MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

WELCOME TO HARRIS!

1ST WORKSHOP ON HARDWARE REVERSE ENGINEERING

CHRISTOF PAAR

JANUARY 24-25, 2023

THANKS TO THE HARRIS TEAM!

Julian Speith

Nils Albartus

Steffen Becker

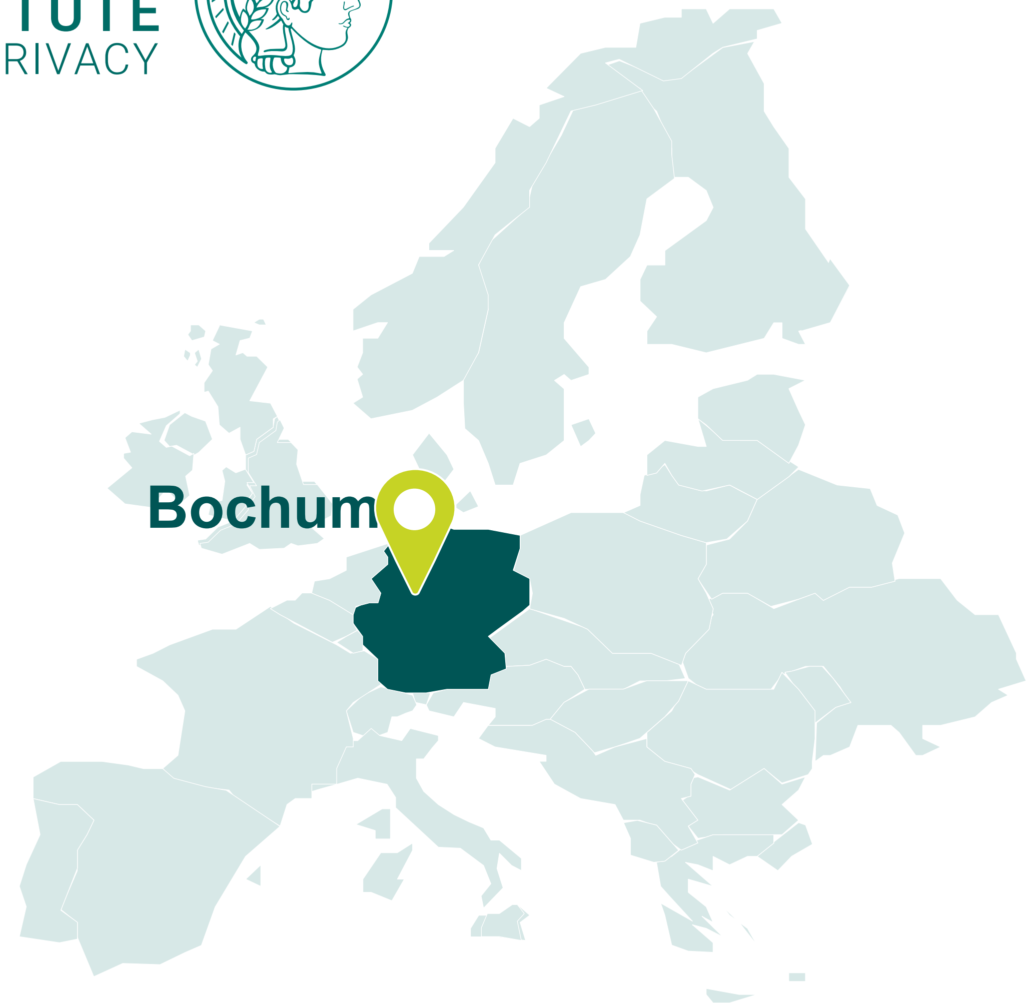
Agenda

- **Welcome to HARRIS**
- Some Thoughts on Hardware Reverse Enginering

CYBERSECURITY ECOSYSTEM IN BOCHUM

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

RUB



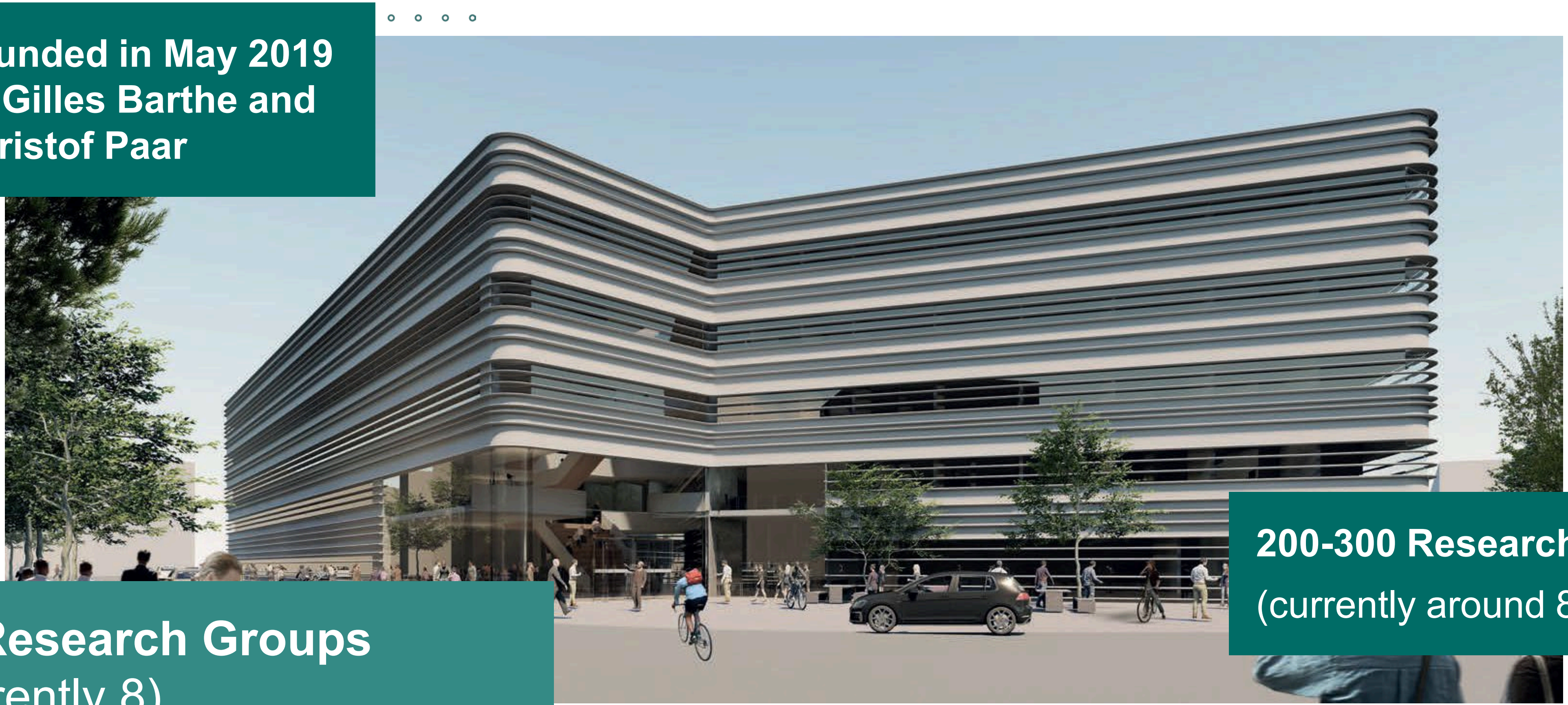
CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

HGI
HORST
GÖRTZ
INSTITUTE

CUBE 5
Creating Security

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY (MPI-SP)

Founded in May 2019 by Gilles Barthe and Christof Paar



18 Research Groups
(currently 8)

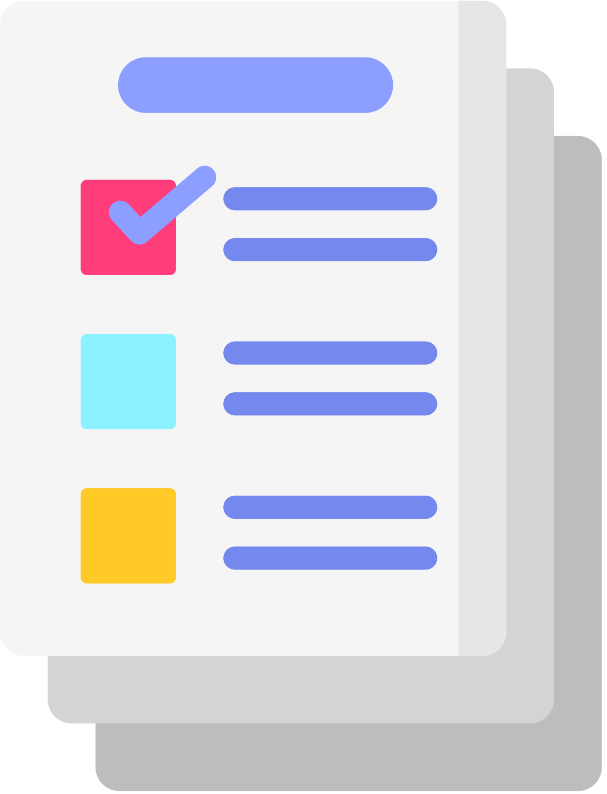
200-300 Researchers
(currently around 80)

HARRIS 2023 STATISTICS

- **Over 80 participants**
  - Industry, government and academia
  - International!
    - Estonia, France, Germany, Israel, Netherlands, Norway, Singapore, Spain, Switzerland, Ukraine, USA…
- **20+ talks on Hardware Reverse Engineering**
  - Keynote by Olivier Thomas, Texplained (France)

GENERAL OUTLINE

- **Talks on Hardware Reverse Engineering**
- **Rapid Research Rendezvous**
- **Discussion Tables**



GENERAL OUTLINE

- **Talks on Hardware Reverse Engineering**
  - Location: Beckmanns Hof
  - 20+ talks of 20 minutes each (including Q&A)
- **Rapid Research Rendezvous**
- **Discussion Tables**

GENERAL OUTLINE

- Talks on Hardware Reverse Engineering

- **Rapid Research Rendezvous**
- **Idea: 15 minute exchange on research in small groups**
  - Location: Beckmanns Hof during coffee breaks
  - Everyone received random partners in the back of their nametag

- **Discussion Tables**

GENERAL OUTLINE

- Talks on Hardware Reverse Engineering
- Rapid Research Rendezvous
- **Discussion Tables**
  - Location: MC building
    (location 2 on the map; we will walk there together)
  - Get together in small groups to discuss future research and spark future collaborations
  - You can still make suggestions by 3pm

DAY 1 - SCHEDULE

- **11.00 – 11.30: Rapid Research Rendezvous 1 (incl. Coffee)**
- **11.30 – 12.30: Session 1: Trust & Assurance (Chair: Christof Paar)**
- **12.30 – 13.30: Lunch Break**
- **13.30 – 14.30: Session 2: Sample Preparation & Imaging (Chair: Bernhard Lippmann)**
- **14.30 – 15.00: Rapid Research Rendezvous 2 (incl. Coffee)**
- **15.00 – 16.10: Session 3: Netlist Analysis (Chair: Georg Sigl)**
- **16.30 – 18.00: Discussion Tables @ MC**
- **18.00 – End: Dinner @ Q-West**

DAY 2 - SCHEDULE

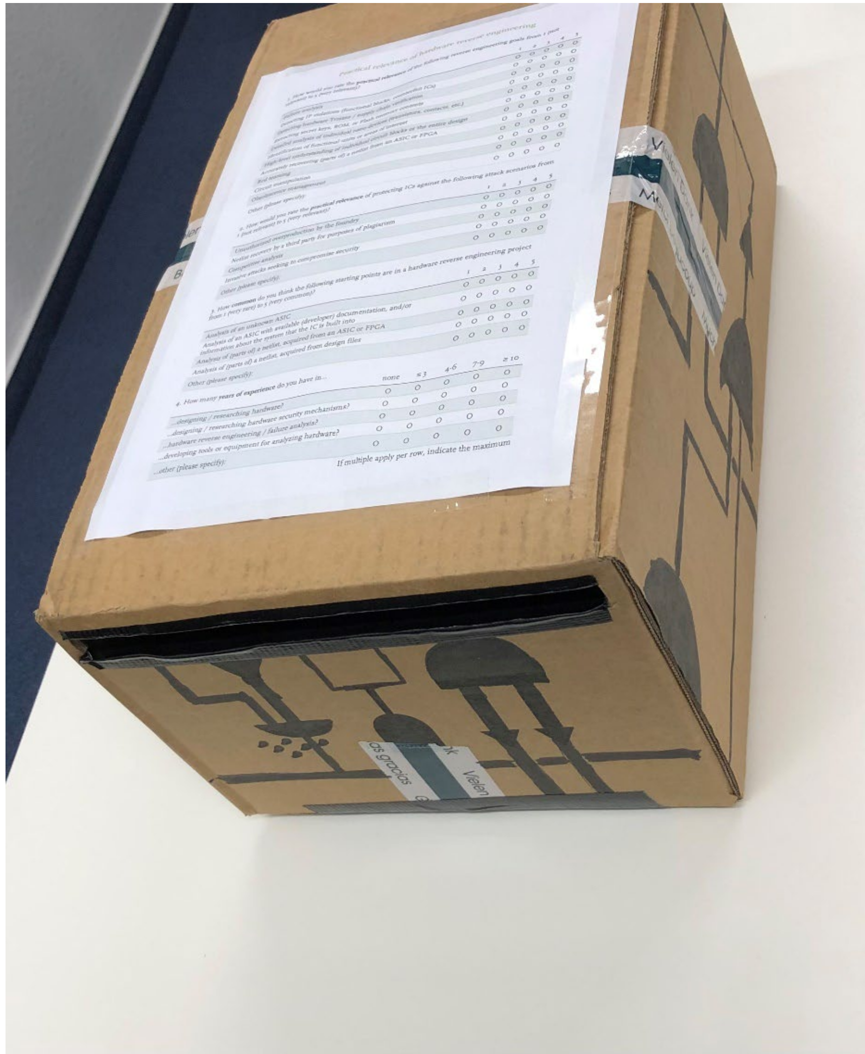
- **09.40 – 11.00: Session 4: Evaluation & Open-Source Silicon** (Chair: Stephan Nickell)
- **11.00 – 11.30: Coffee Break**
- **11.30 – 12.30: Keynote by Olivier Thomas, Texplained**
- **12.30 – 13.30: Lunch**
- **13.30 – 14.30: Session 5: Selected Aspects of HRE** (Chair: Jürgen Frinken)
- **14.30 – 15.00: Coffee Break**
- **15.00 – 16.10: Session 6: Hardware Trojans** (Chair: Jean-Pierre Seifert)

STUDY AT HARRIS 23

Practical relevance of hardware reverse engineering

1. How would you rate the **practical relevance** of the following reverse engineering goals from 1 (not relevant) to 5 (very relevant)?

	1	2	3	4	5
Failure analysis	○	○	○	○	○
Detecting IP violations (functional blocks, counterfeit ICs)	○	○	○	○	○
Detecting hardware Trojans / supply chain verification	○	○	○	○	○



Practical relevance of hardware reverse engineering

1. How would you rate the **practical relevance** of the following reverse engineering goals from 1 (not relevant) to 5 (very relevant)?

	1	2	3	4	5
Failure analysis	○	○	○	○	○
Detecting IP violations (functional blocks, counterfeit ICs)	○	○	○	○	○
Detecting hardware Trojans / supply chain verification	○	○	○	○	○
Extracting secret keys, ROM, or Flash memory contents	○	○	○	○	○
Detailed analysis of individual nano-devices (transistors, contacts, etc.)	○	○	○	○	○
Identification of functional units or areas of interest	○	○	○	○	○
High-level understanding of individual circuit blocks or the entire design	○	○	○	○	○
Accurately recovering (parts of) a netlist from an ASIC or FPGA	○	○	○	○	○
Red teaming	○	○	○	○	○
Circuit manipulation	○	○	○	○	○
Obsolescence management	○	○	○	○	○
Other (please specify):					

2. How would you rate the **practical relevance** of protecting ICs against the following attack scenarios from 1 (not relevant) to 5 (very relevant)?

	1	2	3	4	5
Unauthorized overproduction by the foundry	○	○	○	○	○
Netlist recovery by a third party for purposes of plagiarism	○	○	○	○	○
Competitive analysis	○	○	○	○	○
Invasive attacks seeking to compromise security	○	○	○	○	○
Other (please specify):	○	○	○	○	○

3. How **common** do you think the following starting points are in a hardware reverse engineering project from 1 (very rare) to 5 (very common)?

	1	2	3	4	5
Analysis of an unknown ASIC	○	○	○	○	○
Analysis of an ASIC with available (developer) documentation, and/or information about the system that the IC is built into	○	○	○	○	○
Analysis of (parts of) a netlist, acquired from an ASIC or FPGA	○	○	○	○	○
Analysis of (parts of) a netlist, acquired from design files	○	○	○	○	○
Other (please specify):	○	○	○	○	○

4. How many **years of experience** do you have in...

	none	≤ 3	4-6	7-9	≥ 10
...designing / researching hardware?	○	○	○	○	○
...designing / researching hardware security mechanisms?	○	○	○	○	○
...hardware reverse engineering / failure analysis?	○	○	○	○	○
...developing tools or equipment for analyzing hardware?	○	○	○	○	○
...other (please specify):	○	○	○	○	○

If multiple apply per row, indicate the maximum

HARRIS 2024?

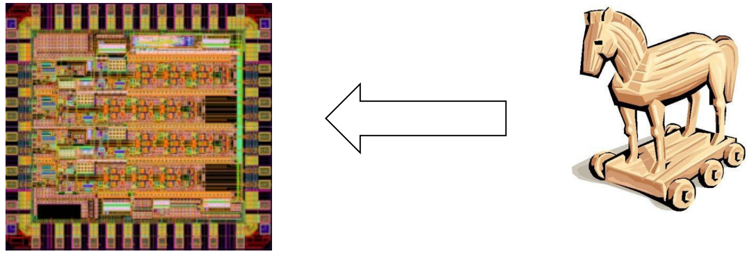
- We already received questions about HARRIS 2024 and will setup an optional mailing list to keep you informed if (and when) HARRIS 2024 will happen

Agenda

- Welcome to HARRIS
- **Backdoors and Hardware Reverse Enginering**

HARDWARE TROJANS

“Malicious change to an IC that adds or remove functionality”



Many rather unpleasant “applications”

TROJAN INJECTION & ADVERSARIES SCENARIOS

Defense Science Board
Task Force
On
HIGH PERFORMANCE
MICROCHIP SUPPLY

[illegible]

ing

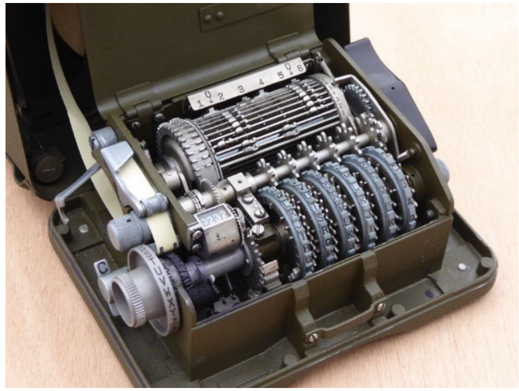
Hostile hardware blocks
("IP-cores")

NSA's *interdiction*

during shipment

Built-in by
manufacturer

HISTORICAL PERSPECTIVE: COLD WAR

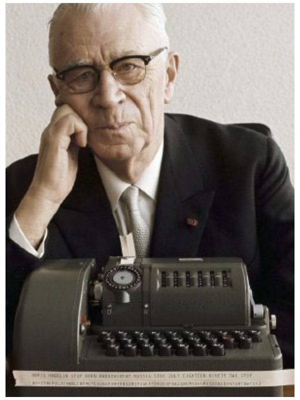


US WWII

M-209 encryption machine

AB Cryptoteknik

by Boris Hagelin

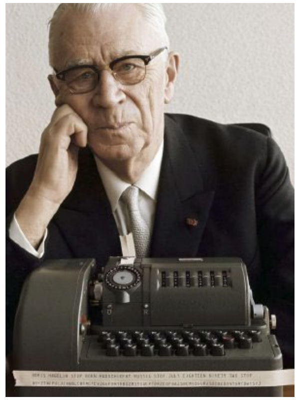


Cold War

C-52 encryption machine

Crypto AG

by Boris Hagelin



HISTORICAL PERSPECTIVE: COLD WAR

alleged cooperation between *Crypto AG* and intelligence services

Strong indication that C-52 was artificially weakend

HISTORICAL PERSPECTIVE: COLD WAR

1986 Berlin bombing

„La Belle discothèque“

retaliatory air strikes against Libya

HISTORICAL PERSPECTIVE: 2019

- How trustworthy is foreign-made equipment?

Bloomberg
Businessweek

October 8, 2018

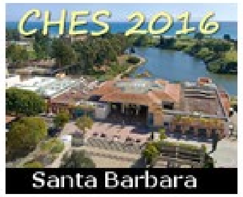
The Big Hack

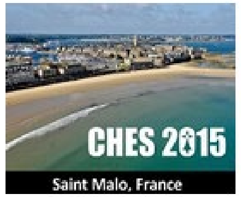
How China used a tiny chip to infiltrate America's top companies

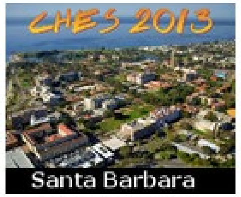
Backdoors in routers ?

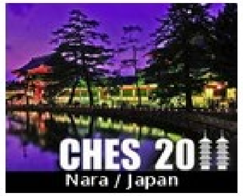
… or in mobile networks?

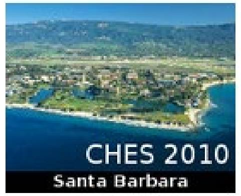
WHAT ABOUT THE SCIENTIFIC COMMUNITY?

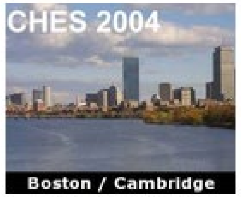


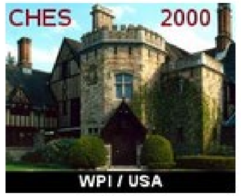


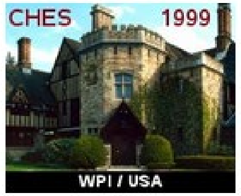






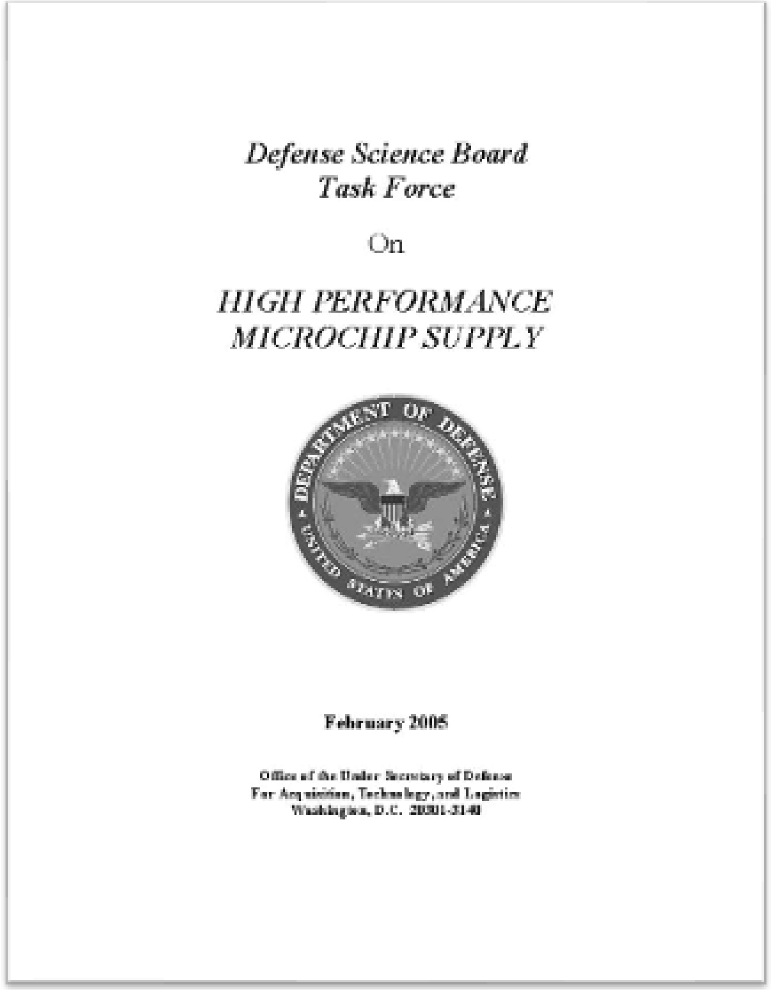






very little work prior to 2005 ….

U.S. DEPARTMENT OF DEFENSE REPORT (2005)



Defense Science Board
Task Force

On

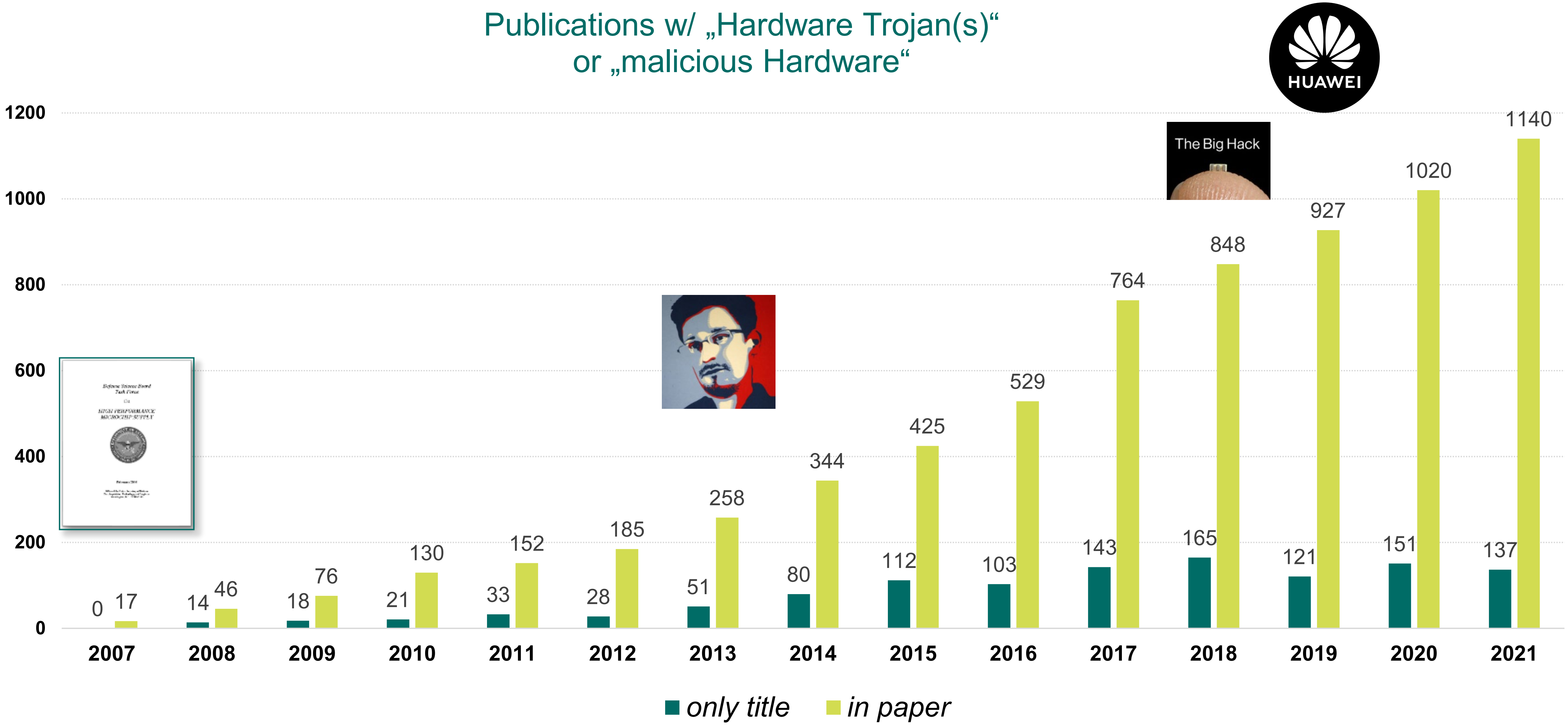
HIGH PERFORMANCE
MICROCHIP SUPPLY

February 2005

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

2005 DoD report triggers research on hardware Trojans

HARDWARE TROJANS AND THE SCIENTIFIC COMMUNITY


Publications w/ „Hardware Trojan(s)“
or „malicious Hardware“

Quelle: Google Scholar, last update: May 2022

SO, WHY DO WE NEED HARDWARE REVERSE ENGINEERING?

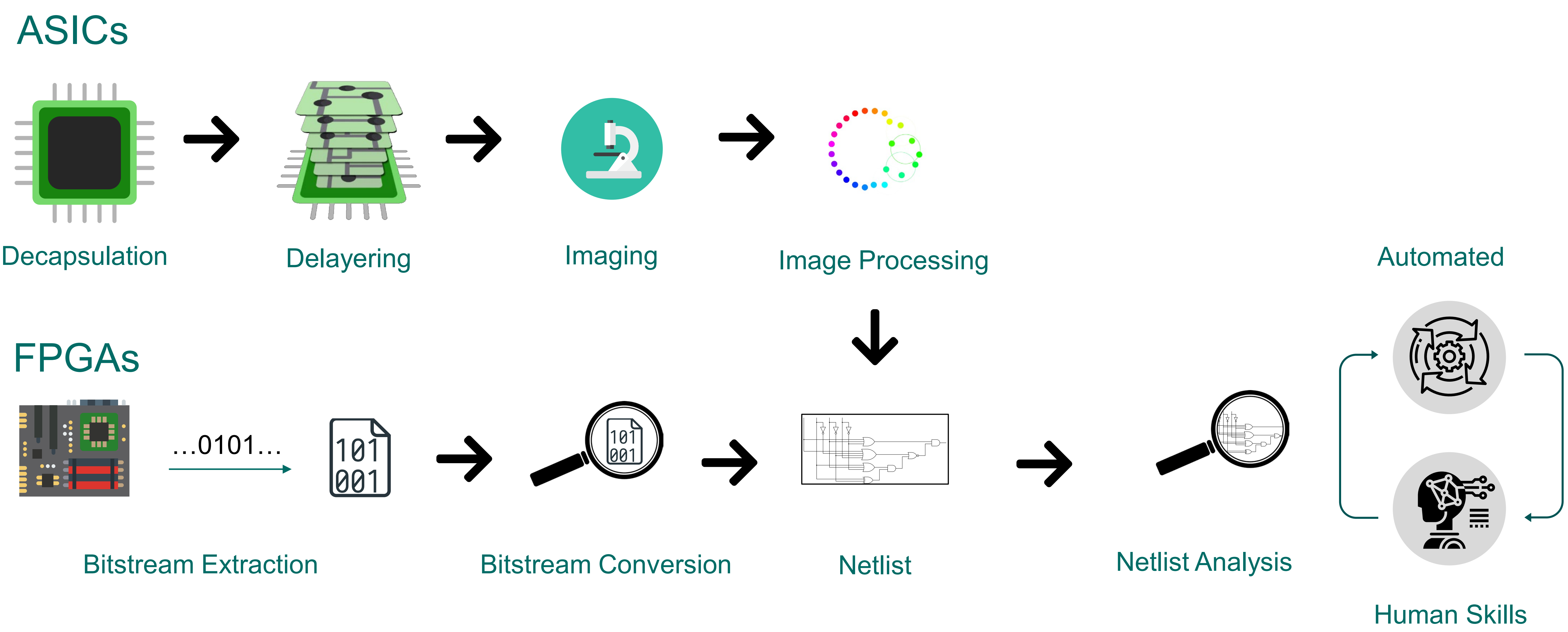
for understanding HW Trojans

- Constructively: detection of Trojans
- Destructively: for insertion of Trojans

… many other motivations for understanding HW Trojans

- Detecting IP theft
- Competitive analysis
- Fault detection
- …

STEPS IN HARDWARE REVERSE ENGINEERING



ASICs

Decapsulation

Delayering

Imaging

Image Processing

FPGAs

Bitstream Extraction

Bitstream Conversion

Netlist

Netlist Analysis

Automated

Human Skills

ENJOY HARRIS!

Christof Paar

Max Planck Institute for Security and Privacy