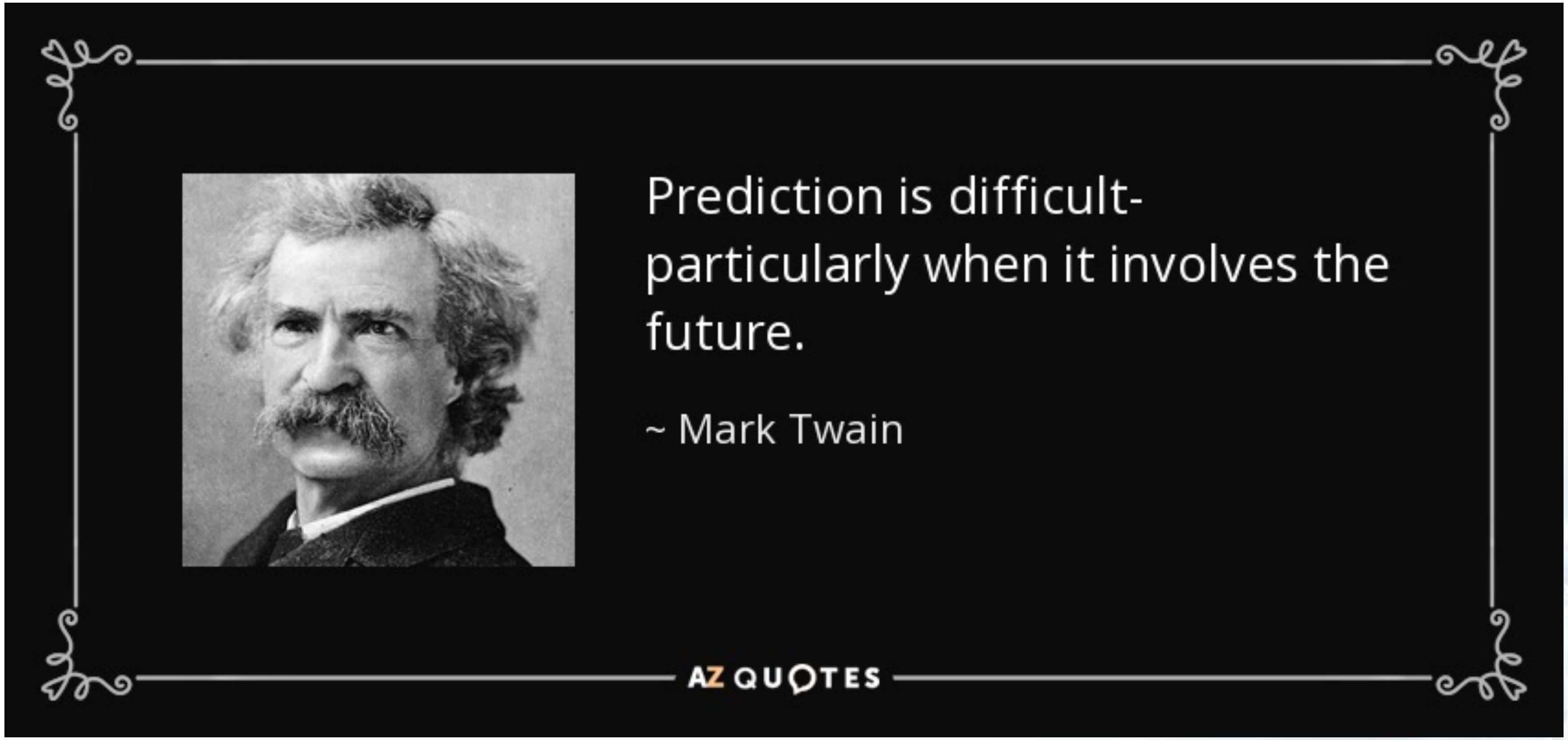
Artificial Intelligence: Opportunities and Threats in the Cyberspace

Marc-André Ryter
Expert in Security Policy
Armed Forces Staff

CYBERSECURITY ROMANIA
- BUCHAREST TALKS -
Prima Ediție - 4 Iunie 2019

Why is Artificial Intelligence such a hot topic?



Prediction is difficult- particularly when it involves the future.

~ Mark Twain

AZ QUOTES

(R)Evolution is unavoidable

Higher speed

Complementarity man-machine

Potential

Improvement

Civil - military = same risks

Act on external providers

Disturb management/conduct

Use human errors

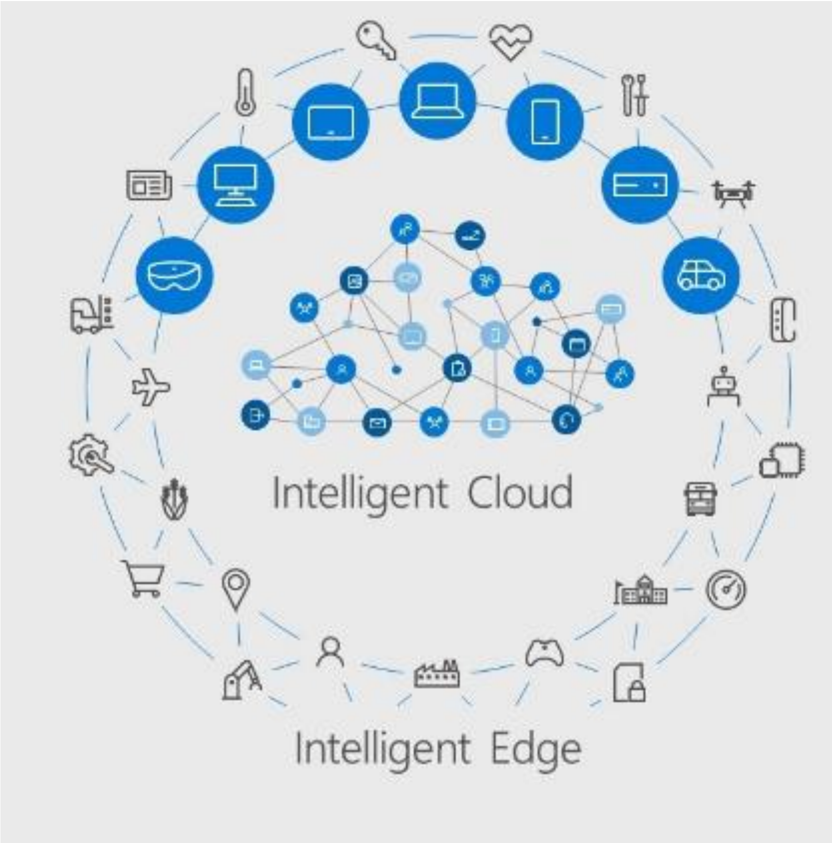
Create dysfunction

Target global systems/networks

Artificial Intelligence: why is it a problem?

© PARAMOUNT PICTURES

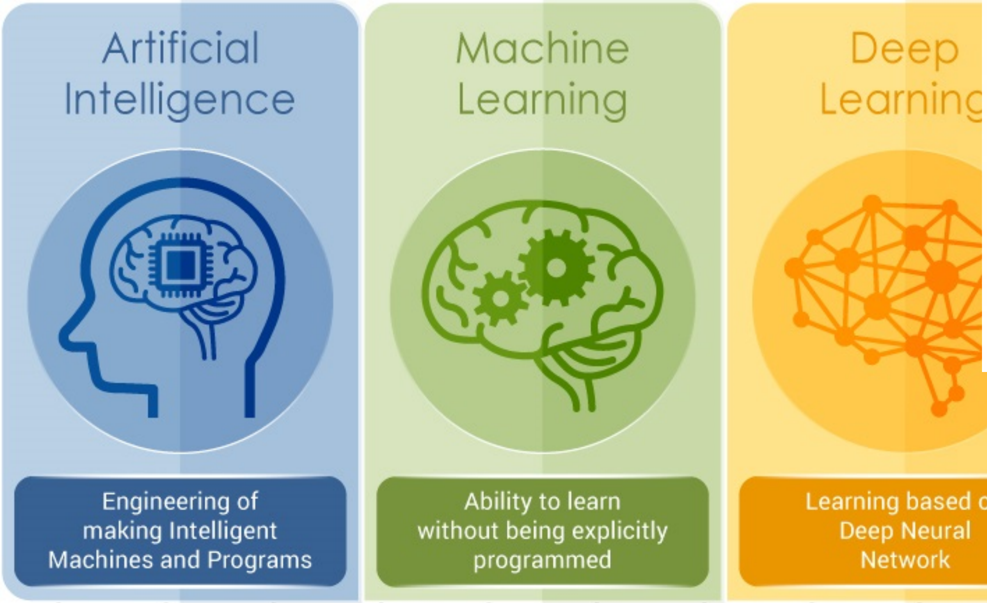
What comes in mind first



What is really dangerous

Artificial Intelligence: the real dangers

Uncontrolled automated learning


Artificial Intelligence

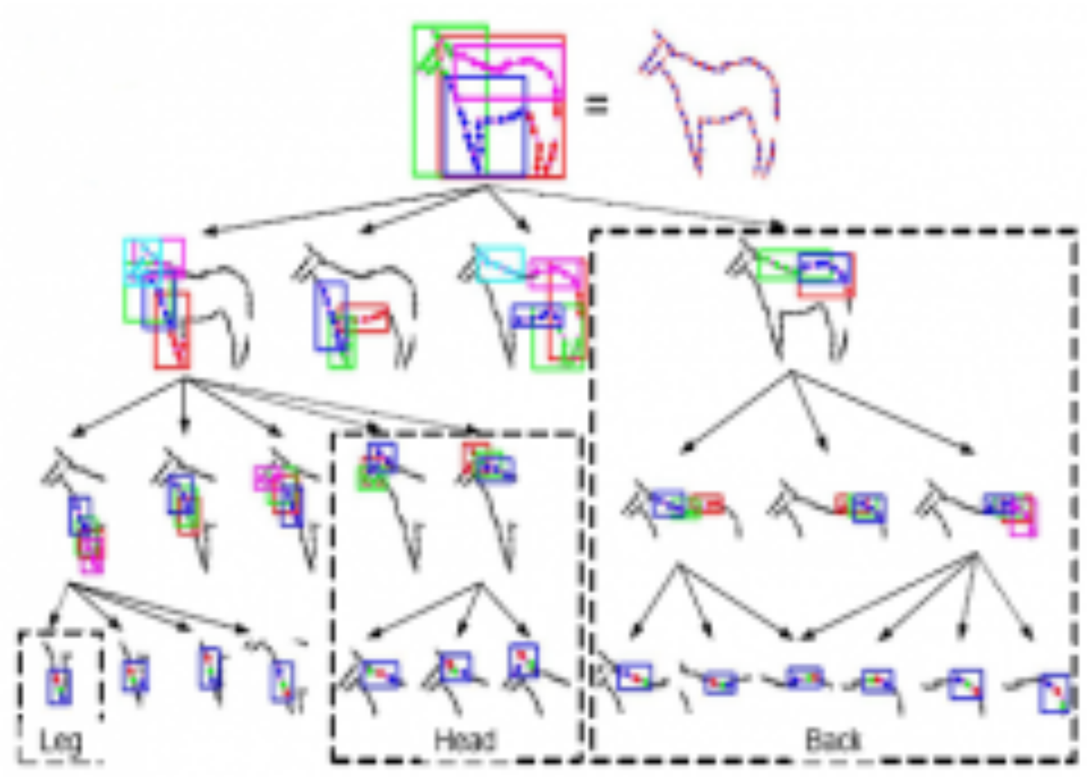
Engineering of making Intelligent Machines and Programs

Machine Learning

Ability to learn without being explicitly programmed

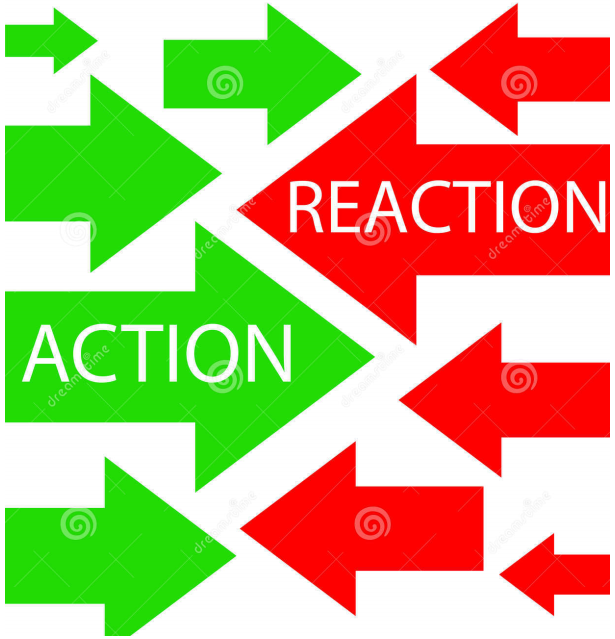
Deep Learning

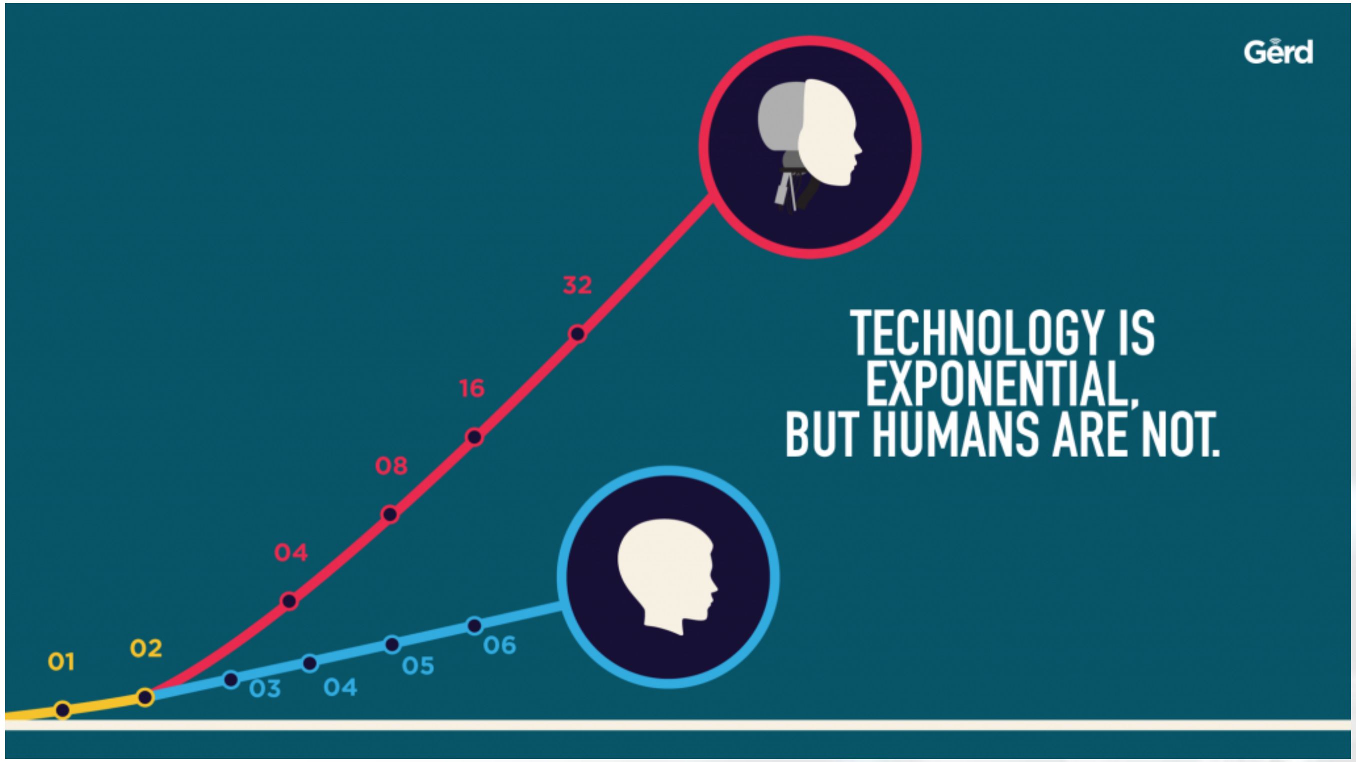
Learning based on Deep Neural Network



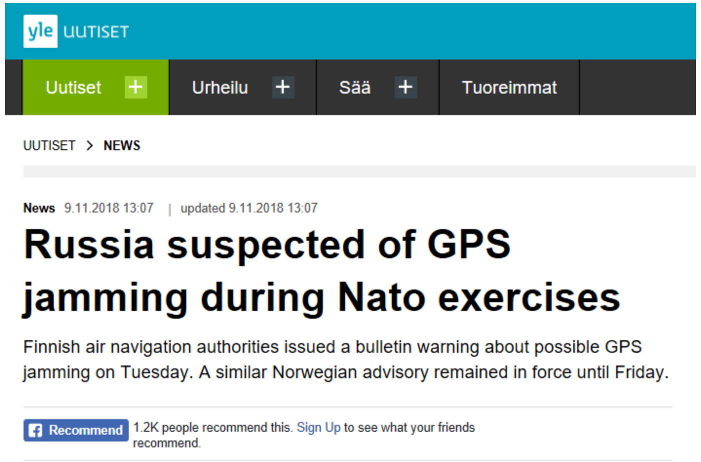
Artificial Intelligence: the real dangers

Very fast action-reaction





Artificial Intelligence: the real dangers


yle UUTISET
Uutiset +
Urheilu +
Sää +
Tuoreimmat
UUTISET > NEWS

News 9.11.2018 13:07 | updated 9.11.2018 13:07

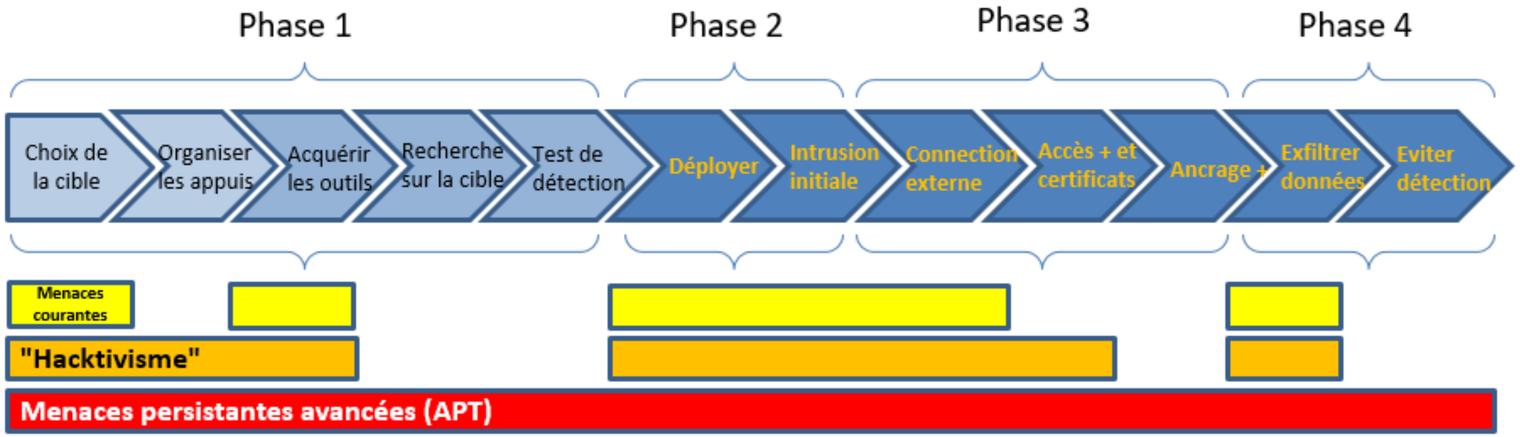
Russia suspected of GPS jamming during Nato exercises

Finnish air navigation authorities issued a bulletin warning about possible GPS jamming on Tuesday. A similar Norwegian advisory remained in force until Friday.

Recommend
1.2K people recommend this. Sign Up to see what your friends recommend.

New types of attacks (including chatting between computers)

Nature des menaces et phases



Phase 1: Choix de la cible, Organiser les appuis, Acquérir les outils, Recherche sur la cible, Test de détection

Phase 2: Déployer, Intrusion initiale

Phase 3: Connection externe, Accès + et certificats, Ancrage +

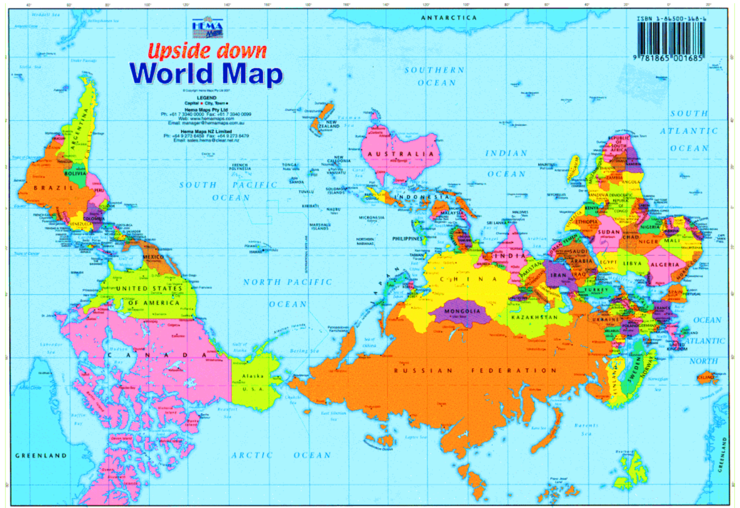
Phase 4: Exfiltrer données, Eviter détection

Menaces courantes

"Hacktivisme"

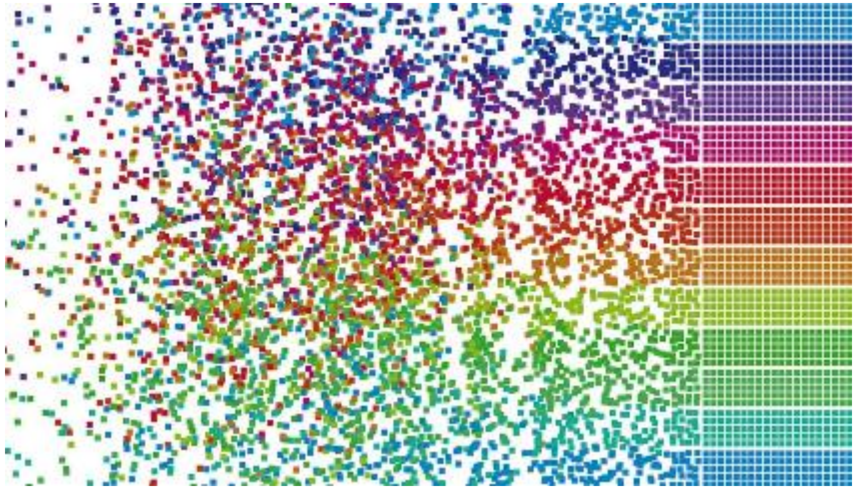
Menaces persistantes avancées (APT)

Artificial Intelligence: the real dangers



Available to many actors

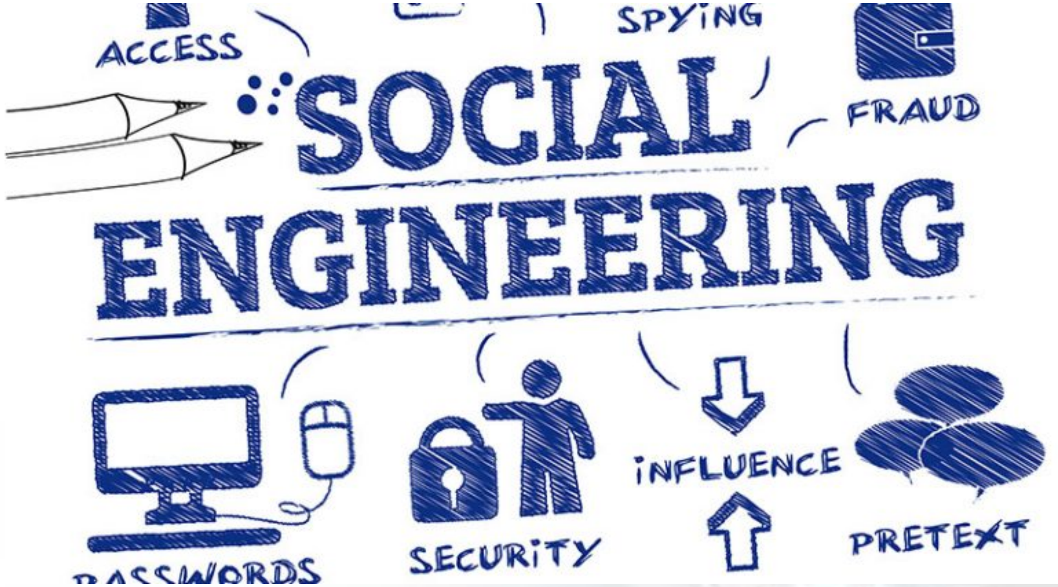
Artificial Intelligence: the real dangers



Connecting enormous amount of data

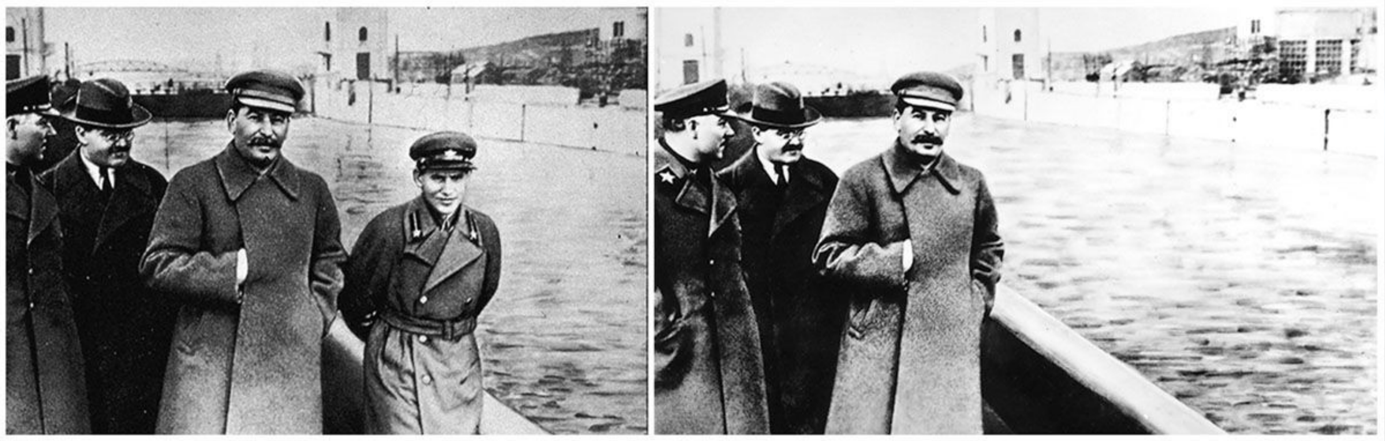
Artificial Intelligence: the real dangers

Improving social engineering

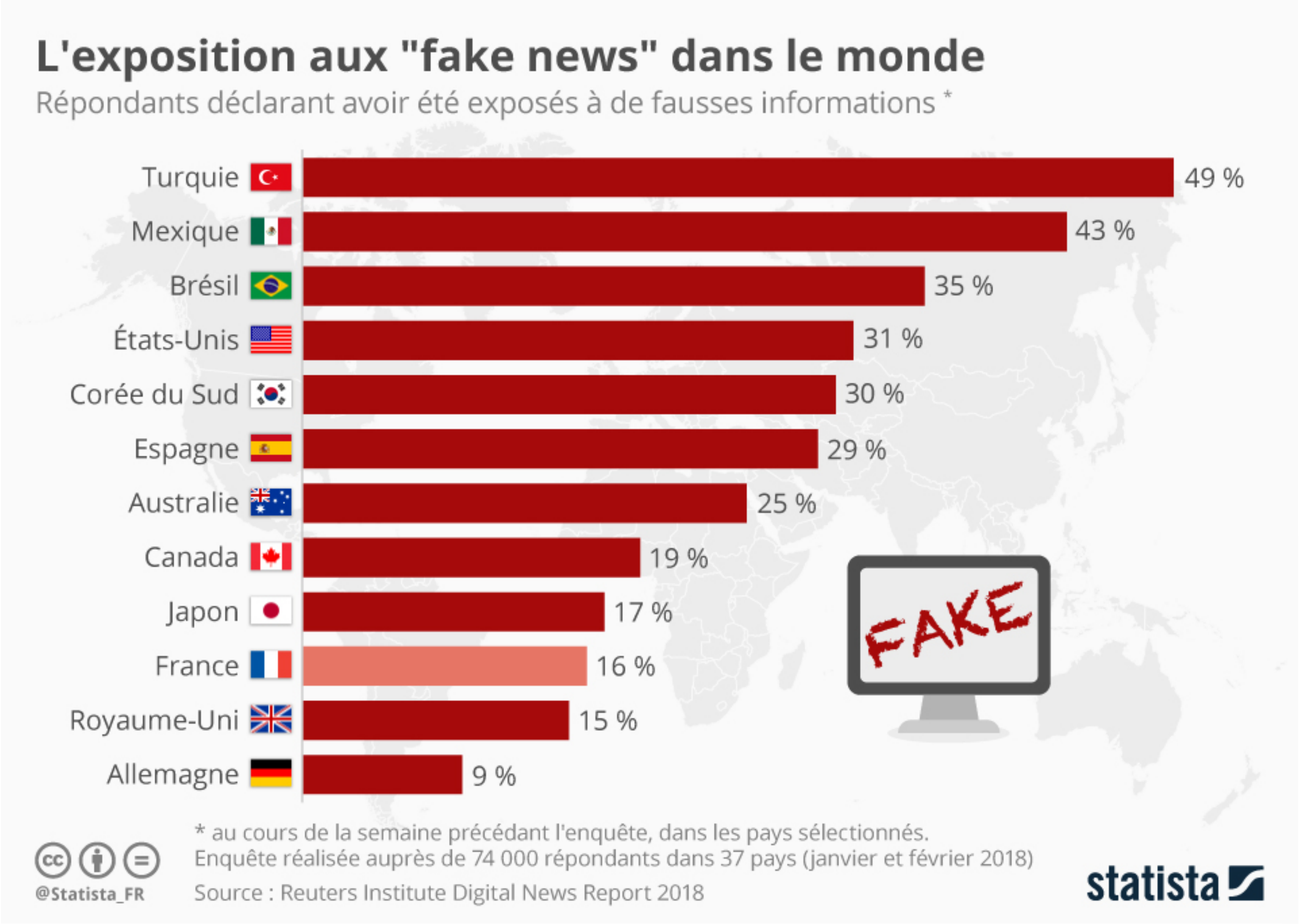


Artificial Intelligence: the real dangers

Creating falsified content (including videos)



Artificial Intelligence: the real dangers



L'exposition aux "fake news" dans le monde

Répondants déclarant avoir été exposés à de fausses informations *

* au cours de la semaine précédant l'enquête, dans les pays sélectionnés.
Enquête réalisée auprès de 74 000 répondants dans 37 pays (janvier et février 2018)

Source : Reuters Institute Digital News Report 2018

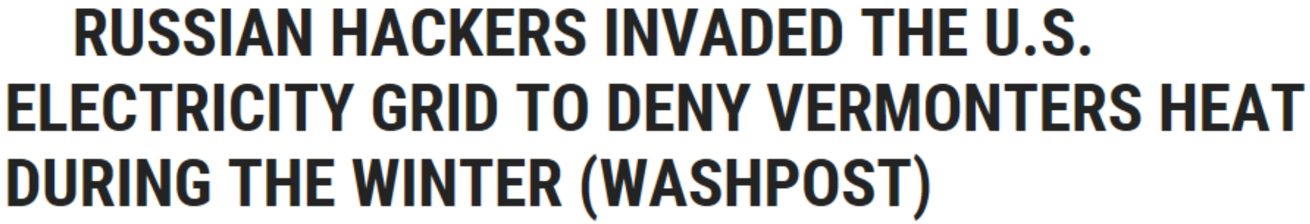
@Statista_FR statista

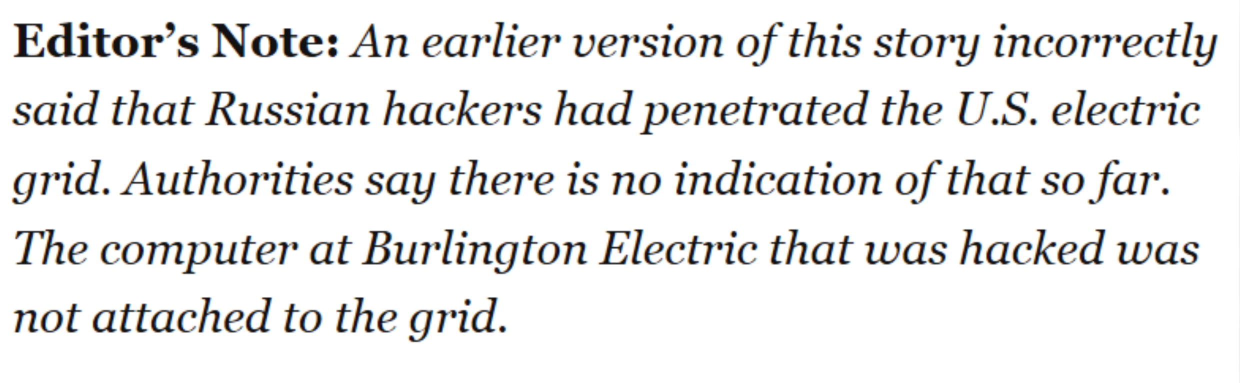
UN ÉTAT DOIT POUVOIR BLOQUER LES INFORMATIONS NUISIBLES.
VOUS VOYEZ ? JE VOUS AVAIS DIT QU'IL SERAIT D'ACCORD.
FAKE NEWS
KAK

Artificial Intelligence: the real dangers

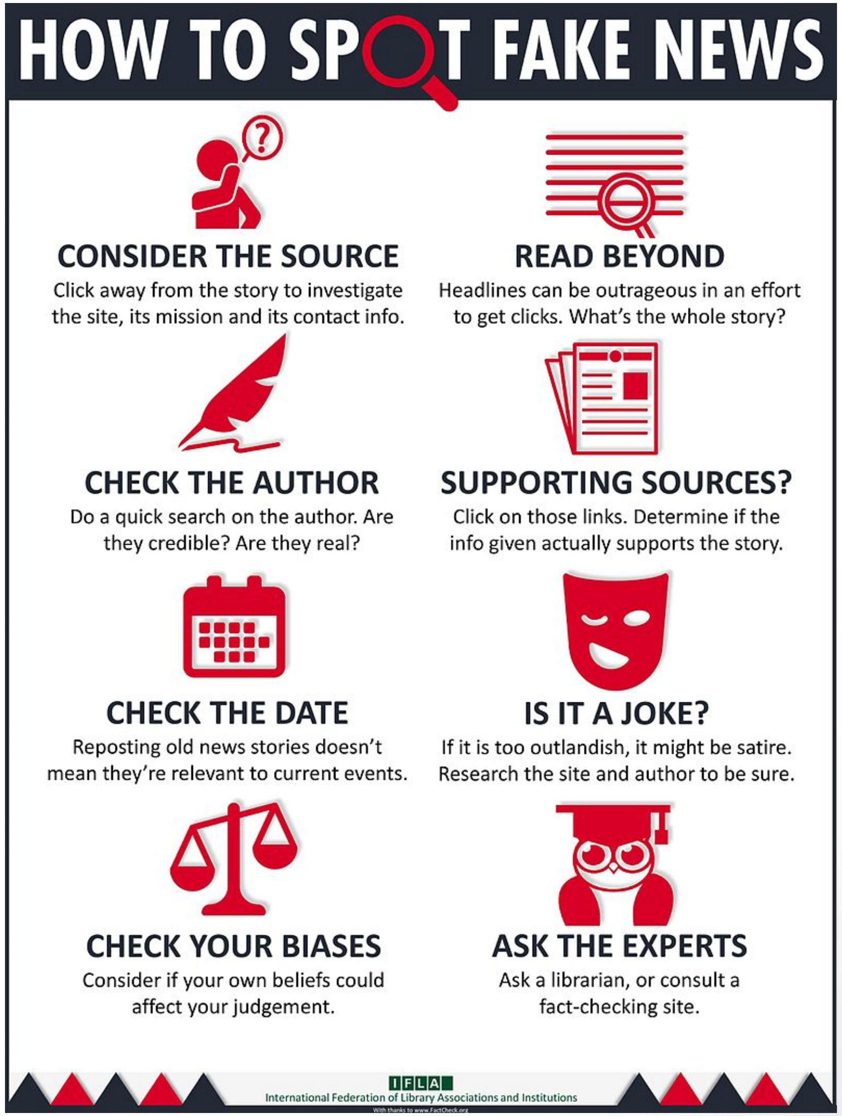
LIVE
breakyourownnews.com
BREAKING NEWS
NEW DOG AND DINOSAUR BREED
16:24
KID MAKES TUTORIAL ON HOW TO ACCESS THE NEWS ONLINE | TWO NEW IPHONES RE

December 2016:


RUSSIAN HACKERS INVADED THE U.S. ELECTRICITY GRID TO DENY VERMONTERS HEAT DURING THE WINTER (WASHPOST)


Editor's Note: *An earlier version of this story incorrectly said that Russian hackers had penetrated the U.S. electric grid. Authorities say there is no indication of that so far. The computer at Burlington Electric that was hacked was not attached to the grid.*

Artificial Intelligence: the real dangers



HOW TO SPOT FAKE NEWS

CONSIDER THE SOURCE
Click away from the story to investigate the site, its mission and its contact info.

READ BEYOND
Headlines can be outrageous in an effort to get clicks. What's the whole story?

CHECK THE AUTHOR
Do a quick search on the author. Are they credible? Are they real?

SUPPORTING SOURCES?
Click on those links. Determine if the info given actually supports the story.

CHECK THE DATE
Reposting old news stories doesn't mean they're relevant to current events.

IS IT A JOKE?
If it is too outlandish, it might be satire. Research the site and author to be sure.

CHECK YOUR BIASES
Consider if your own beliefs could affect your judgement.

ASK THE EXPERTS
Ask a librarian, or consult a fact-checking site.

IFLA
International Federation of Library Associations and Institutions
With thanks to www.FactCheck.org

Artificial Intelligence: the real dangers

Finding and using all vulnerabilities

Summary

Connecting enormous amount of data

Uncontrolled automated learning

Very fast action-reaction

Improving social engineering

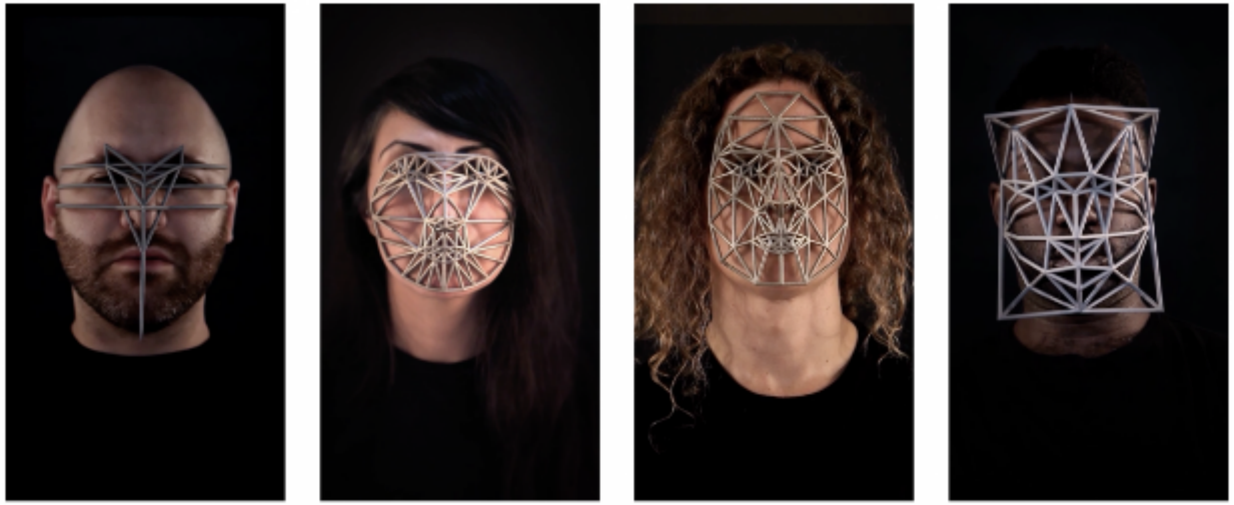
New types of attacks
(chatting between computers)

Creating falsified content
(videos)

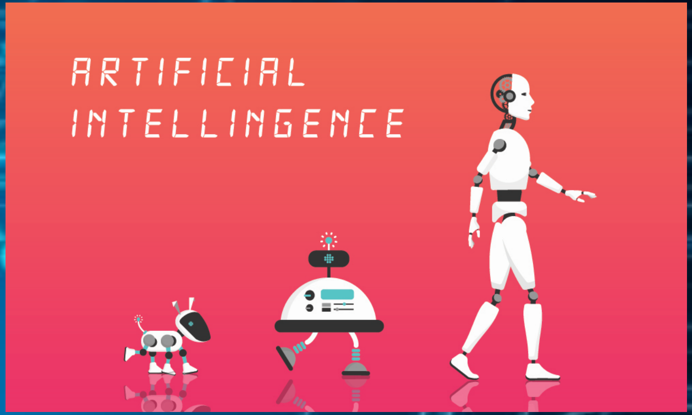
Available to many actors

Finding and using all vulnerabilities

Ways to cheat AI



Necessary security measures



Control development and use of AI

Necessary security measures

Permanent and collective effort

Necessary security measures

Train, again and again

Necessary security measures

Protect networks

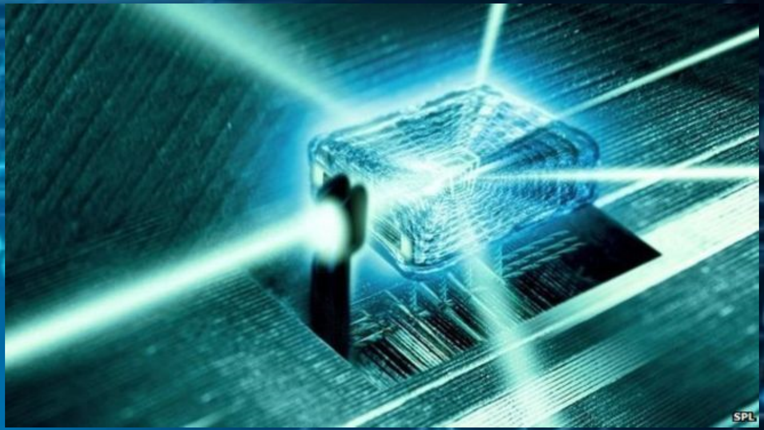
Necessary security measures

Handle new as well as old threats

Necessary security measures

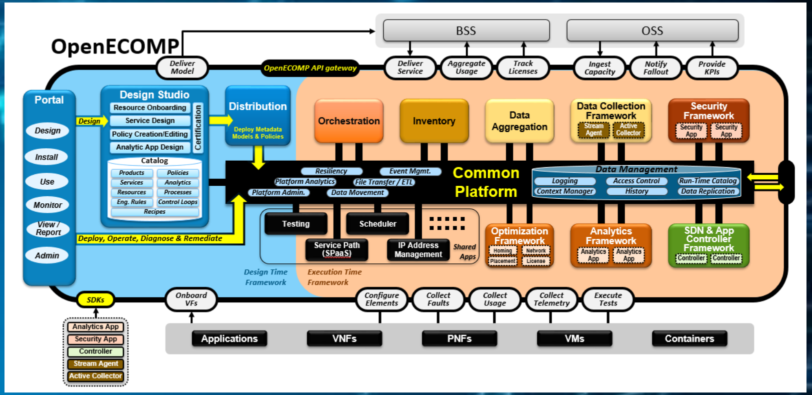
Improve resilience

Necessary security measures



Adapt to potential of machines

Necessary security measures



Promote multidimensional security (profiles)

Necessary security measures

ANTICIPATE
CHALLENGE
INTERPRET
DECIDE
ALIGN
LEARN

Implement flexible Leadership (anticipation)

Necessary security measures

Cooperation for security (information sharing)

Necessary security measures: Summary

Control development and use of AI

Permanent and collective effort

Train, again and again

Protect networks

Handle new as well as old threats

Improve resilience

Adapt to potential of machines

Promote multidimensional security (platform)

Implement flexible command

Cooperation for security (information sharing)

Contacts and Q&A

- marc-andre.ryter@vtg.admin.ch
- +41 58 463 16 70