (IS). After an initial phase of machine learning, the UBA (User Behavior Analytics) systems analyze the behavior of users and the network's components. They can then react to "abnormal" events and weak signals that are often a warning of a furtive cyberattack.

Using AI, it is possible to categorize the large volumes of massive data transferred up from the IS's various sensors and generate security alerts, without knowing beforehand what type of attack will be mounted. This unprecedented approach has produced effective UBA platforms developed by IBM, CISCO, and SPLUNK.

On the French front, whilst Thales offers equivalent solutions, two cybersecurity companies (ITRUST, in Toulouse, for information systems, and SENTRYO, in Lyon, for industrial networks) have managed to develop UBA supervision platforms rivalling the American solutions. Their respective successes prove that it is possible to build a competitive and scalable French offering at international level even with limited means. A third company (the Trust In Soft startup) is making its mark in the promising segment of code proofing by developing solutions that make it possible to certify portions of programming as safe code (free of bugs and security flaws). This technology relies on computer algebra to automatically prove the safety of a piece of programming.

AI cybersecurity

This new field of expertise is key to determining just how much confidence users will place in automated systems equipped with Artificial Intelligence. Consumers will not be prepared to adopt autonomous cars and pilotless planes unless the AI embedded in them is perfectly safe.

Recent research work undertaken by French experts* (amongst others) have exposed cases of neural networks being attacked using contradictory examples. This type of attack works by digitally introducing image noise into images, such as those of animals, or traffic signs, which the neural network is normally well able to recognize, but which it sees as being a totally different image, once the image noise has been introduced. For example, this can cause the AI to interpret the Stop sign as a right of priority sign! It is easy to see how AI cybersecurity issues are today becoming central to the design of autonomous systems. The French Artificial Intelligence ecosystem and its R&D have a key role to play at international level. To achieve this, however, France must manage to retain its data science researchers and, crucially, work swiftly to build a favorable environment for its startups developing cybersecurity solutions for AI.

In these two disciplines, we have available to us a dynamic pool of talent possessing all the necessary qualities to make us a world leader! Have we not already shown that we are capable of becoming world champions?

ERIC COHEN

FOUNDER & CEO OF KEYRUS

[1] *Les assises de la sécurité* – Monaco https://www.lesassisesdelasecurite.com/
[2] IoT statistics – Gartner report https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
[3] 2016-2018 Kaspersky report on ransomware https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf