How would cybersecurity change if we had better computers?

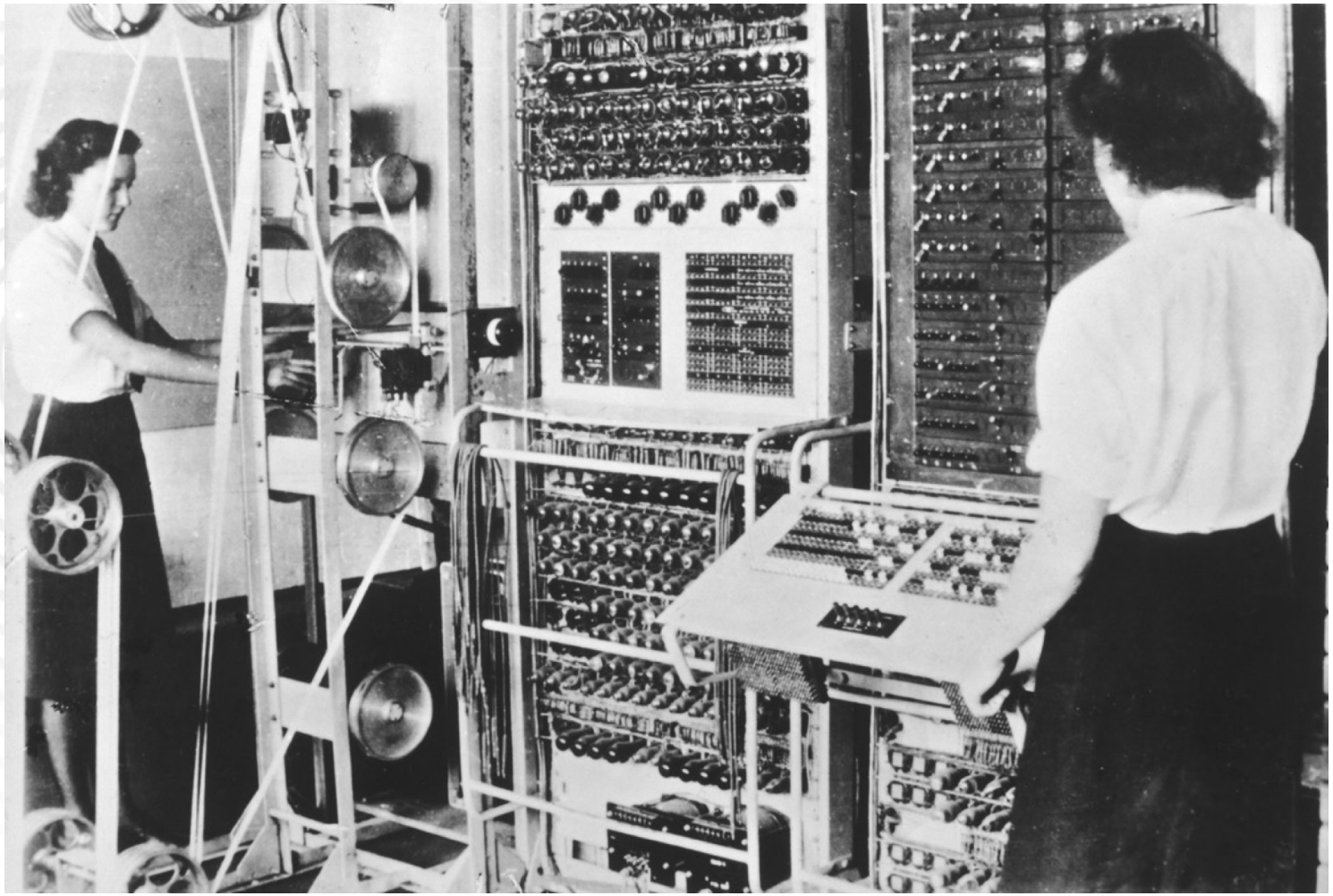
Cybersecurity Deep Dive, German-Baltic Digital Summit

Dan Bogdanov, PhD
Head of the Department of Privacy Technologies
@danbogdanov

On May 25th, 2018, GDPR entered into force in Europe

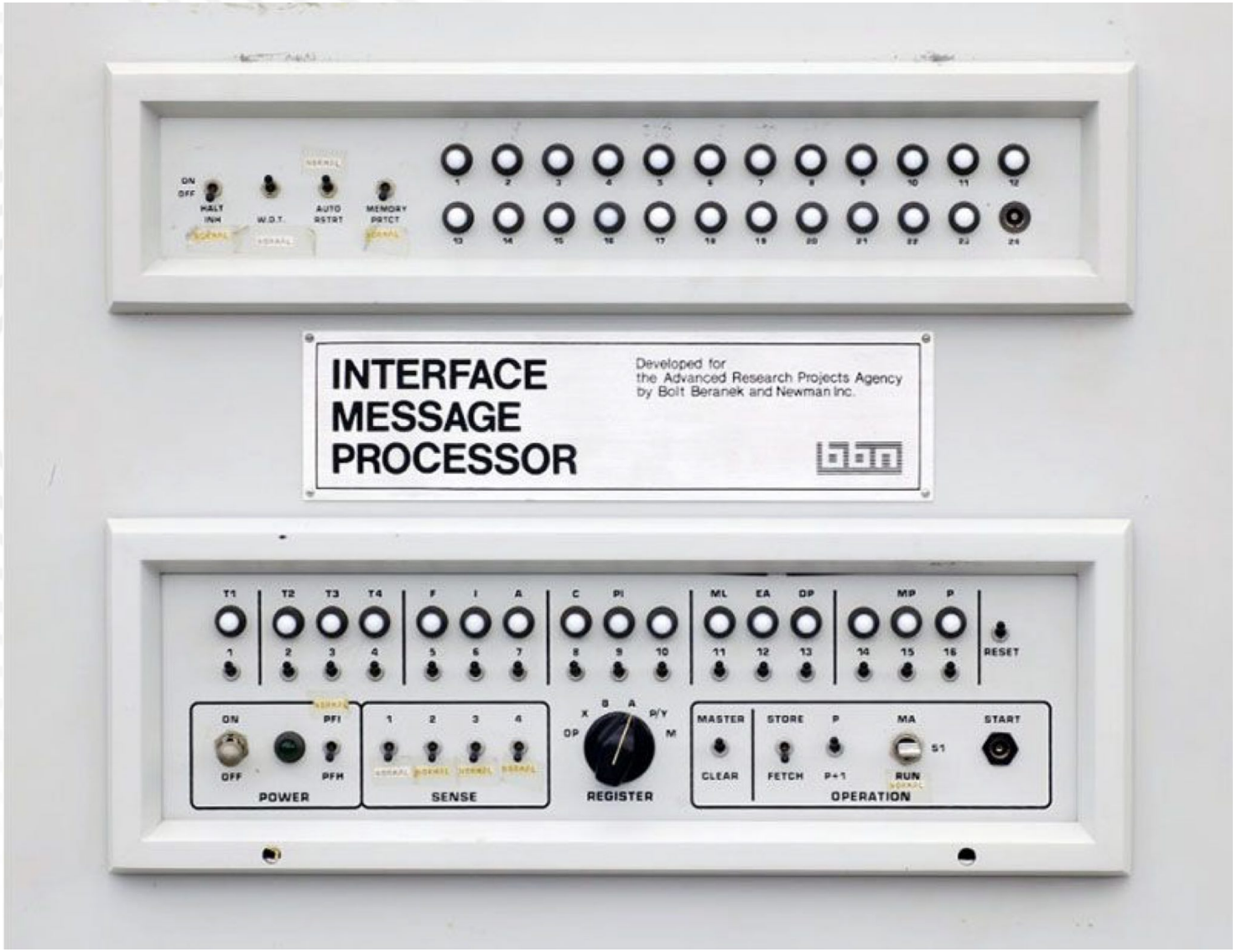
When did we start to need this?

The first programmable, digital computer



- **The Colossus**
- Built in UK in 1943
- Used to break the Lorenz SZ device
- Security was not a concern at the time
- Ironically, breaking security was the main goal of the machine
- *Picture courtesy of The History Blog*

The first packet-switched network router



- **The Interface Message Processor**
- Built by BBN in 1969
- Used to build the ARPANET
- Security was not a concern at the time
- Ease of growing the network was
- *Picture courtesy of the Computer History Museum*

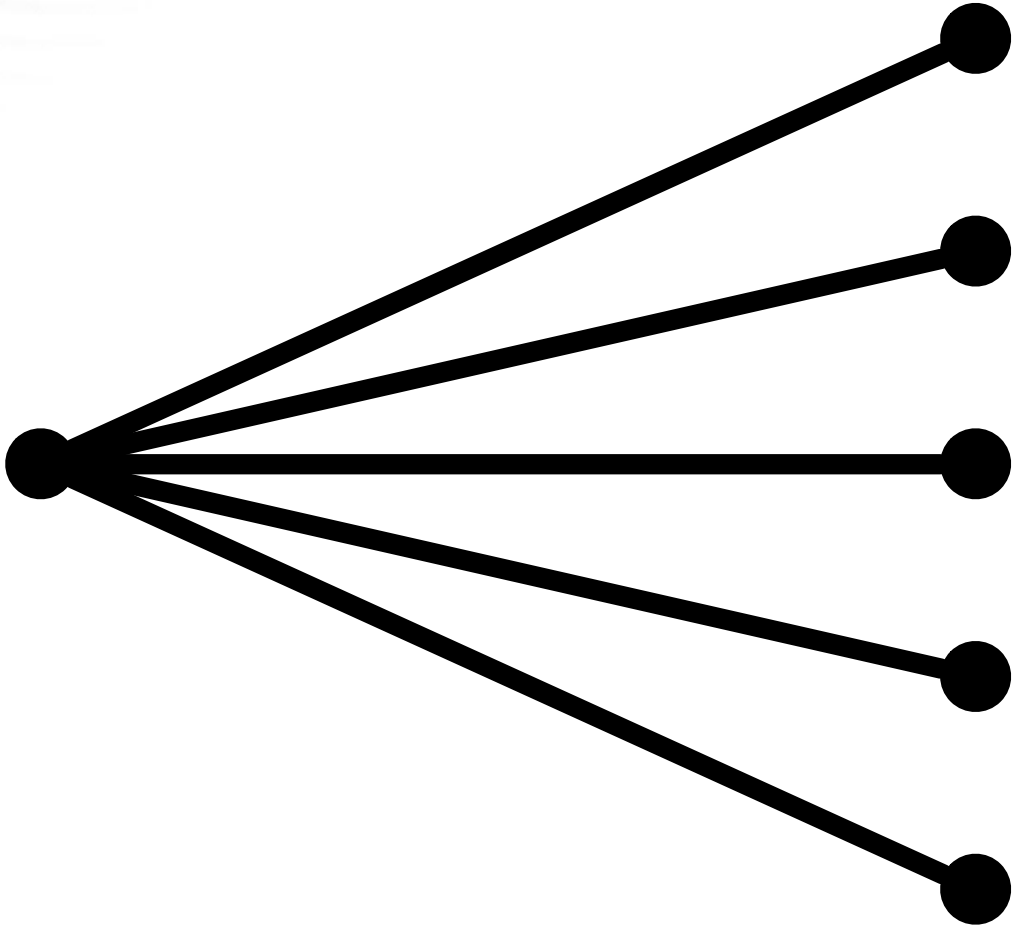
CYBERNETICA

The first computer alone has no security problems

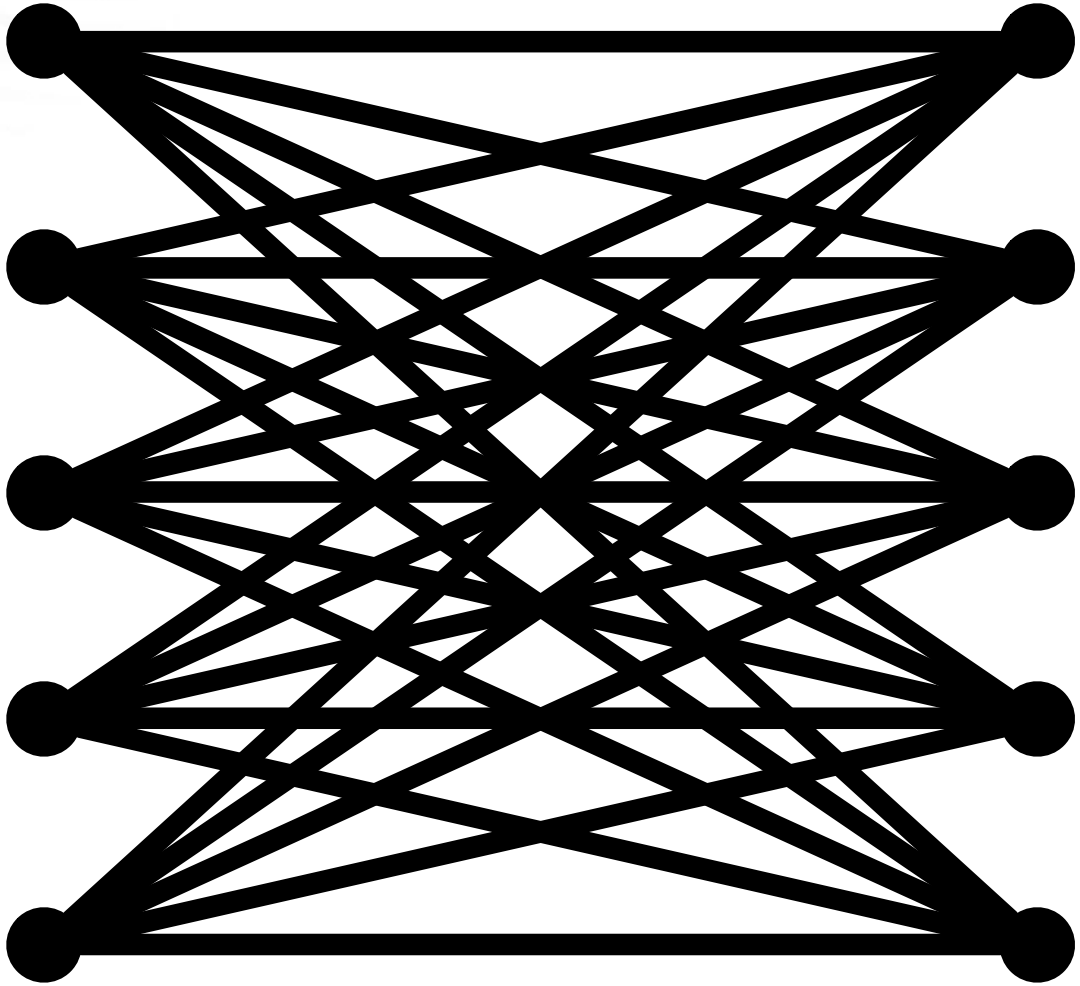
Two computers create competition (and secrets!)

Two computers talking to each other can create value

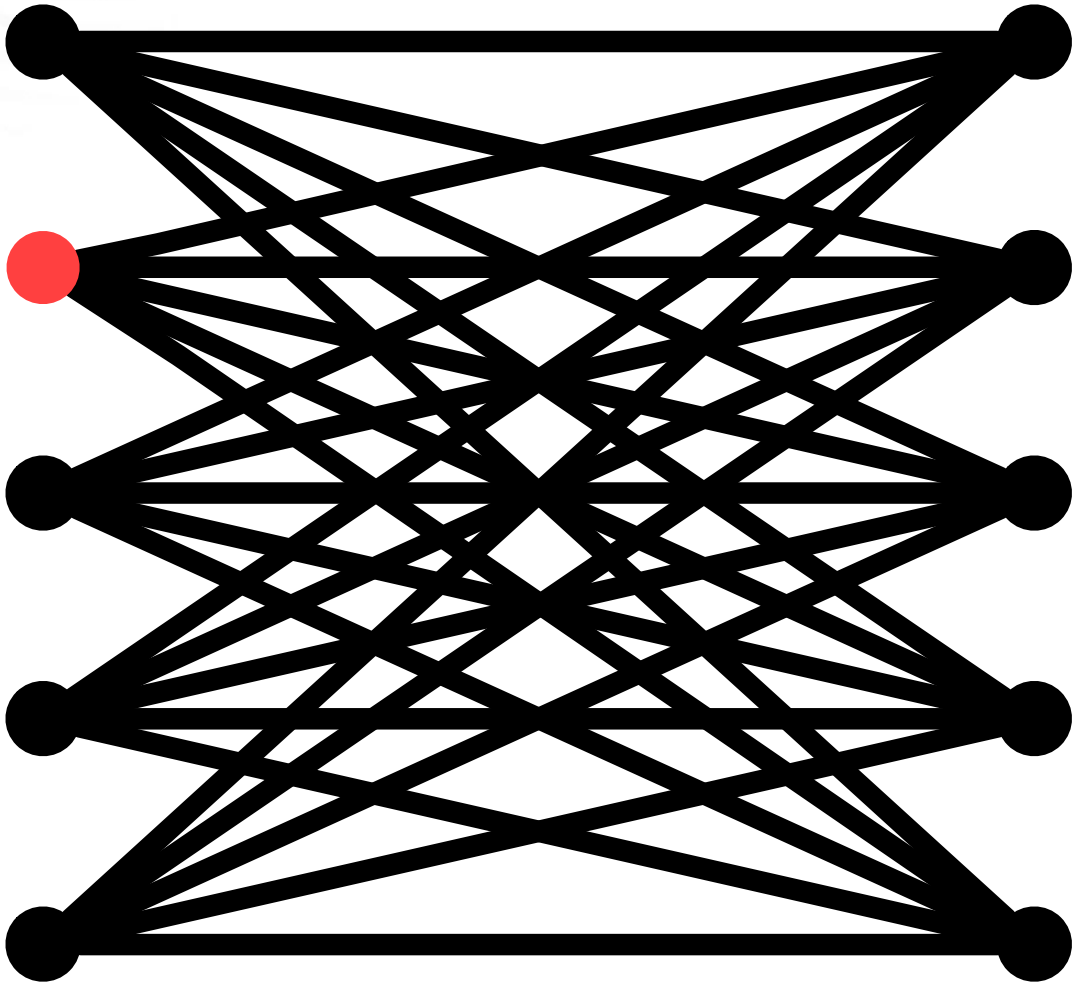
More is better, as it can create efficiencies in society



A full network is where we are now

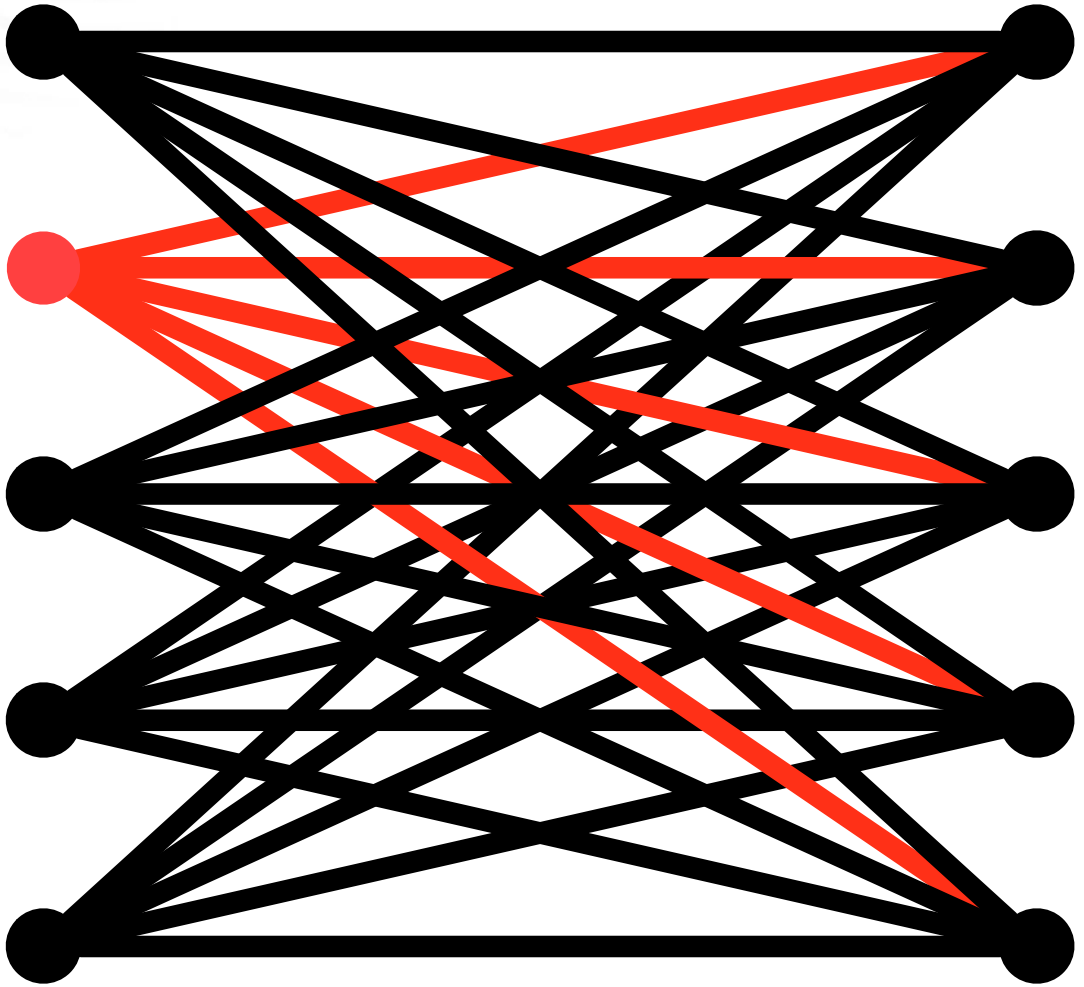


Today, we have to protect every node…



CYBERNETICA

…and edge, patching security in step by step

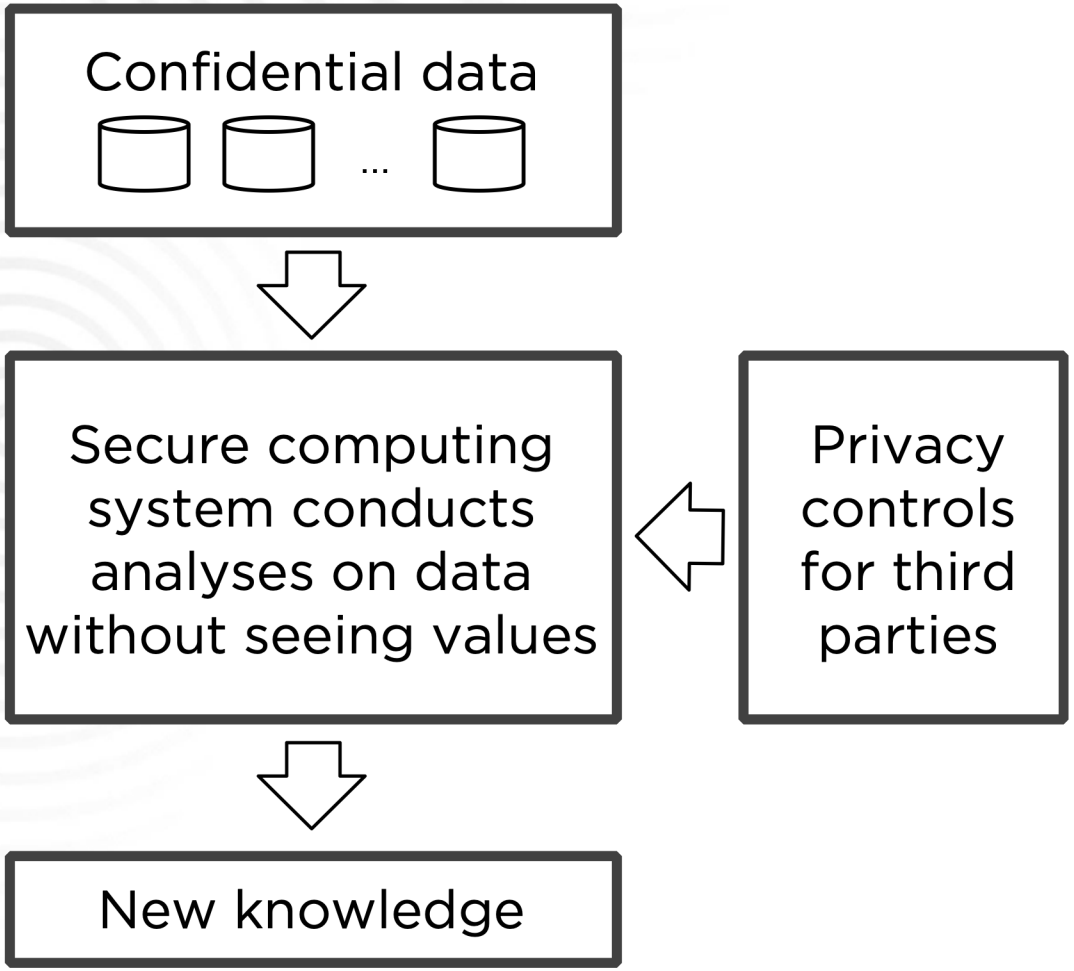


CYBERNETICA

What if we had better computers?

CYBERNETICA

Secure computing technologies for data-driven services

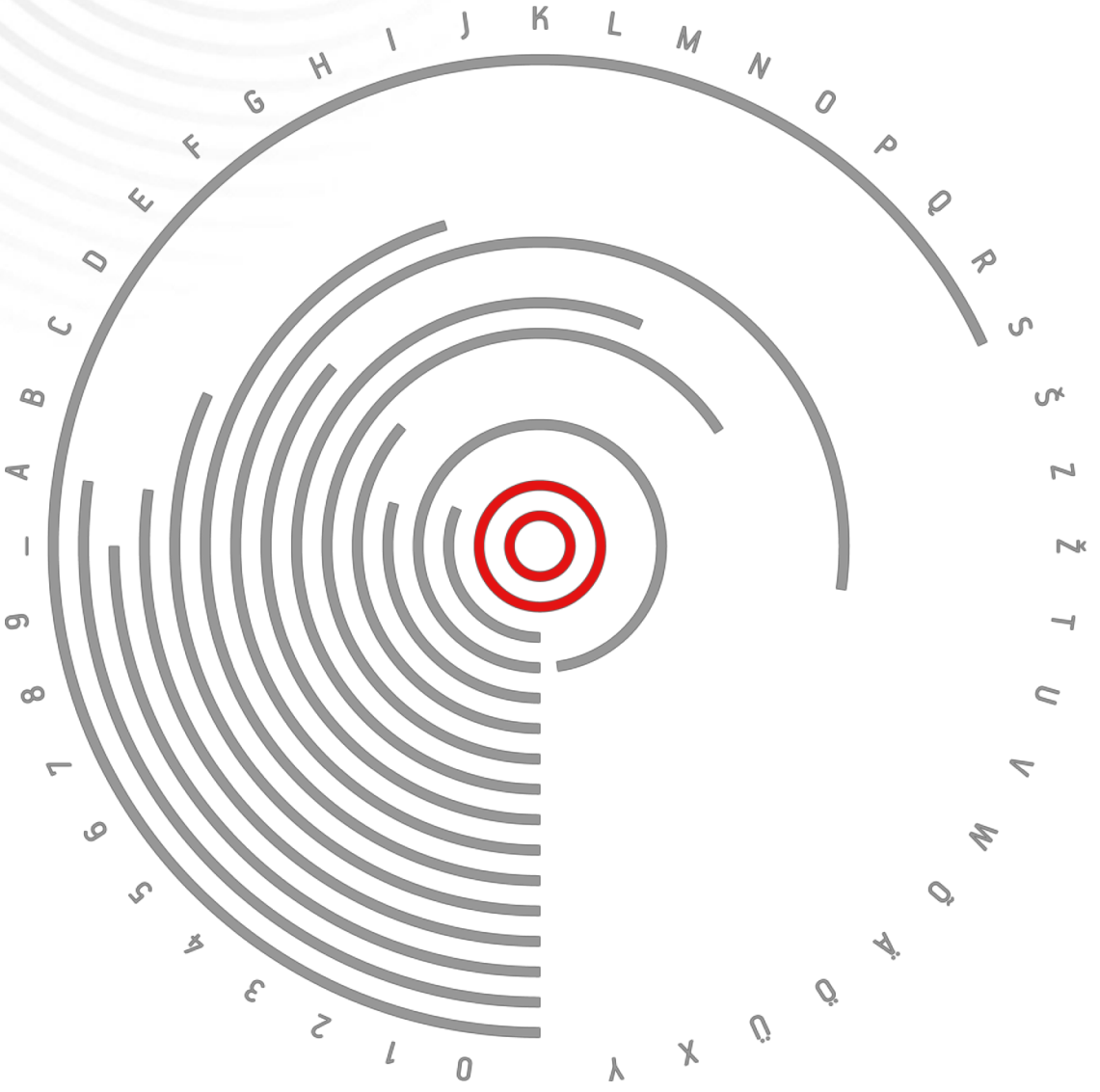


- Data owners encrypt data on-site and upload to the system.
- Data analysts build and run queries without accessing the data.
- The secure computing system processes the queries without removing the protection.
- Authorised users receive query results in an encrypted format.
- **There is no single party who can access a confidential record.**

Interesting legal precedent on secure computing

- In Estonia in 2015, a social science research company (CentAR) used the Sharemind secure computing system to link
  - 10 000 000 salary tax records from the Estonian Tax Office
  - 600 000 education records from the Ministry of Education
- to analyse the relations between working and not graduating the university on time.
- The Data Protection Agency stated that no personal data was being processed in this study.
- Precedent validated under the GDPR by Uni Göttingen.


CYBERNETICA


A B C D E F G H I J K L M N O P Q R S Ś T U V W O Ó X Y 0 1 2 3 4 5 6 7 8 9 –