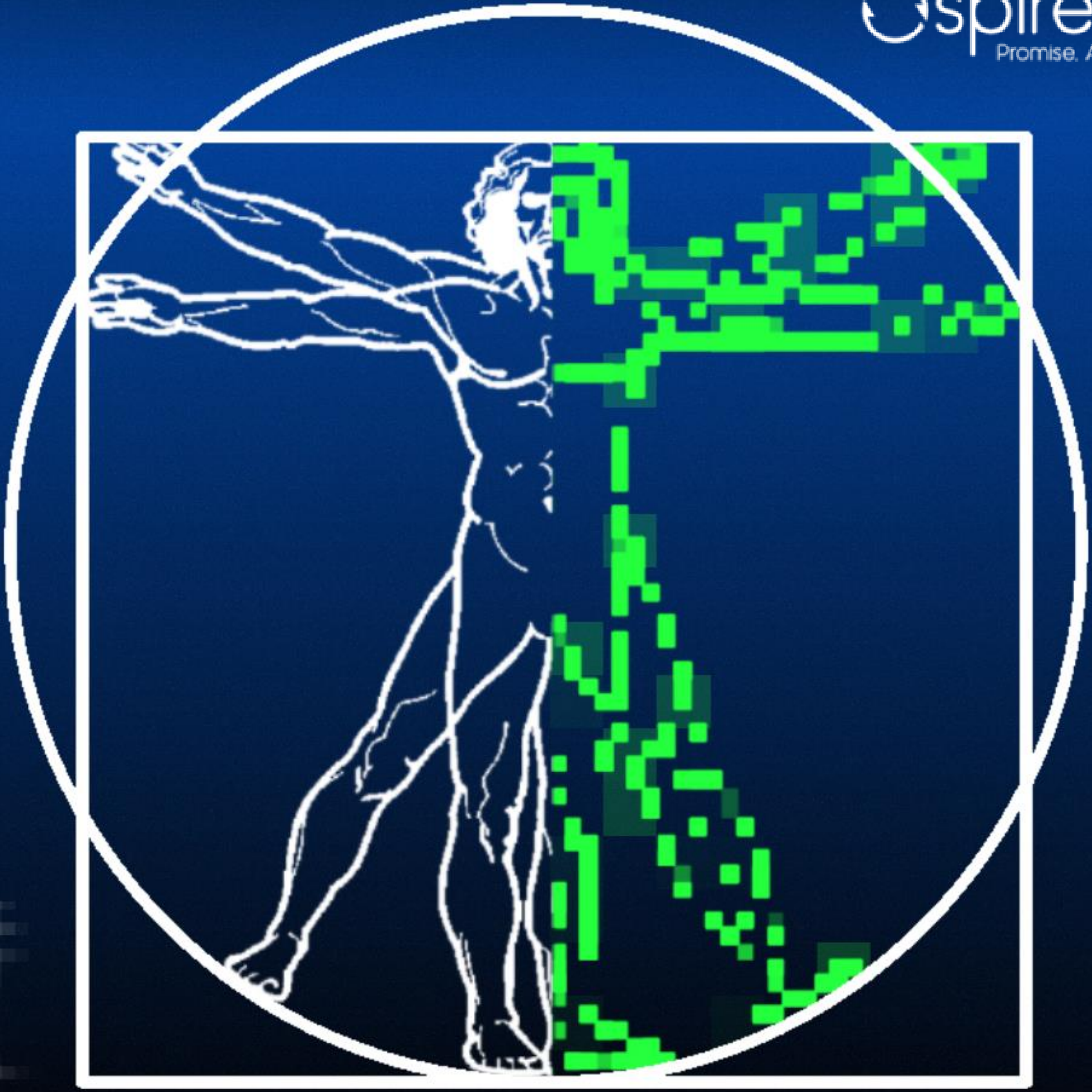
Hacking v2.0 in the 21st century

Are we ready for the security challenges of tomorrow?



THE SECURITY EVENT \ 7-9 SEPTEMBER 2021
NEC BIRMINGHAM UK

Aleksander Gorkowienko

Senior Managing Consultant
Spirent Communications

Welcome to the 21st century – the century of data

The man in the machine

The idea that the human mind one day will be transferred to the machine is not new.

“Digital preservation of consciousness” – is it only a science fiction or a possible **way to immortality?***

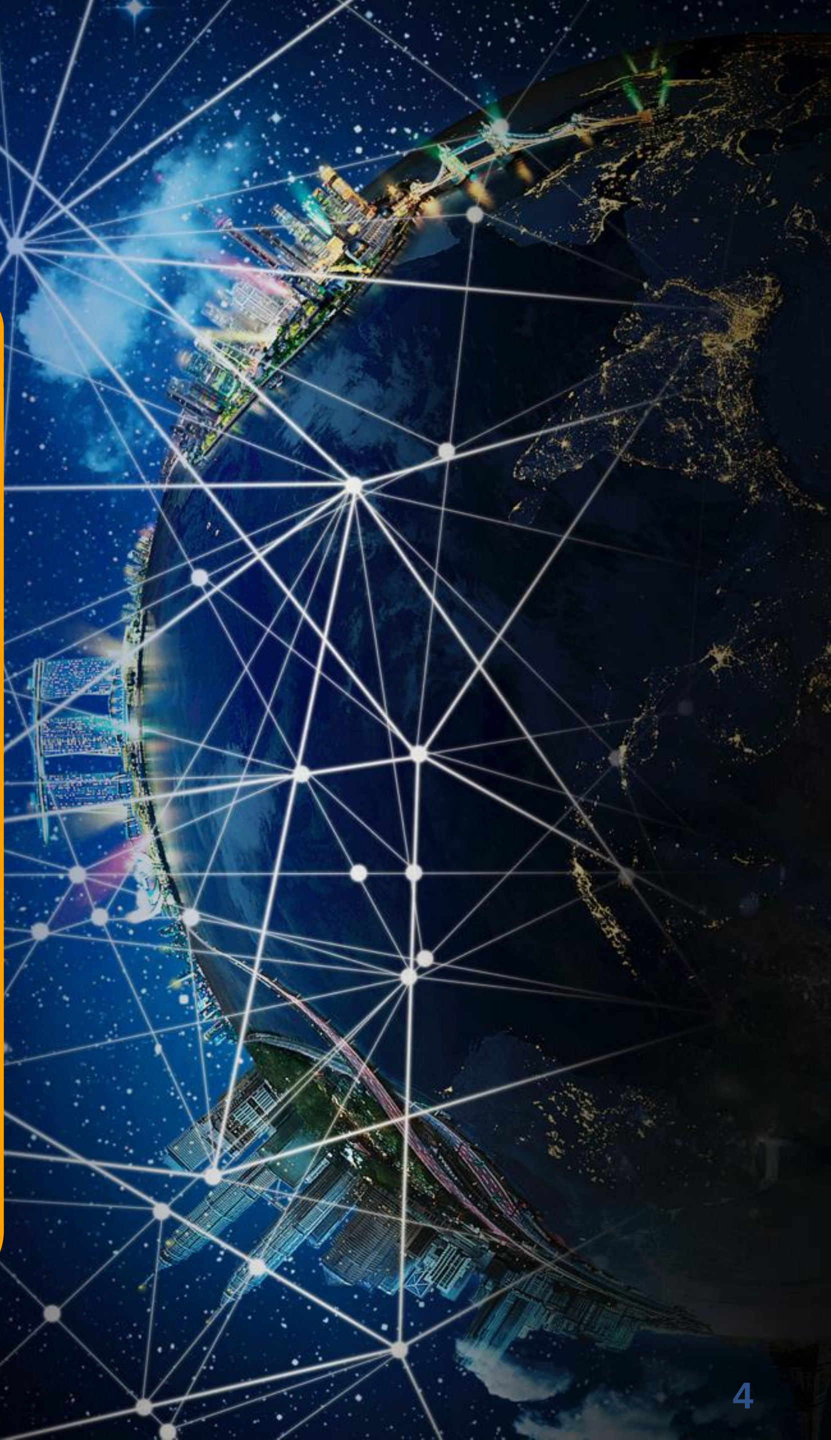
**probably as usual, it will be for the chosen few*

We are “not there yet”, but…

The more technology has advanced, **the greater is its impact** on our society.

Affected by technology

- All social aspects of life
- Working
- Travelling
- Shopping
- Communication
- Science and research
- Entertainment
- …



Signs that you live in the 21st century

- Practically **nothing these days can be done without the Internet**
- We are not living our life, ***we record it***
- We have a **hard time going off-line** and focusing on the present
- We cannot live a single day **without having a mobile phone**
- We **lose skills** for direct human interaction and we **lose creativity**
- **We share an enormous amount of information** about us online even not being aware of it
- We have much **fewer concerns about our privacy**

Signs that you live in the 21st century

"Nomophobia" - the fear of being without a mobile phone or being out of mobile phone signal range

- As of June 2019, **96% of Americans** own a cellphone of some kind.
- **66% of the population** shows signs of nomophobia
- **71%** of smartphone owners sleep with or next to their mobile phone on a typical night.
- The average smartphone owner will click, tap or swipe their phone **2,617 times a day**.
- In the 18 to 29 year old age category, **22%** of smartphone using respondents admitted to checking their device **every few minutes**.
- On average, people will spend **5 years and 4 months of their lifetimes** on social media.
- **33%** of teens spend more time socialising with close friends online rather than having in-person interaction.

https://www.slicktext.com/blog/2019/10/smartphone-addiction-statistics/

Our life becomes more digital

Information about you in a digital form

- **Citizenship data** (passport, biometry, police records)
- **Banking** (accounts, transactions, social status)
- **Property ownership** (property, mortgage, etc.)
- **Medical data** (digital health records, conditions, prescriptions, medication)
- **Search queries** (thoughts, questions, interests, worries, problems, desires)
- **Mobile communication** (phone records, text messages, geolocation)
- **Social media** (thoughts, emotions, interests, hobby)
- **Wearables** (physical activity, health, sleep pattern, emotional state, geolocation)

This digital YOU who becomes a target

Information about you in a digital form

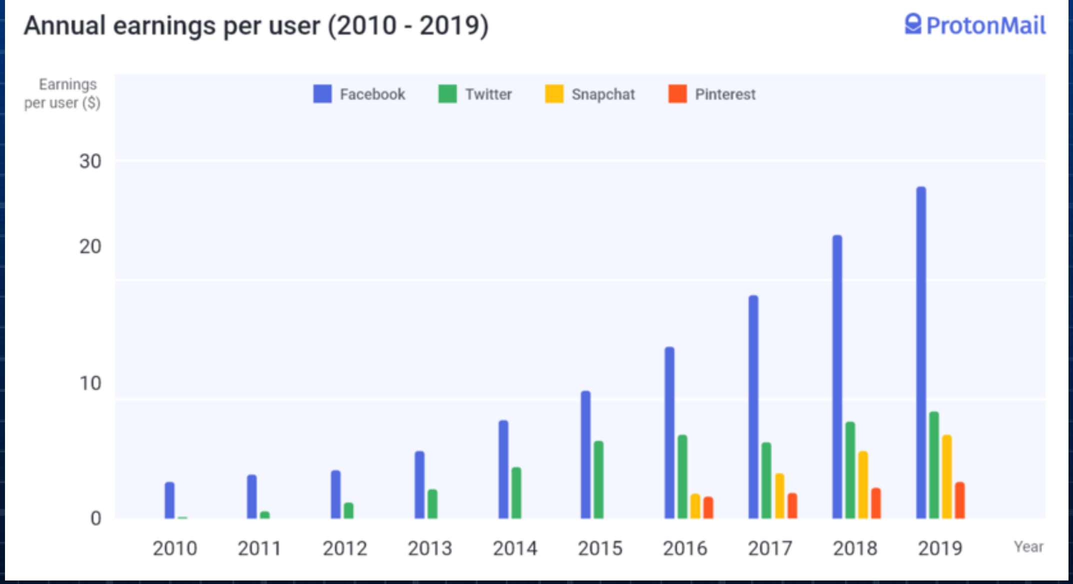
- **Citizenship data** (passport, biometry, police records)
- **Banking** (accounts, transactions, social status)
- **Property ownership** (property, mortgage, etc.)
- **Medical data** (digital health records, conditions, prescriptions, medication)
- **Search queries** (thoughts, questions, interests, worries, problems, desires)
- **Mobile communication** (phone records, text messages, geolocation)
- **Social media** thoughts, emotions, interests, hobby)
- **Wearables** (physical activity, health, emotional state, geolocation)

Hacking systems which know us better than we know ourselves

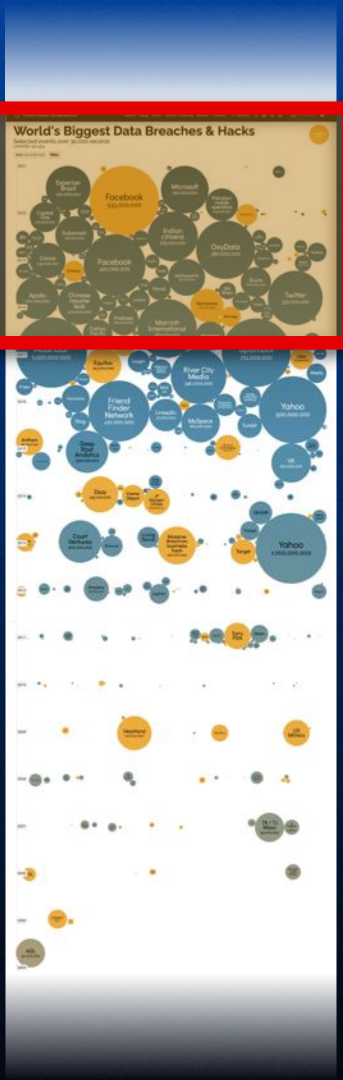
How are big companies collecting the data?

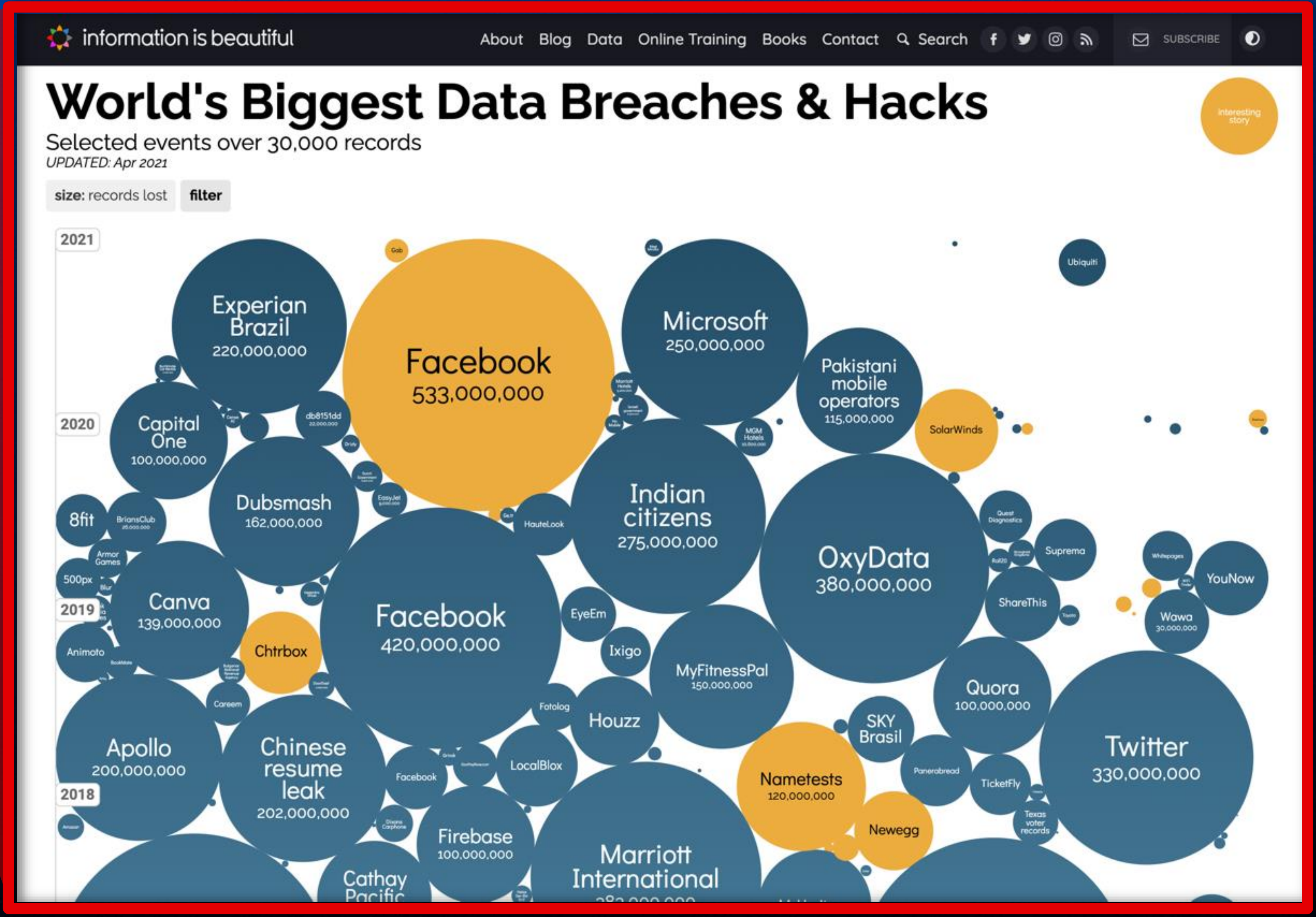
Big Brother is tracking your every digital step

- Links which you click (obvious), IP, cookies, supercookies, time zone, tracking pixels, browser fingerprint (system metrics, CPU, fonts, etc.), canvas or WebGL fingerprint, etc.
- Your social connections, links, references to you
- Search queries
- Time you spend on the webpage ("ingesting" content)
- Speed and depth of scrolling through the content
- All digital emotions: "likes", smiles, etc.
- Content you share (text, digital media)
- Geolocation data
- Cross-device tracking (deterministic and probabilistic)
- Your voice and video recordings and facial recognition



The collected data about us is never safe





information is beautiful

About Blog Data Online Training Books Contact Search SUBSCRIBE

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

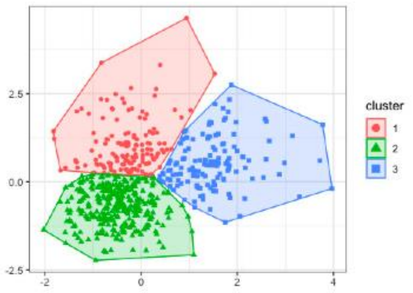
UPDATED: Apr 2021

size: records lost filter

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Your digital profile can be used against you

Behavioural data

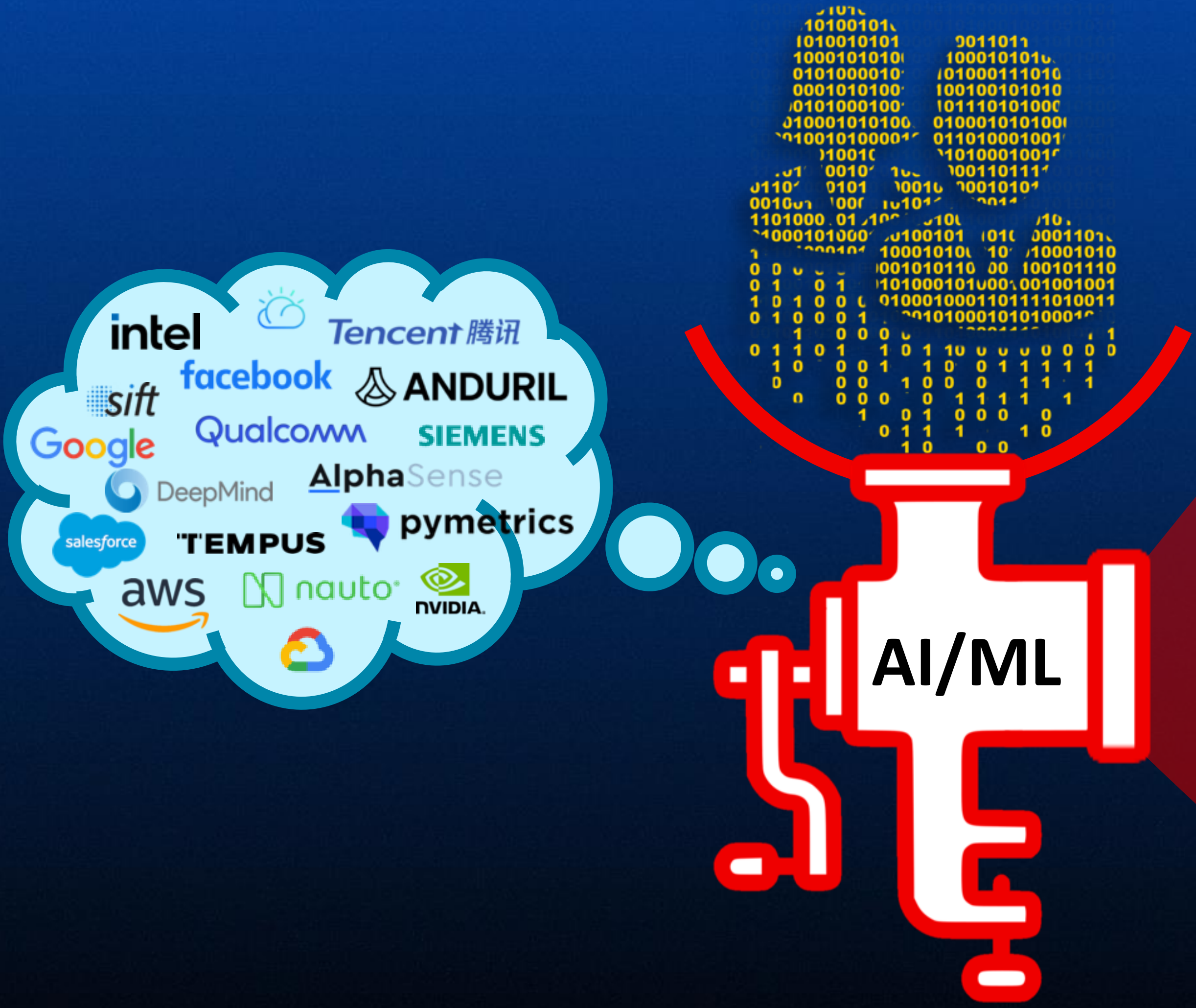


- Statistical analysis
- Analysis by AI/ML
- High-dimensional data mining

YOUR DIGITAL PROFILE

- Who you are
- What you are
- Behavioural patterns
- “Social score”
- Professional skills
- Political preferences
- Desires and fantasies
- Fears
- Wishes
- Doubts
- …

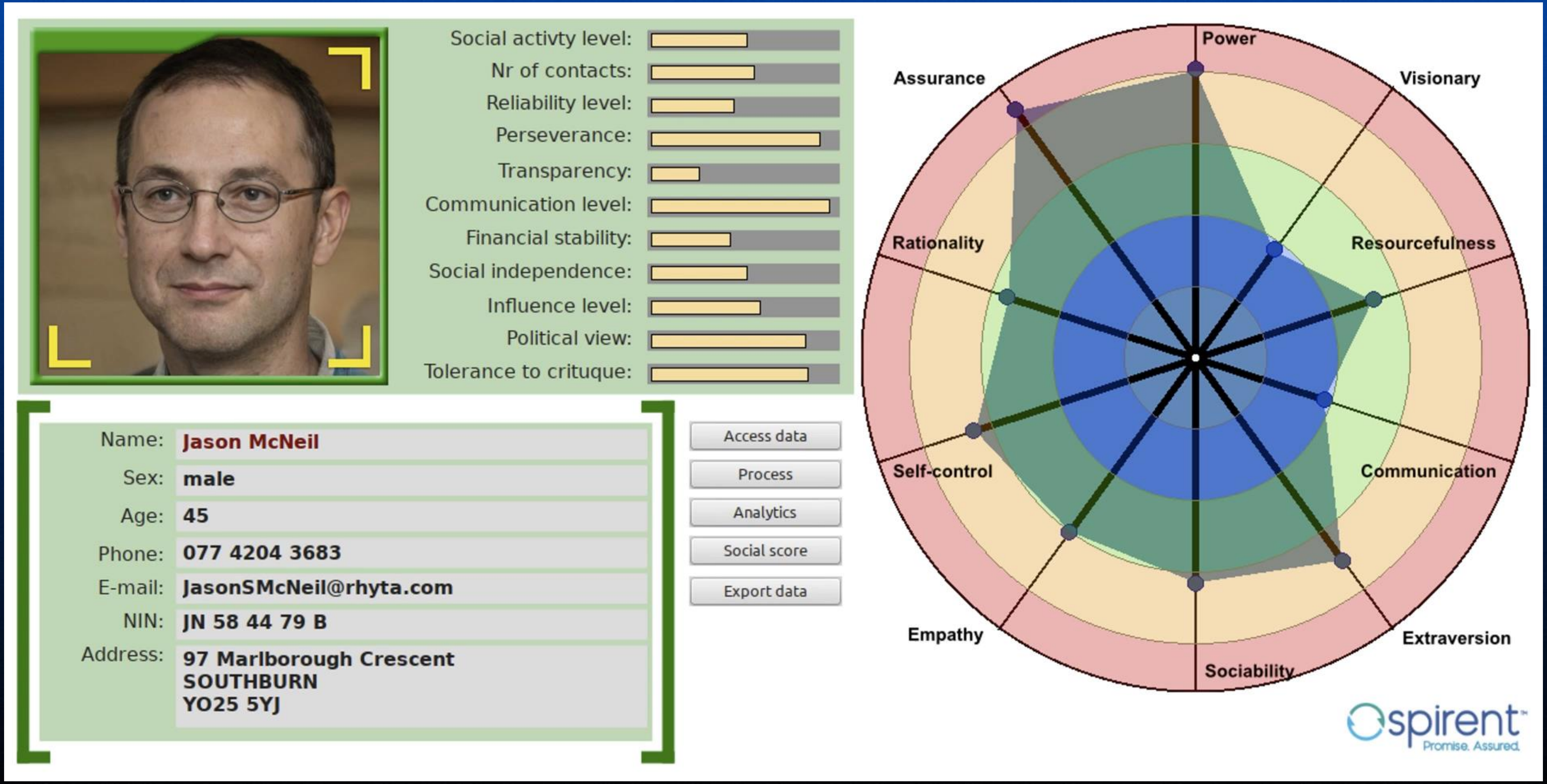
What if all this data is processed by AI/ML?



Manipulation techniques “tailored” to you

- Abusing your behavioural patterns
- Controlling the facts that you like
- Playing with the information that you don’t like
- Calculating your “sweet spot” for feeding (any) information
- Playing with your fears or doubts
- Manipulating your emotional states

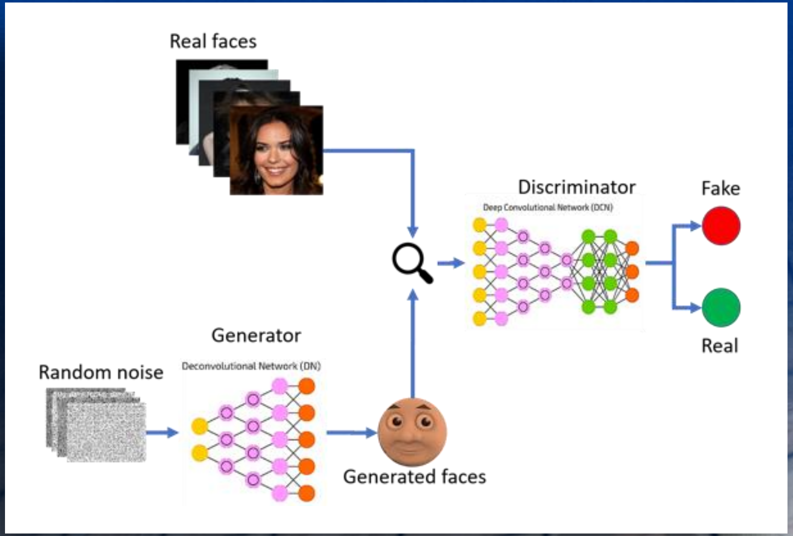
YOU become a (valuable!) product



Name:	Jason McNeil
Sex:	male
Age:	45
Phone:	077 4204 3683
E-mail:	JasonSMcNeil@rhyta.com
NIN:	JN 58 44 79 B
Address:	97 Marlborough Crescent SOUTHBURN YO25 5YJ

Fun fact: all those images were generated by AI

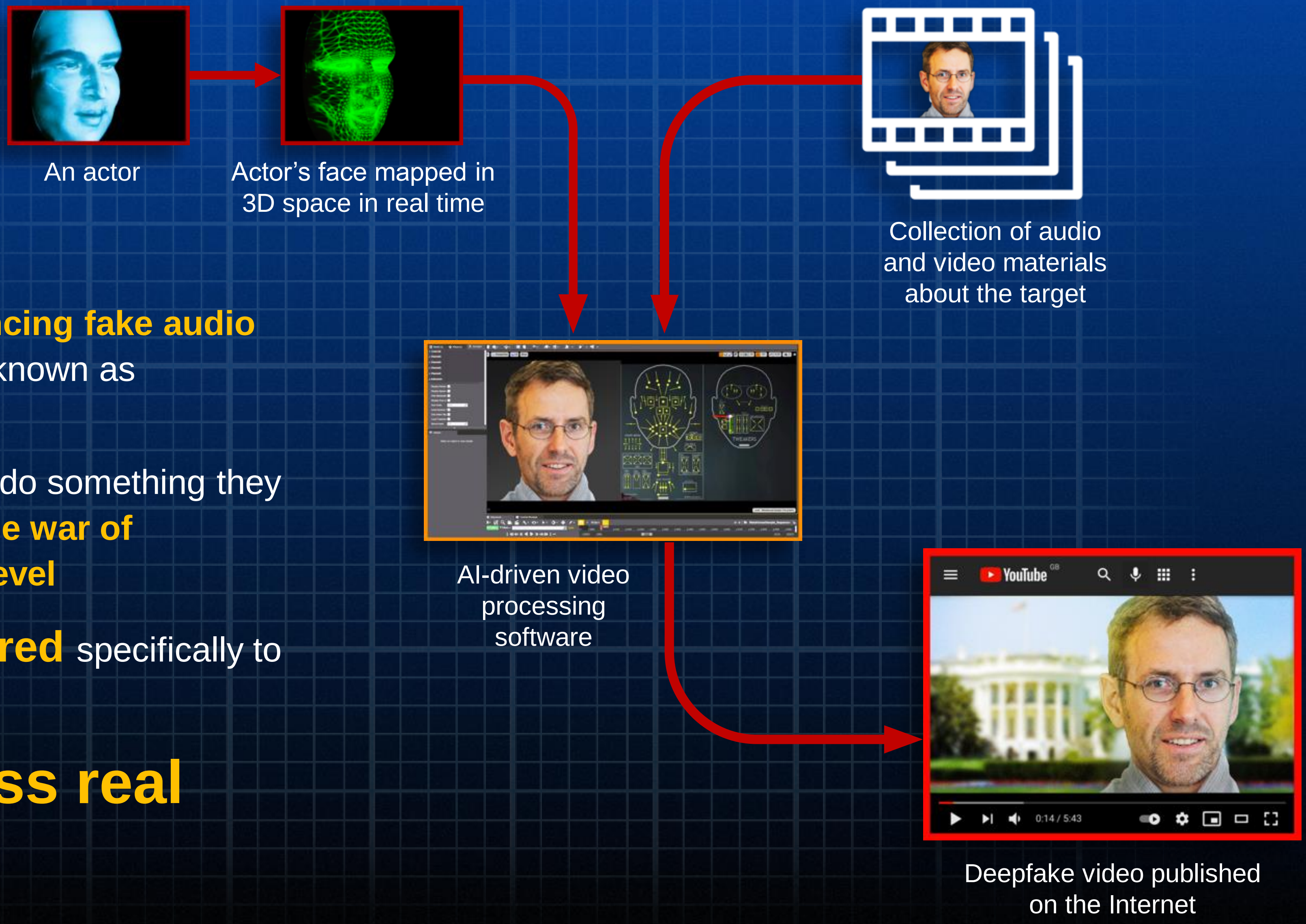
We used GAN AI (Generative Adversarial Network)



A generative adversarial network **(GAN)** is a new class of AI/ML frameworks. Two neural networks endlessly contest with each other in a kind of game (a form of a zero-sum game, where one agent's gain means the other agent's loss).

When seeing is no longer believing

- AI/ML could make creating **convincing fake audio and video** relatively easy. This is known as “deepfakes”.
- Making a person appear to say or do something they did not has the potential to **take the war of disinformation to a whole new level**
- **What if the deepfake is tailored** specifically to you based on your profile?
- **What if we can dismiss real events as fake?**



An actor

Actor’s face mapped in 3D space in real time

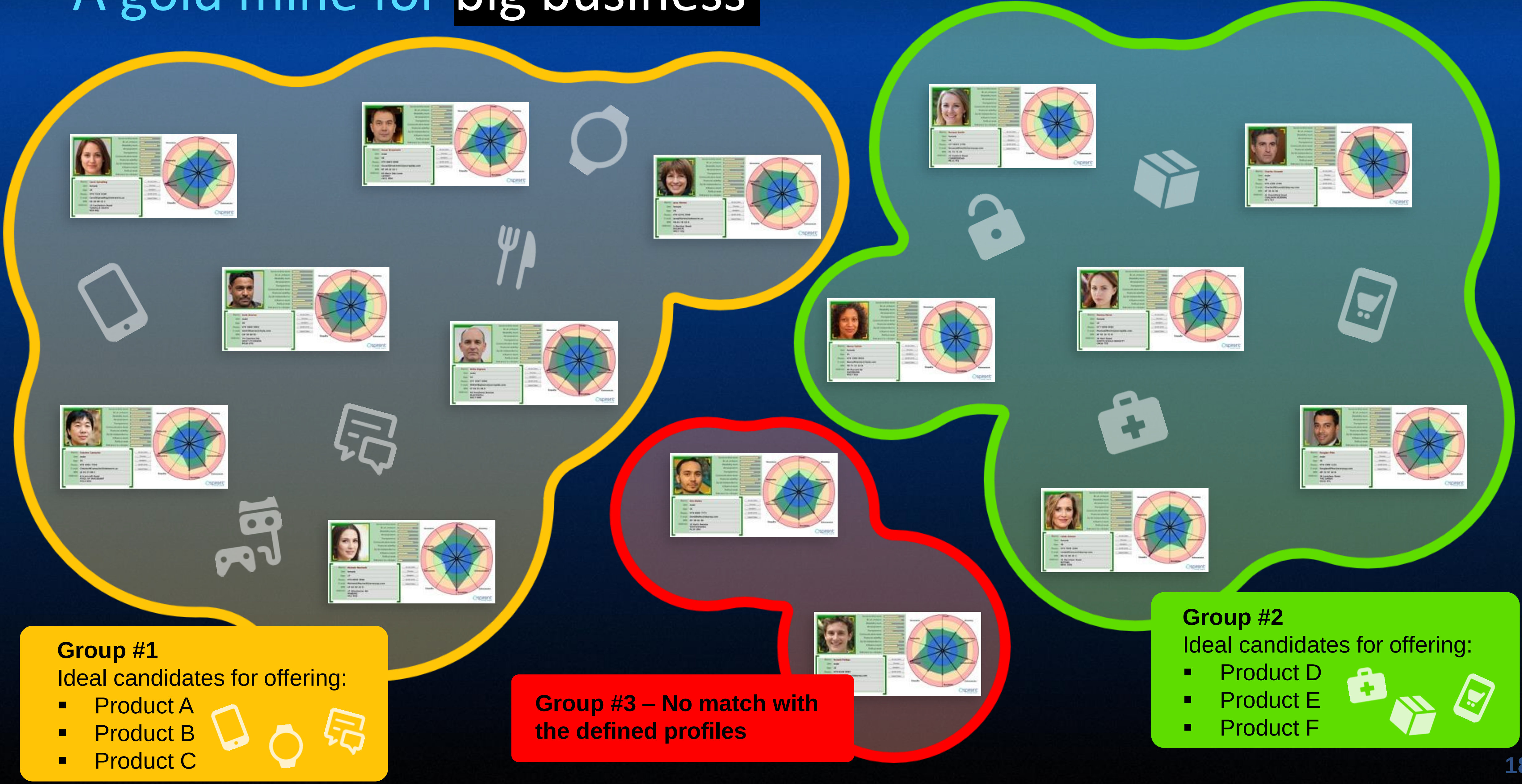
Collection of audio and video materials about the target

AI-driven video processing software

Deepfake video published on the Internet

The data about you is a gold mine!

A gold mine for big business



Group #1
Ideal candidates for offering:

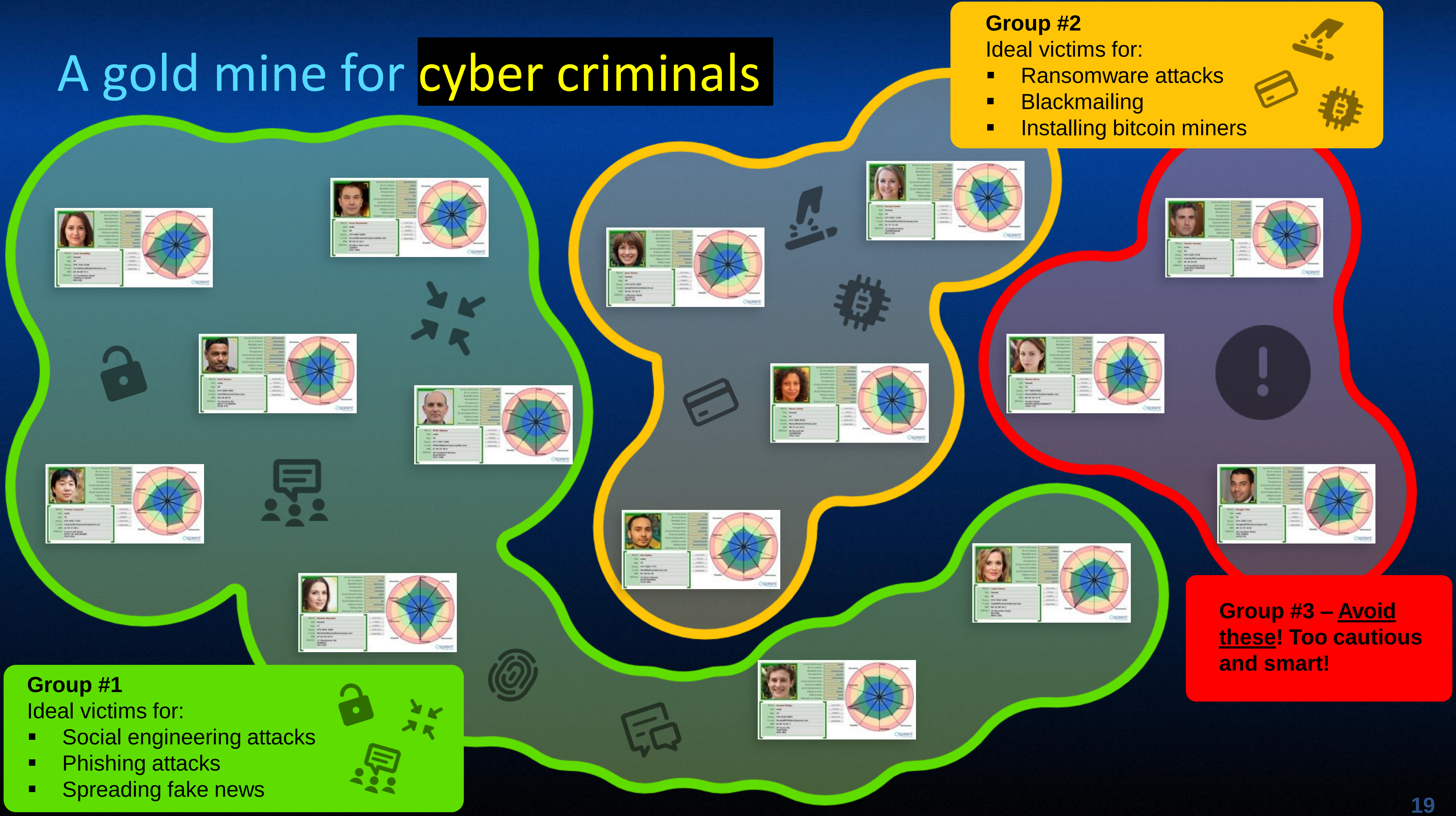
- Product A
- Product B
- Product C

Group #3 – No match with the defined profiles

Group #2
Ideal candidates for offering:

- Product D
- Product E
- Product F

A gold mine for cyber criminals



Group #2
Ideal victims for:
- Ransomware attacks
- Blackmailing
- Installing bitcoin miners

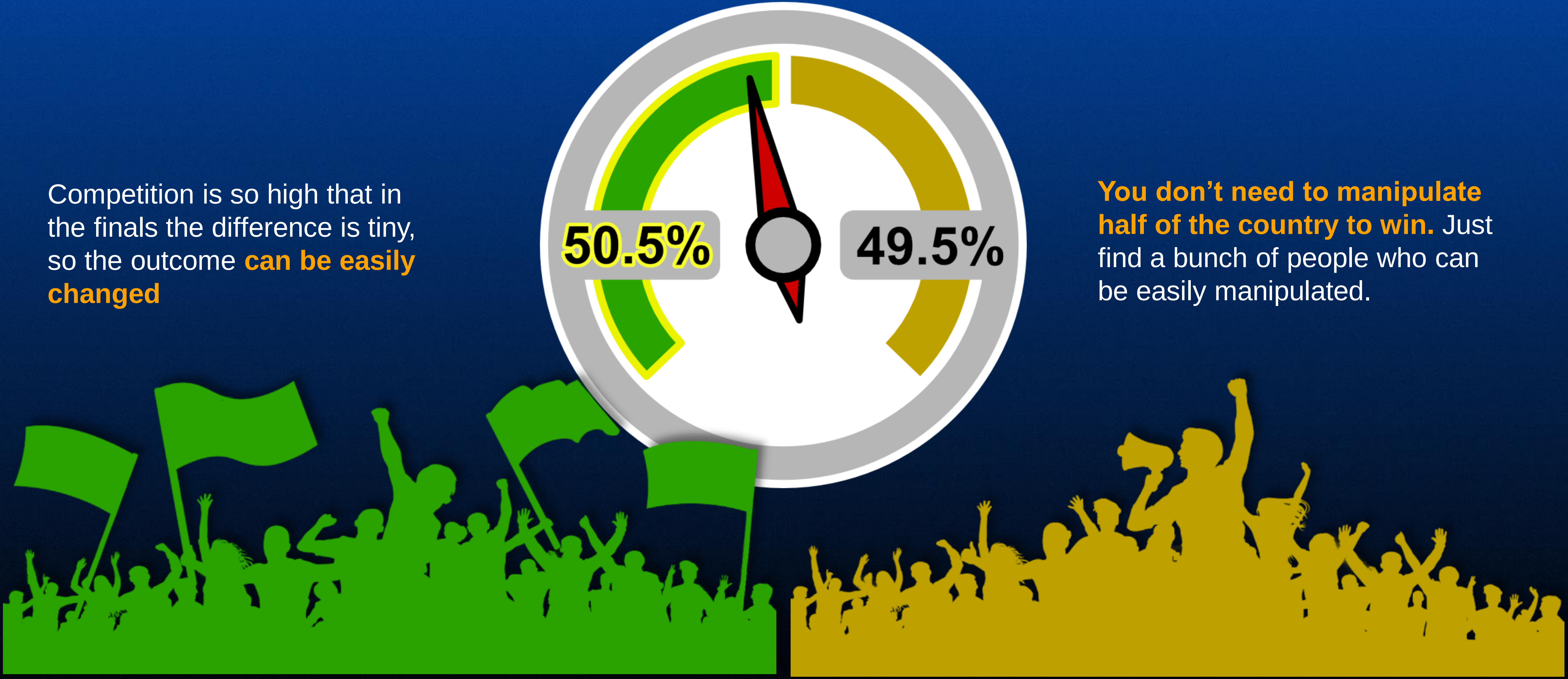
Group #3 – Avoid these! Too cautious and smart!

Group #1
Ideal victims for:
- Social engineering attacks
- Phishing attacks
- Spreading fake news

Changing the political course of the nation

Easier than you think!

Competition is so high that in the finals the difference is tiny, so the outcome **can be easily changed**

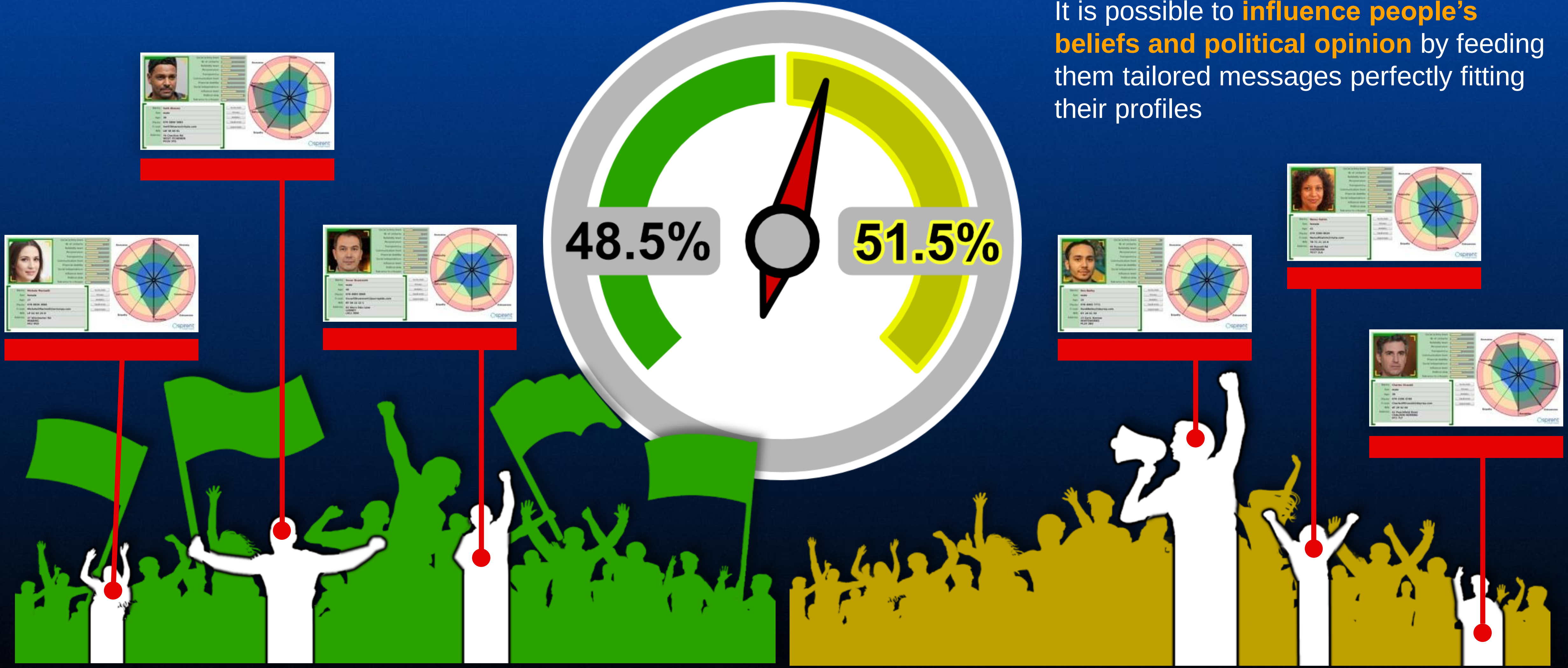


You don't need to manipulate half of the country to win. Just find a bunch of people who can be easily manipulated.

Changing the political course of the nation

Easier than you think!

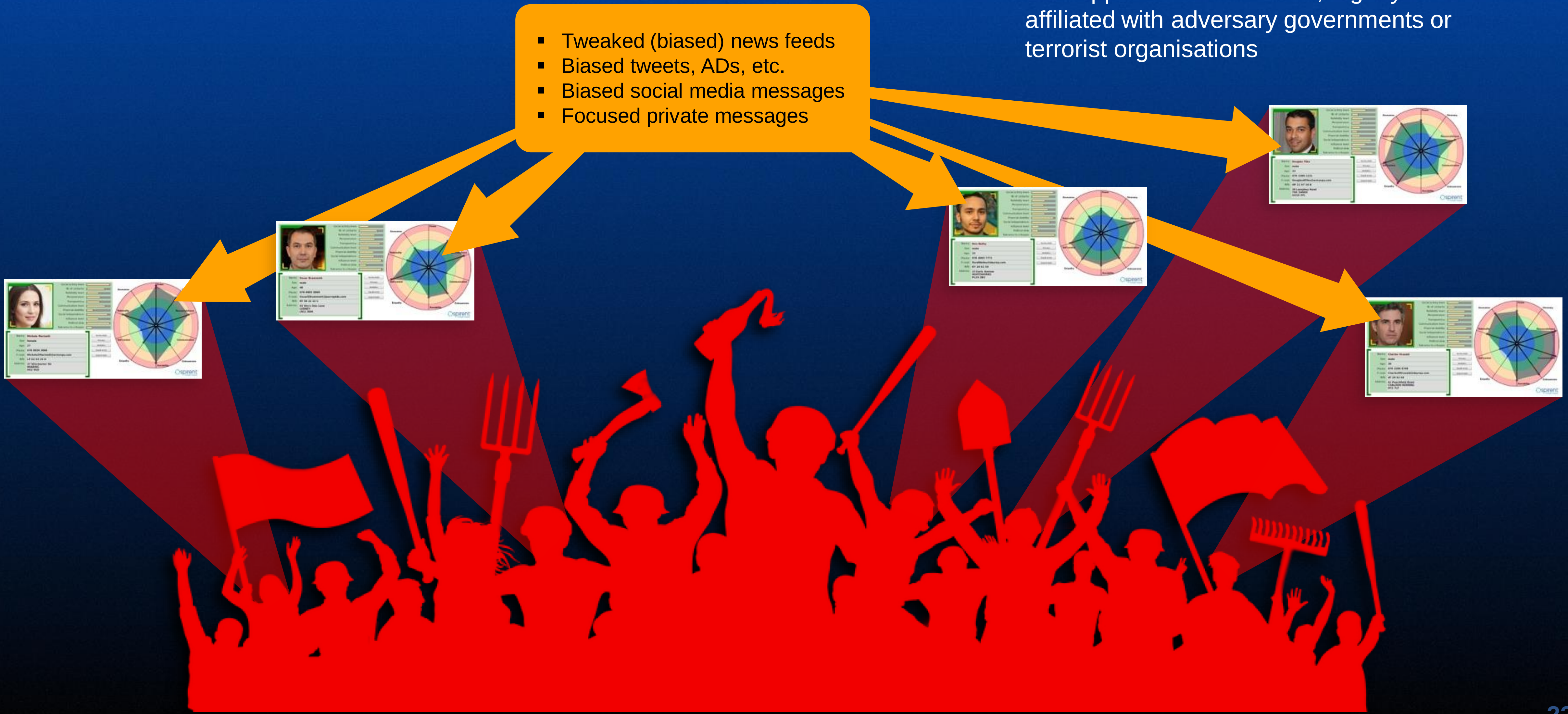
It is possible to **influence people’s beliefs and political opinion** by feeding them tailored messages perfectly fitting their profiles



Radicalisation of society

Easier than you think!

This approach can be used, e.g. by hackers affiliated with adversary governments or terrorist organisations



- Tweaked (biased) news feeds
- Biased tweets, ADs, etc.
- Biased social media messages
- Focused private messages

Balancing life on the grid

Measuring and scoring our paths in life

There are multiple tracking and scoring systems already

- Credit scoring
- Car insurance no-claim discount system
- Driving license penalty points
- Tracking, blacklisting and reward systems on all major websites
- Point-based immigration system
- Point-based job applications
- Reward systems in online games
- Reward system in online shopping websites and sales platforms
- COVID tracking applications
- Online reviews

What if all that can be combined in a single **unified score** you carry through your whole life?

Dreaming about nationwide social rating

Science-fiction or reality?

- Imagine this: everything you can do in life, every move and interaction - all is reduced to a single rating scale.
- A high rating opens many doors and opportunities for you.
- A low rating will shut you off from the rest of society.
- **All actions in your life are tracked.** They increase or decrease your score depending on what your actions are.
- The system can be used for individuals and also for companies and organisations.

Scoring our paths in life

Science-fiction or reality?

▲ **What can improve your social score?**

- Paying bills on time
- Good social behaviour
- Donation to charities

Rewards:

- Discounts on energy bills
- Better interest rates with banks
- Various discounts, e.g. on car insurance
- Renting things without deposits

▼ **What can bring down your score?**

- Bad driving habits
- Debts
- Bad online behaviour (can you quantify it btw?)
- Buying cigarettes and alcohol
- Travelling without a ticket
- Stealing electricity

Punishments:

- Travel bans
- Slow Internet
- Ban from higher education
- High interest rates with banks, no discounts
- Ban from business-class tickets or services
- Ban from luxury hotels and entertainment

A system ripe for manipulation

- First question: **who operates and curates the system?**
- Many rating systems used today are built on large volumes of historical data and AI/ML models that predict the future behaviour and successes of system participants
- The system can be abused by various artificial manipulations, aiming e.g. lowering someone's score for malicious purposes
- System can leak sensitive information about its users
- System using automated/biometric recognition (e.g. featuring AI/ML algorithms) can be vulnerable to manipulation

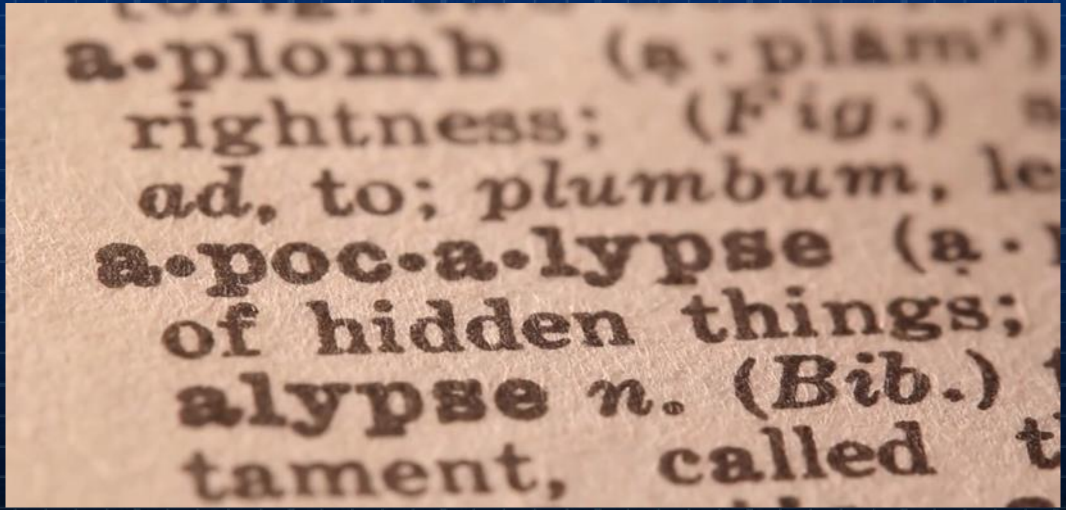
The fabric on this garment is designed to trigger Automated License Plate Readers (ALPR) in European Union countries, adding dummy and unhelpful data to the systems

A system ripe for manipulation

- Can the amount of Instagram followers or YouTube subscribers affect one’s success in business and in life? **Absolutely!**
- Could fake negative on-line reviews affect your business? Unfortunately **yes!**
- A **social rating can become a second currency** where, by manipulating the mechanisms used for establishing the rating, your score can be converted into real money and vice versa by criminals.

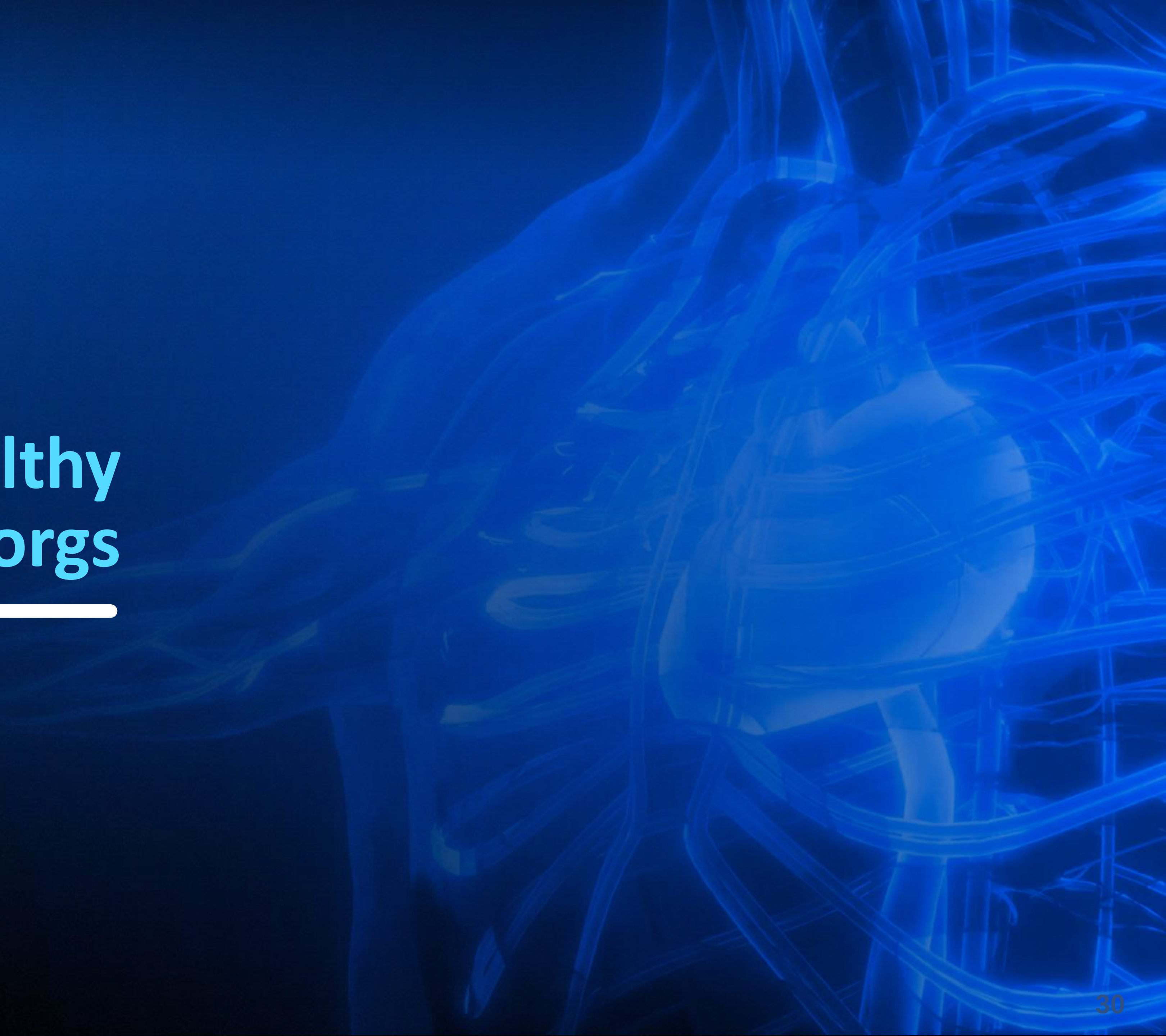
Consequences? Unpredictable.

It is hard to predict the consequences of a social scoring system that can determine your present and your future while being simultaneously easy to manipulate and vulnerable to cyber attacks.



a·plomb (a·plam')
rightness; (Fig.)
ad, to; plumbum, le
a·poc·a·lypse (a·
of hidden things;
alypse n. (Bib.)
tament, called t

Not so healthy cyborgs



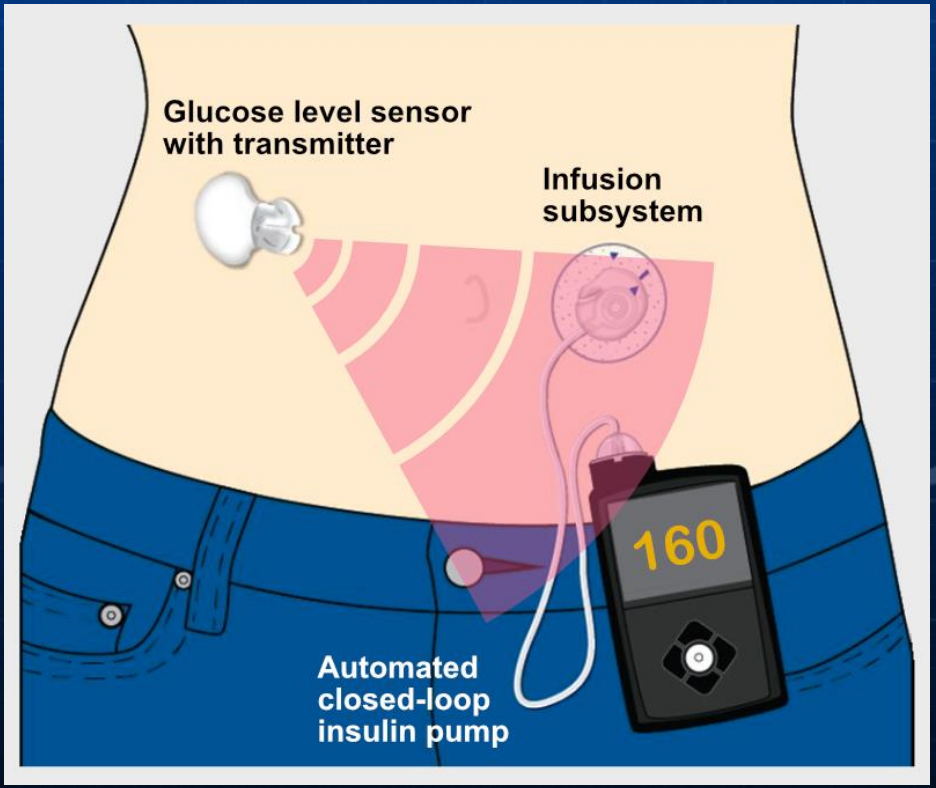
Devices can help with our health

Monitoring:

- Temperature
- Blood pressure
- Pulse and oxygen level
- Blood glucose level

Controlling:

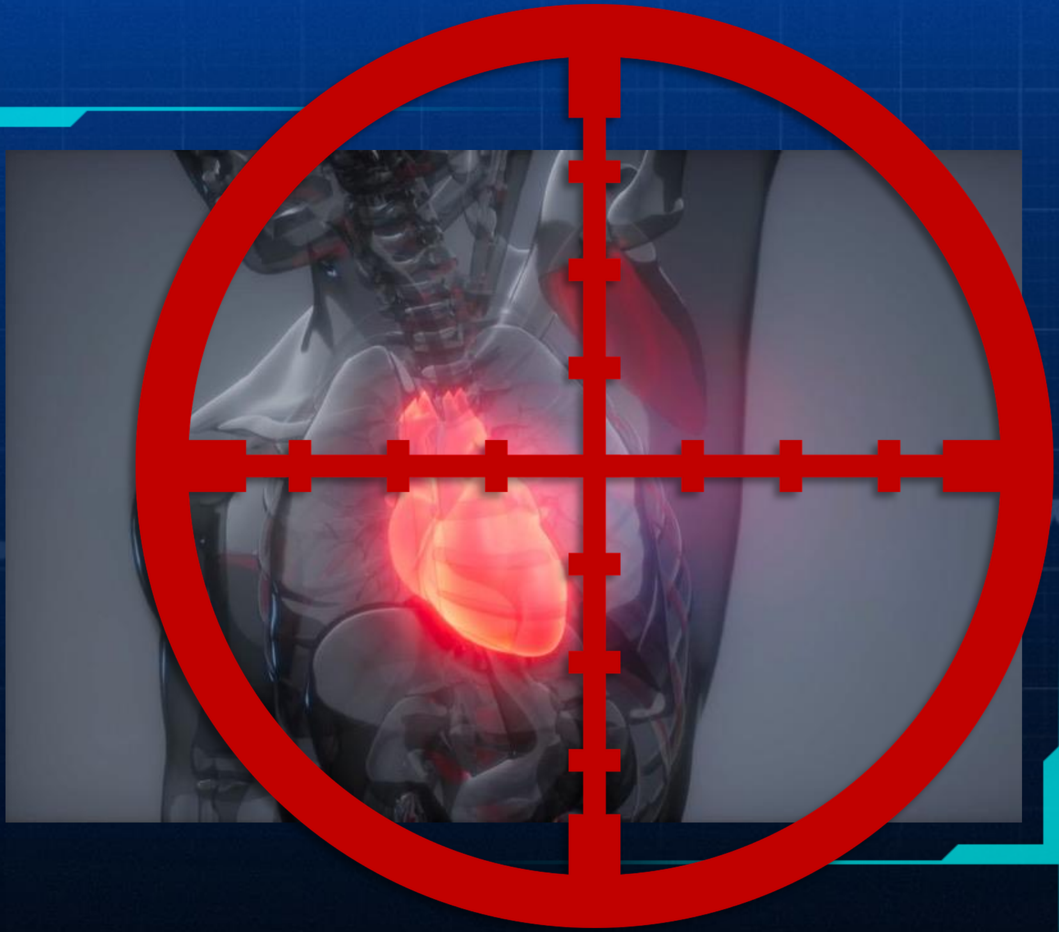
- Heart rhythm control (cardiac pacemakers)
- Heart failures (implantable defibrillators)
- Glucose level (closed-loop artificial pancreas)
- Automated personal drug delivery systems (infusion pumps)
- Bionic limbs
- Neural system (e.g., Neuralink)


Glucose level sensor with transmitter
Infusion subsystem
160
Automated closed-loop insulin pump

Can a hacker break your heart?

Possible attacks on medical devices:

- Denial of service (DoS)
- Malicious reconfiguration of the device's operational parameters
- Wireless upload of malicious firmware to the implanted device
- Changing dosage of administered drugs
- Changing the data from sensors
- Stealing the patient's medical data
- Blackmailing the patient
- Hacking drug infusion pumps
- Hacking hospital infrastructure



3D printed drugs

Medication tailored to you – a miracle or a curse?

- **Multiple drugs** with fine-tuned dosage and release time can be **combined in one pill**, prepared and 3D printed specifically for you. Amazing, right!
- However… **Security will be shifted** from large pharma companies **to your local pharmacy**. Which security can be better protected? Let's guess?
- OK, you go to a pharmacy and receive a pack of white pills. **How can you be sure about what is inside?**
- Possible **lethal attacks:**
  - Changing drug(s)
  - Changing drug(s) dosage
  - Changing drugs compatibility (e.g., allow antihypertensive drugs and NSAIDs)

Rise of killer robo-surgeons

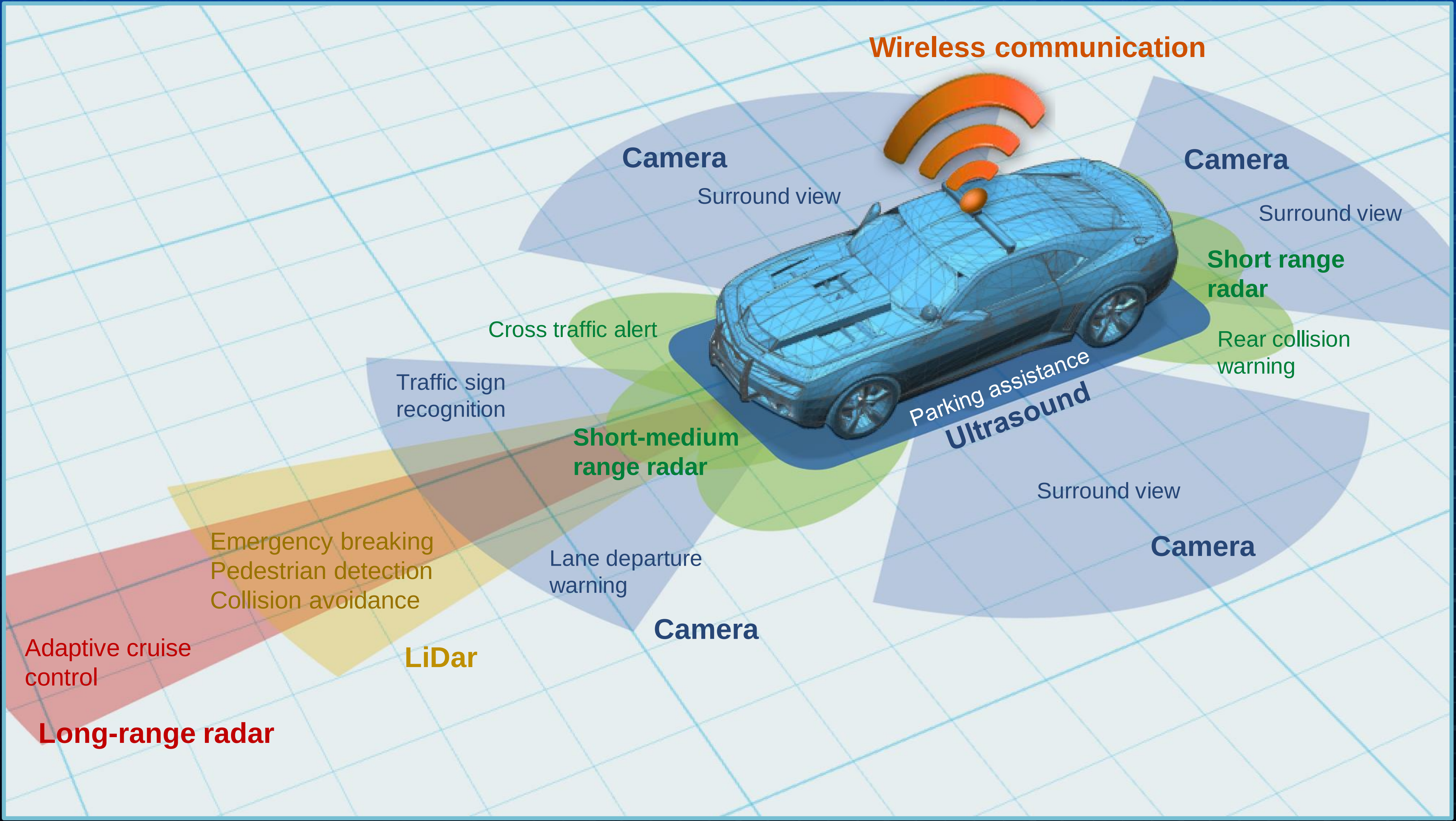
What if remote surgery systems been hacked?

© Intuitive Surgical

- Good news: surgical robots are here and they do top-quality jobs.
- Now they are not autonomous and always operated by a qualified surgeon – locally or remotely.
- In the future some routine elements of the procedure can be automated and handled by AI.
- Possible **lethal attacks:**
  - Denial of service (in cases of locally and remotely operated robot). What about BSOD in the middle of the procedure?
  - Changing the precision level of devices
  - Re-programming robo-surgeon’s AI

How to survive a car crash in the 21st century

The modern car is packed with technology



Typical ADAS sensors used in modern smart and self-driving cars

Sensors generate an insane amount of data

1.5 hrs of driving generates

4TB of data

- Can we not only process, transmit and store but also **sufficiently protect** this sensitive information?
- An additional problem is that this information **must be shared with the other cars** on the road in real time to optimize traffic.

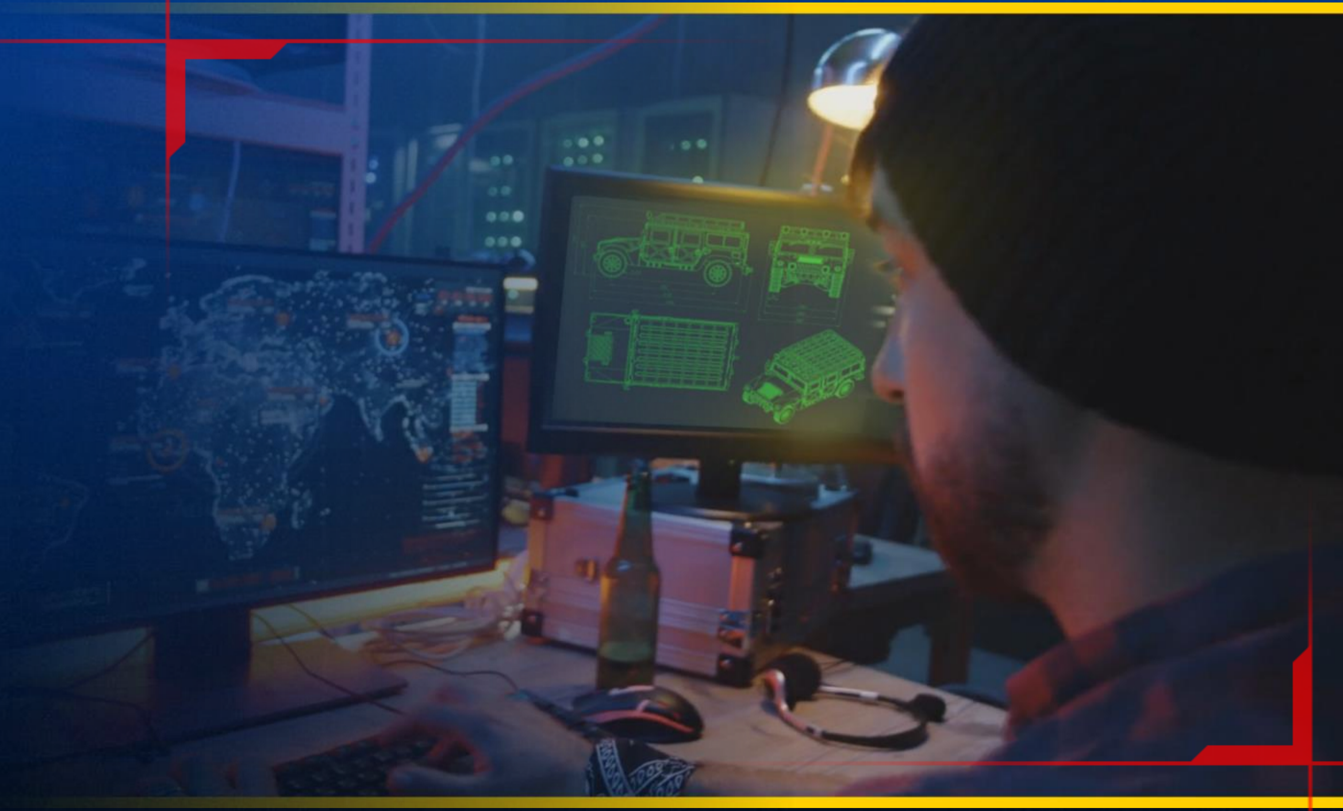
An enormous amount of data is exchanged

Every car must share the following information in real time:

- Unique ID, and basic information about the car model
- Technical parameters of the car
- The trajectory of the car (direction, road map)
- Maintained speed and current acceleration/deceleration
- Number of people inside
- Basic (or detailed?) information about passengers
- Car’s own weight and current load
- Number of detected cars around, relative distance to them
- Technical condition of the car and failure codes
- Information from about the road condition, obstacles, etc.
  - data from own sensors
  - data passed by other cars on the road

What can be hacked? Everything.

- Car communication with dedicated automotive infrastructure **(V2X)**
- Car communication with the other cars (autonomous and normal cars) – **(V2V)**
- Car **sensors**
- Main **car computer**
- Artificial Intelligence **(AI) algorithms**
- Internal communication, e.g. over **CAN Bus**
- Connected **third-party devices**, e.g. mobile phones



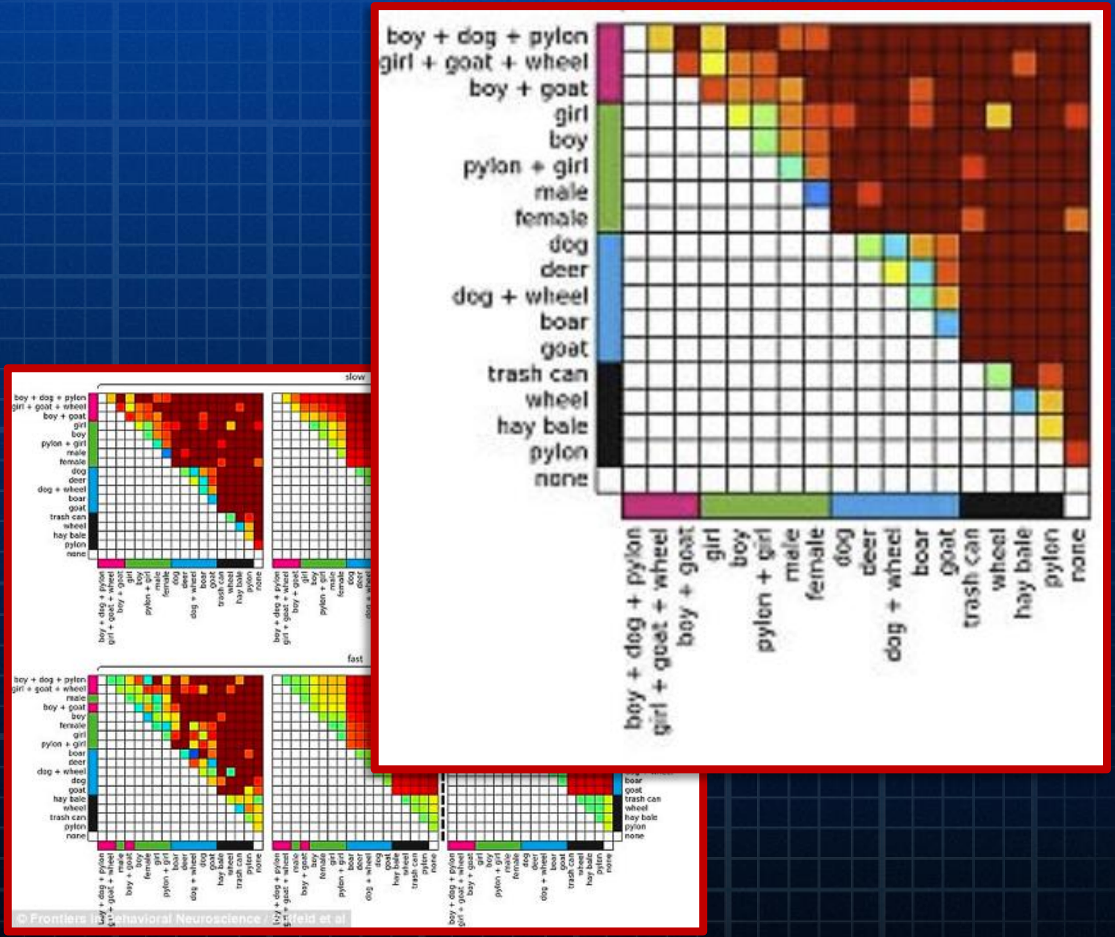
Who is going to die in a car crash

Researchers from The Institute of Cognitive Science at the University of Osnabrück **created a formula** that placed a variety of living things and objects in order, **based on their 'value of life', or survival.**

People were asked to **drive a car in virtual reality** in a typical suburban neighborhood, where they had to face unexpected objects. These included inanimate objects, animals and humans and the volunteers had to decide whom to keep alive and well… who has to die.

The results were measured by statistical models, which created **a set of rules that gives an insight into the moral decisions we make**.

A “social dilemma” appears in which <u>people could end up making conditions less safe for everyone by acting in their own self-interest.</u>



(c) Frontiers in Behavioral Neuroscience

Who is going to die in a car crash

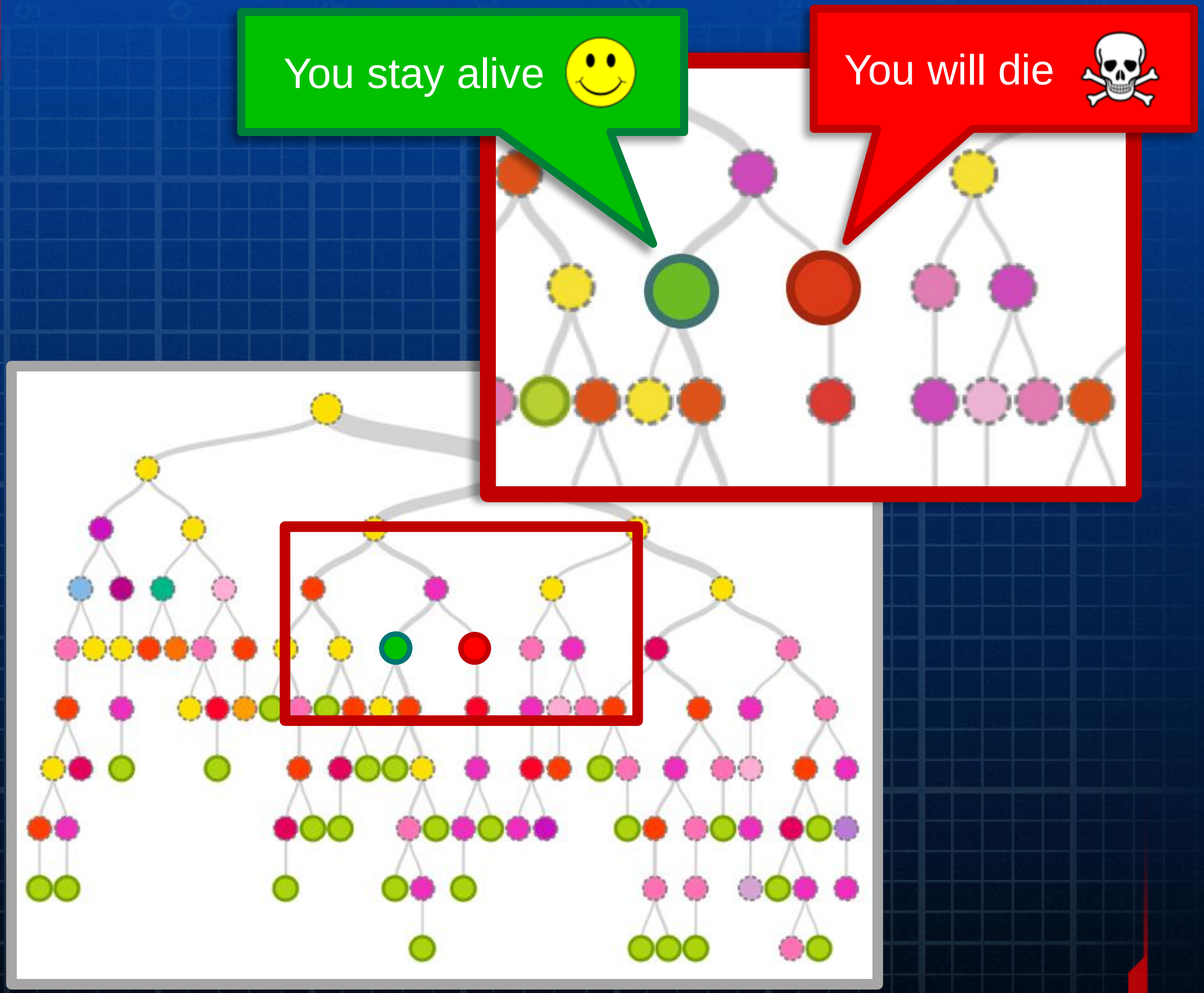
We should expect that this type of **logic will be implemented in self-driving cars** very soon.

In case of **accident the algorithm will choose who should survive**. The driverless vehicle will decide whether to hit an animal or inanimate object, rather than a pedestrian.

How to make a choice between a **child** passenger or a **group of pedestrians** (or V2V information from another car you will collide with about **a whole family traveling together**)?

What if this logic is "tweaked" by the car owner (e.g. to increase probability of survival)?

What if the **algorithm is hacked?**



The algorithm will decide who will be living and who will die

What hackers can do?

How to increase your chances of survival *(illegally, of course)*

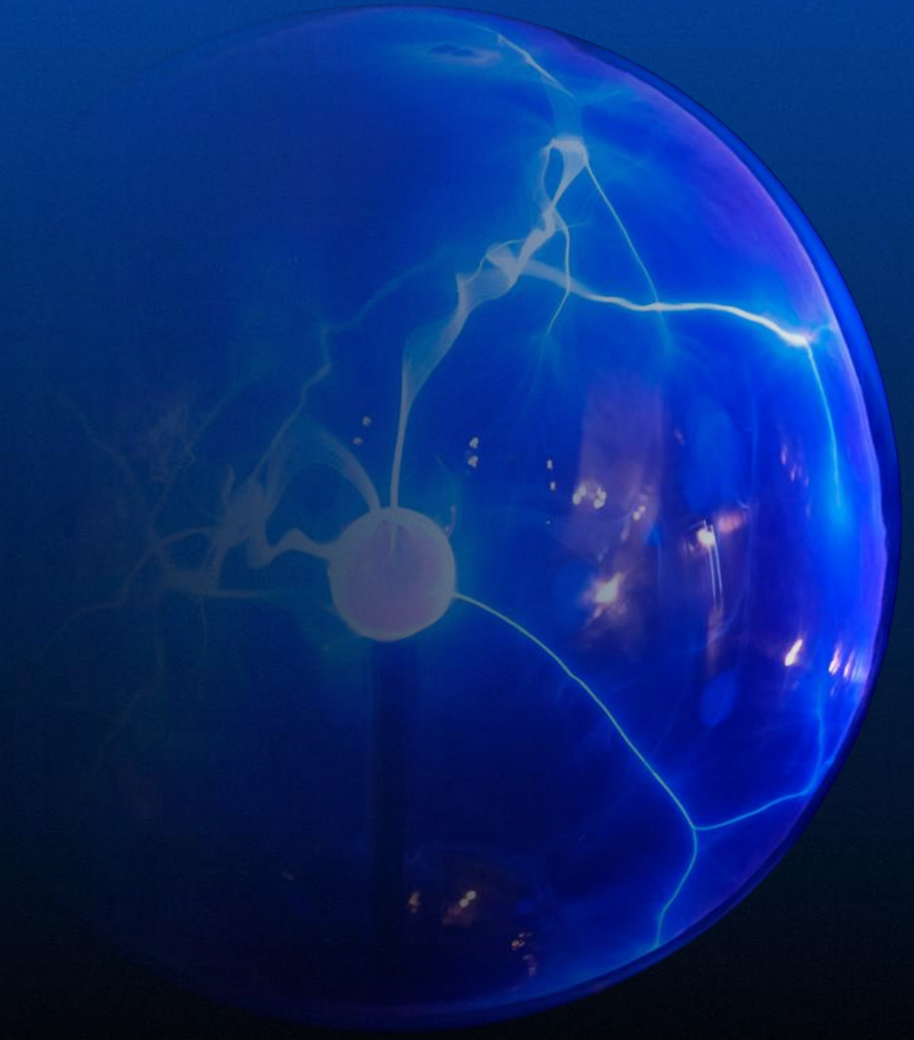
1. **Jam the communication** and leave everything to the chance (means: the collision will not be ”managed” by the car computer).
2. **Broadcast fake information** about the changed road condition, weather, etc.
3. **Hack (tweak or override)** publicly broadcasted parameters of the car:
   - **Who is inside** (e.g. number of people, a VIP or mother with 4 little children)
   - **Static parameters** of the car (car model, width, height, weight, etc.)
   - **Dynamic parameters** of the car (absolute or relative coordinates, direction of driving, velocity, deceleration speed, simulated breaks failure, simulated data from sensors, etc.)

Takeaways

Predictions for the future

We don't have a crystal ball, but…

- **Privacy** will be redefined. Who knows, maybe it will become obsolete
- **Mobile devices and wearables** become the number one target for all types of adversaries
- **AI/ML will be heavily "weaponized"** by corporations and also hackers of all kind
- **Deepfakes** will become ubiquitous. It will be even more difficult to separate truth from lies. AI/ML will be typically used for **tailored social engineering** attacks.
- **Warfare** will heavily **shift to cyberspace**. "Physical" wars are expensive and not "fit for purpose" in 21st century. Instead, regular "digital conflicts" between nations will become a new norm.



What can we do as a society?

- **Law should be "upgraded"** to deal with advanced modern technology, like AI/ML.
- All vendors must be responsible for **embedding cybersecurity** in every system, device or solution.
- As a vendor: before implementing a new high-tech "cool feature" – stop for a moment and think: **Is it safe? Would it make the world better?**
- Cybersecurity of every modern system **should be reviewed on a regular basis,** almost routinely.
- Collection and processing of personal data should be regulated by government.

What can do we as individuals?

- Switch off your electronic gadgets. Enjoy that “untweaked”, “unfiltered” real life! **Live your life** and **feel the emotions!**

- Do not get too excited by all those new gadgets and features. **Think about security implications.** Play an imaginary “war game” and evaluate the security consequences.

- **Don’t share online more than you should**. Think twice before sharing anything. And then think again!

- Always **think before you click.** In the Internet good and bad are, literally, just one click away!

Questions

Thank you!

https://www.spirent.com/Products/SecurityLabs

securityLabs@spirent.com

Aleksander Gorkowienko
e: aleksander.gorkowienko@spirent.com
m: +44 (0) 7974431025