ARTIFICIAL INTELLIGENCE, SEEN BY A CISO

GRÉGORY NOU
ISED, 10/05/2019

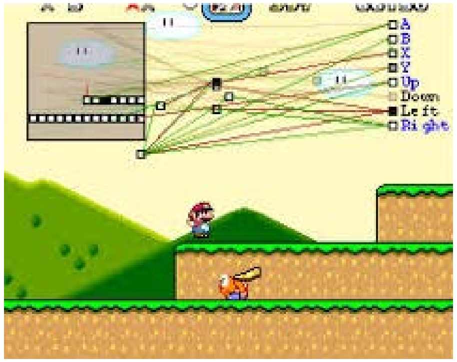
BGL
BNP PARIBAS

La banque d’un monde qui change

Who I am

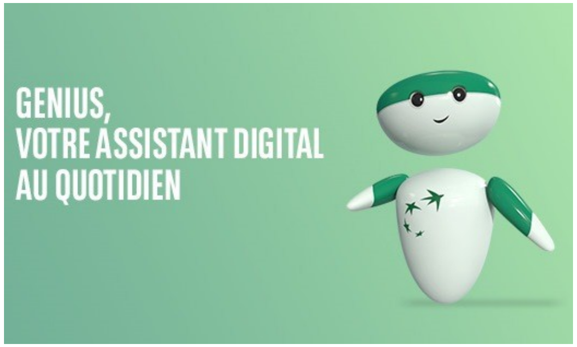
- My name is Grégory Nou
- CISO for BGL BNP Paribas (a bank) since 2015, also in charge of IT risks management
- Graduated from CentraleSupélec, with a specialization on Artificial Intelligence and High-performance computing (CyberSecurity was not really a thing at that time)
- « CISO of the Year » in Luxembourg, nov. 2018

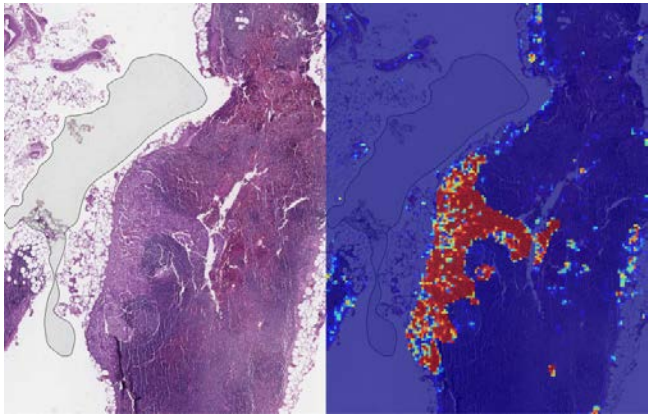
What do we mean by AI?



At its core, artificial intelligence is all about **automatically classifying** things **in arbitrary categories** that **make a sense** from a business perspective, so the user can make the best decision possible.

Being a bit provocative : that’s just (clever) algorithms fed with a lot of data, and that try to transform that data into actionnable information.
Sometimes, we can go as far as letting the machine decide.

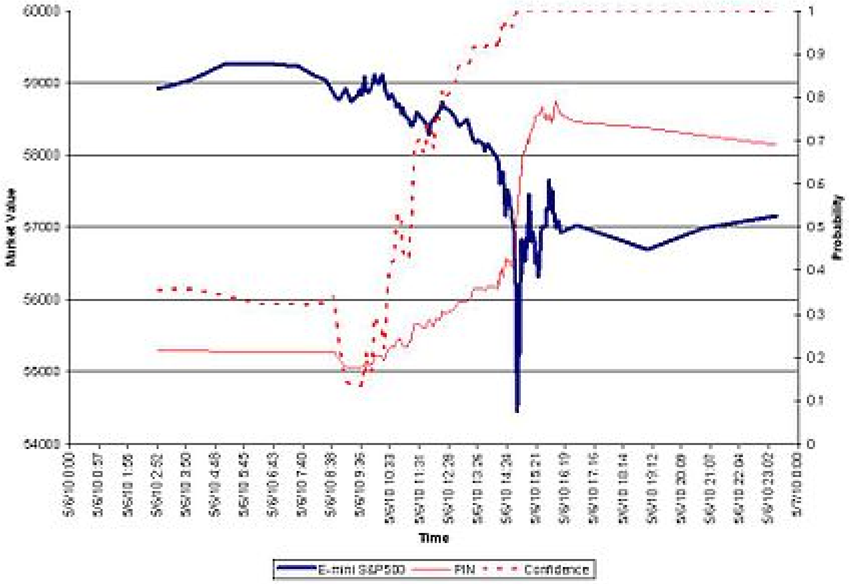




What could possibly go wrong?

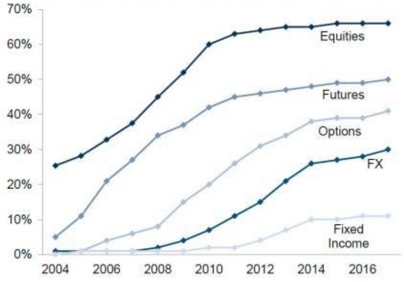
- Programs never fail. Until they do.
- May 6th 2010: **flash crash** of the Dow Jones (-7% in 15 minutes)
- The cause (according the SEC): an issue in an algorithm of High-Frequency Trading that was not able to handle unusual conditions (May 6th was a very volatile day)
- Not everybody lost money that day: a London-based trader allegedly made $40M in profit (and was subsequently arrested and prosecuted for market manipulation)

Since algorithms are deeply involved in price calculation, attacking them is way to make money.



Algorithmic trading has grown across asset classes…

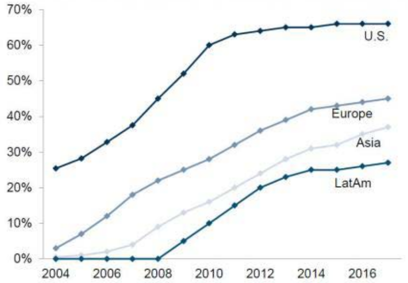
Market share of algorithmic trading by asset class, %



Source: Aite Group, Goldman Sachs Global Investment Research.

…and regions (though the US still leads the way)

Market share of algorithmic trading by region, %

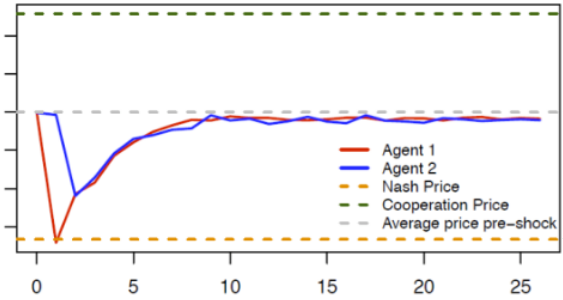


Source: Aite Group, Goldman Sachs Global Investment Research.

What could possibly go worse?

- The Tay's Microsoft experience
  - Tay was an AI-based twitter bot, which became xenophobic and misogynist in less than a day (and 96000 tweets)
  - Lesson: if you don't want your AI to behave stupidly, treat it like a kid: be very careful about what it learns
  - There is research on deceiving ML-based algorithms.

- Did you know that algorithms can recreate cartel, without knowingly doing so?
  - According to Chen et al. (2016), one third of vendors had automated pricing
  - Considering that AI can beat humans at Go, Chess (and Mario), could it beat the human at pricing?
  - Calvano et al. (2019) found that price-fixing (collusion) is an emergent property of AI-based pricing algorithms.



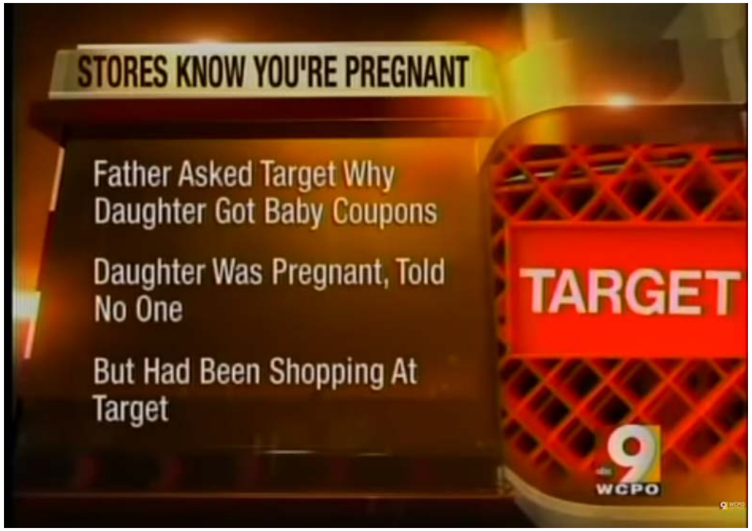
Collusiv e price

Nash Equilibrium

> *What is most worrying is that the algorithms leave no trace of concerted action – they learn to collude purely by trial and error, with no prior knowledge of the environment in which they operate, without communicating with one another, and without being specifically designed or instructed to collude.*

The issue of protecting the data (when you don’t know it’s there)

- As CISO, we’re efficient at protecting « the business »
- Usually, that means protecting its data (Confidentiality, integrity and availability)
- Problem: we can protect only what we’ve identified as having an interest
- Additional issue: it might come with a lot of bad press coverage

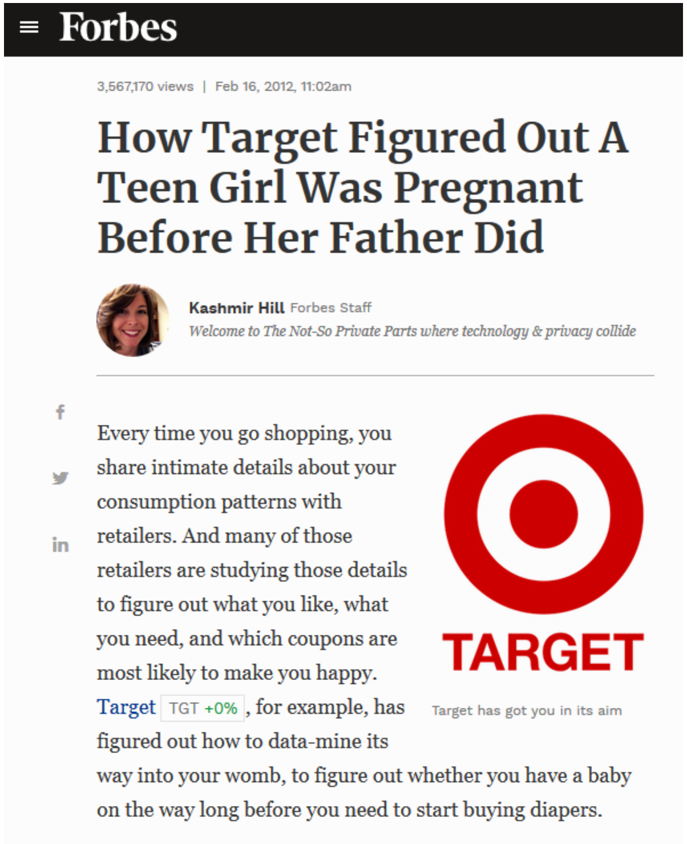


STORES KNOW YOU'RE PREGNANT

Father Asked Target Why Daughter Got Baby Coupons

Daughter Was Pregnant, Told No One

But Had Been Shopping At Target



≡ Forbes

3,567,170 views | Feb 16, 2012, 11:02am

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Forbes Staff
Welcome to The Not-So Private Parts where technology & privacy collide

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +0%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

With AI, the valuable data is not always what you think it is

❖ To be successful in implementing a ML-based algorithm, a scientist has to understand “the business” behind.

Therefore, a successful algorithm is the combination of two equally important factors:

1 The precise electronic transposition of a business process, with all its subtilities

2 A lot of effort, by very clever, experienced and competent people (meaning they’re difficult to hire)

➲ An AI algorithm is a very valuable intellectual property, that has to be protected !

- A lot (= way too much) of literature on “stealing machine learning models via APIs”
- Industrial espionage is a real thing, even for/between startups

A gloom future?

- If we did nothing, yes. But we are acting.

- The challenges posed by AI are not actually new
  - Intellectual property protection
  - The shadowIT tentation (the web in 200x, the cloud in 201x, …)
  - Data protection (BigData)

- To conclude on a positive note, AI can actually help cybersecurity people!
  - Detection of abnormal behaviour in a network
  - Detection and classification of malwares
  - Generic security incident detection
  - Risk assessment (cooperation between Uni's SnT and BGL)

MERCI

BGL BNP PARIBAS
50, av. J.F Kennedy L-2951
Luxembourg
Tél. : +352 42 42-2000

www.bgl.lu