



The diagram features two white line-art profiles of human heads facing each other on a dark, chalkboard-like background. The left head contains three interlocking gears of different sizes, with the text "STRATEGIC BASIC RESEARCH" written below it. An orange arrow points from the left head to the right head, which contains a glowing lightbulb with rays emanating from it, with the text "COLLABORATIVE RESEARCH" written below it.

Strategic Cybersecurity Research and Support for Innovation in Industry

Bart Preneel - COSIC, KU Leuven
Wouter Joosen - DistriNet, KU Leuven
Leuven, November 25, 2019

Cybersecurity Initiative Flanders

"Top Strategic Basic Research Programme"

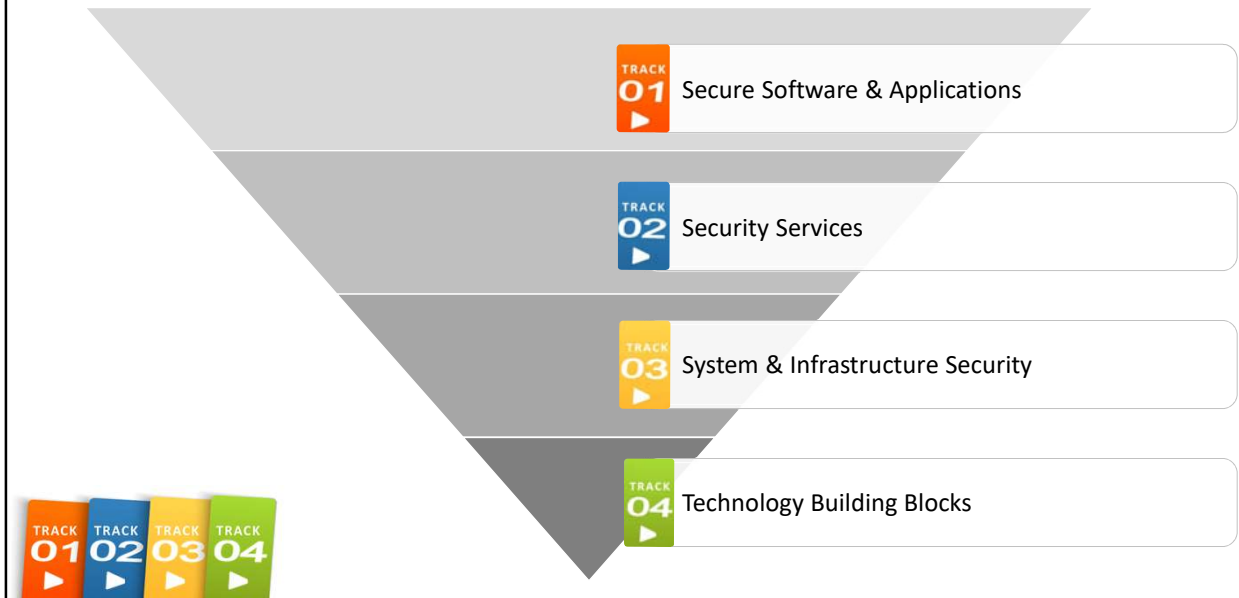


The image shows four vertical bars of different colors (orange, blue, yellow, and green) arranged side-by-side. Each bar has a white play button icon in the center. Below each bar is a specific research track name.

TRACK 01	TRACK 02	TRACK 03	TRACK 04
Secure Software & Applications	Security Services	System & Infrastructure Security	Technology Building Blocks

2

(Potentially) *different audiences* for different research tracks



TRACK 01

Secure Software & Applications

- THEME 1
Secure Software Development Life Cycle (SDLC)
- THEME 2
Program Verification and Security Testing
- THEME 3
Secure Programming Languages & Secure Compilation

4

VERIFICATION ON THE HORIZON

```

void memcpy(unsigned char *dest, unsigned char *src, unsigned size);
/*@ requires dest[..size] |-> _ &*& src[..size] |-> ?cs;
    @ ensures dest[..size] |-> cs &*& src[..size] |-> cs;

n2s(p, payload);
pl = p;

if (hbtype == TLS1_HB_REQUEST)
{
    unsigned char *buffer;
    unsigned char *bp;
    int r;

    buffer = OPENSSL_malloc(1u + 2u + payload + padding);
    bp = buffer;

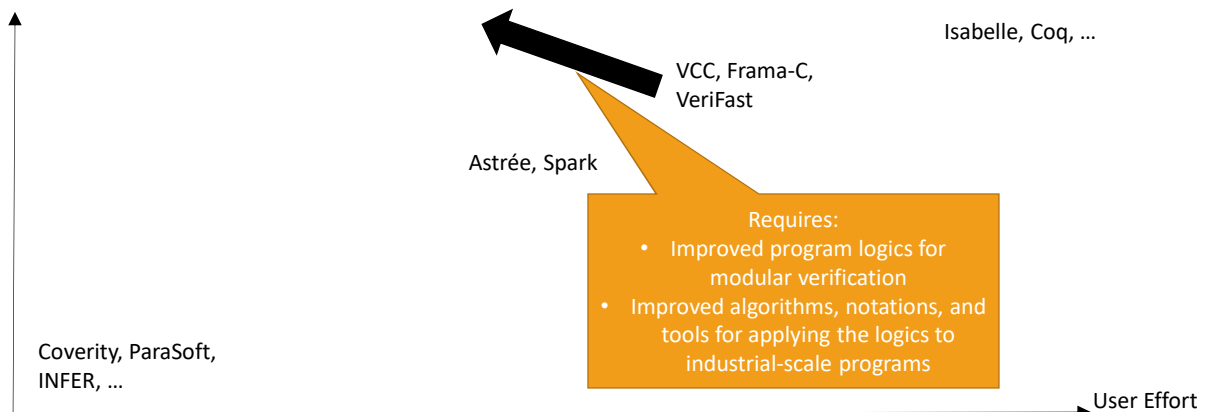
    *bp = TLS1_HB_RESPONSE; bp++;
    s2n(bp, payload);
    memcpy(bp, pl, payload);
    bp += (int)payload;
  
```

THEME 2
01

5

OBJECTIVE

Assurance Level



THEME 2
01

6

TRACK 02

Security Services

- THEME1
Identity Management and Authentication
- THEME 2
Authorization and Audit
- THEME3
Advanced Encryption Techniques and Data Access
Middleware
- THEME4
Policy and Regulation

7

POLICY AND REGULATIONS

TRACK 02

Security Services

EU Council Directive
Critical
Infrastructures
(2008)

EU Cybercrime
Directive
(2013)

PSD2 Directive
(2015)

EU NIS Directive
(2016)

General Data
Protection
Regulation
(2016)

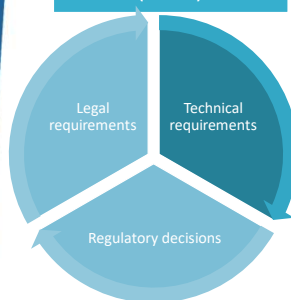
Free-flow of Non-
personal Data
Regulation
(2018)

European Electronic
Communications
Code
(2018)

ePrivacy Regulation
(20xx?)

Directive on Open
Data and PSI
(2019)

Cybersecurity Act
(2019)



8

TRACK 03

System
&
Infrastructure
Security

- THEME 1
System Security
- THEME 2
Network Security
- THEME 3
Security Monitoring and Management

9

2018 Tesla Key fob hack: cloning a key fob in 2 seconds

<https://www.youtube.com/watch?v=aVlYuPzmJoY>

<https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/>

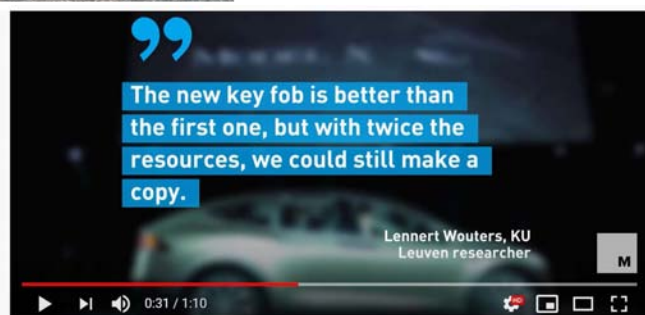


2017: Responsible disclosure (12 months)

2018: new key fobs with proper 80-bit keys (DST-80)

2019: Cloning new fob takes 4 seconds

New responsible disclosure
Over the air update possible



#Tesla #Hackers #ElonMusk
Tesla Model S HACKED AGAIN!

5,279 views • Sep 4, 2019

72 17 SHARE SAVE

**TRACK
04**

Technology
Building
Blocks

- THEME 1
Secure hardware
- THEME 2
Cryptographic algorithms
- THEME 3
Cryptographic protocols
- THEME 4
Secure and efficient cryptographic implementations

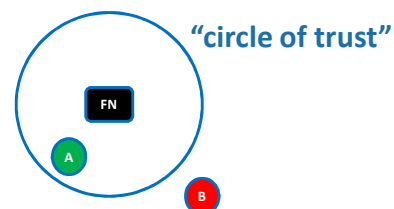
11


Secure RF distance bounding for Bluetooth

Defeating relay attacks



Relay attack Solihull





01 Bart Jacobs

02 Frederik Vercauteren

03 Frank Piessens

04 Ingrid Verbauwhede

TRACK 01 TRACK 02 TRACK 03 TRACK 04

13

EXCELLENCE and DEMAND

Leverage on existing and available excellence

Top Class Basic Research

Top 10 in Europe

A Broad, one-Stop-Shop for ICT Security Research

TRACK 01 TRACK 02 TRACK 03 TRACK 04

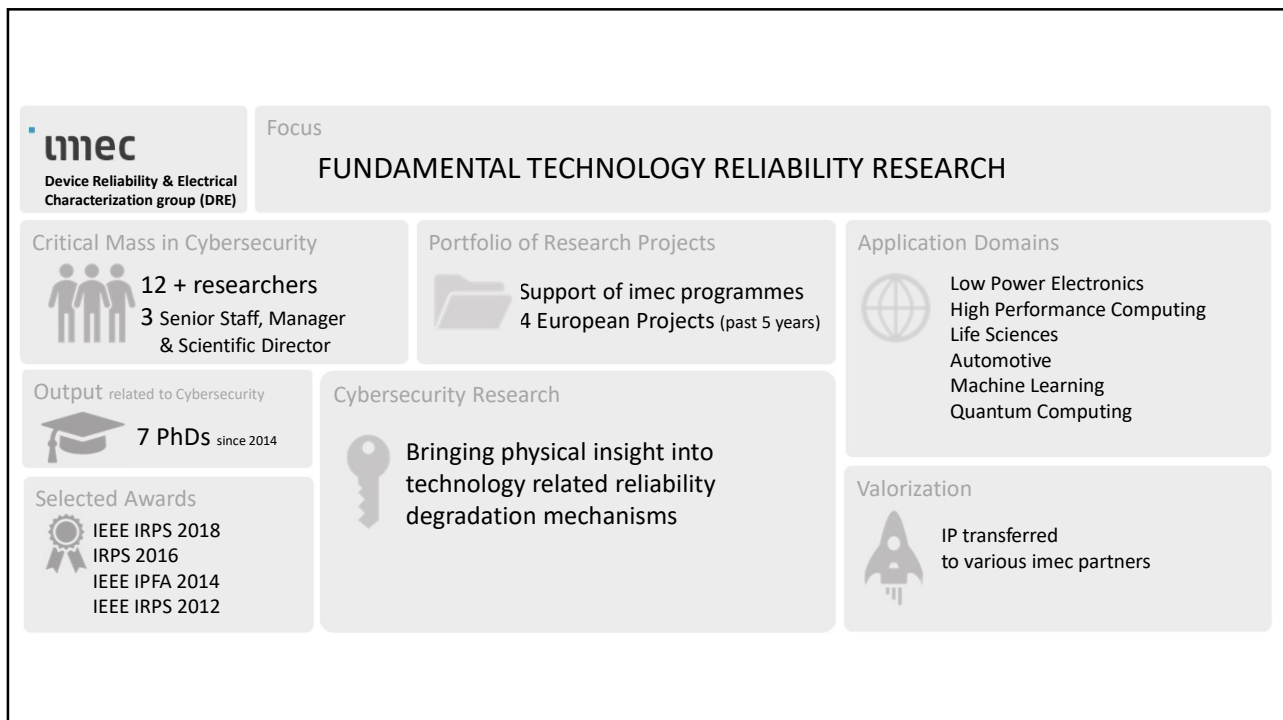
14

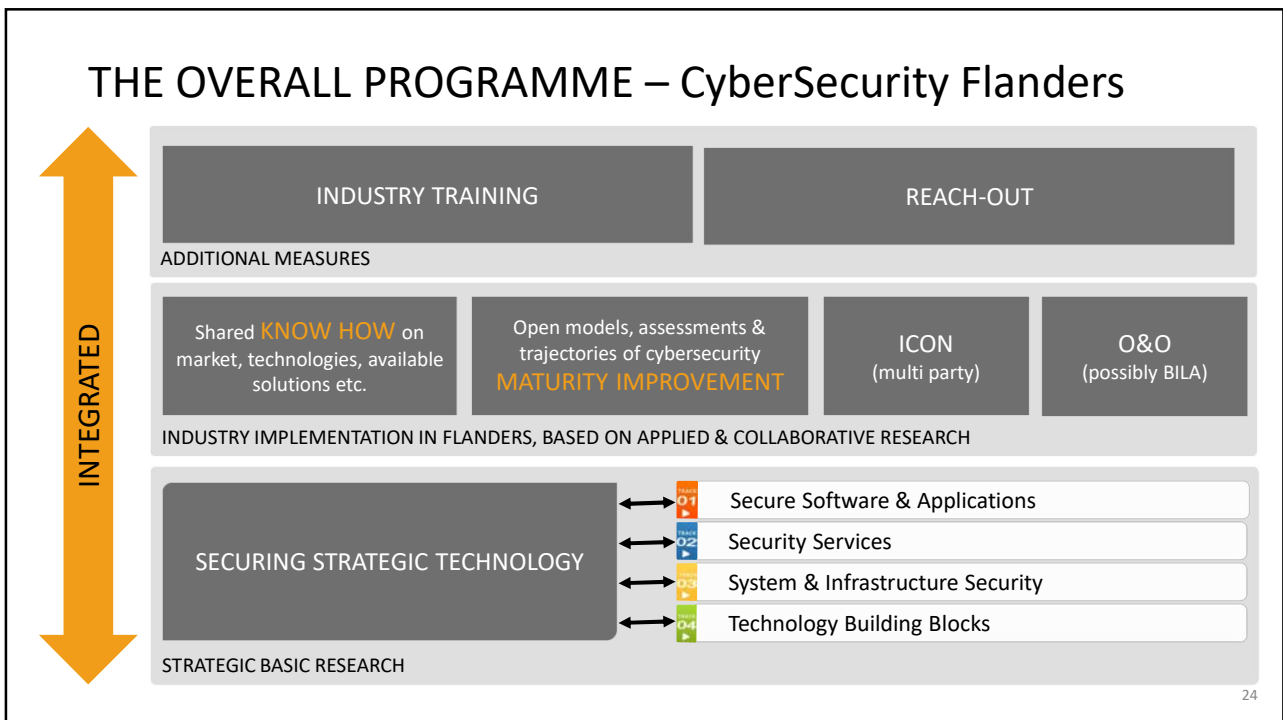
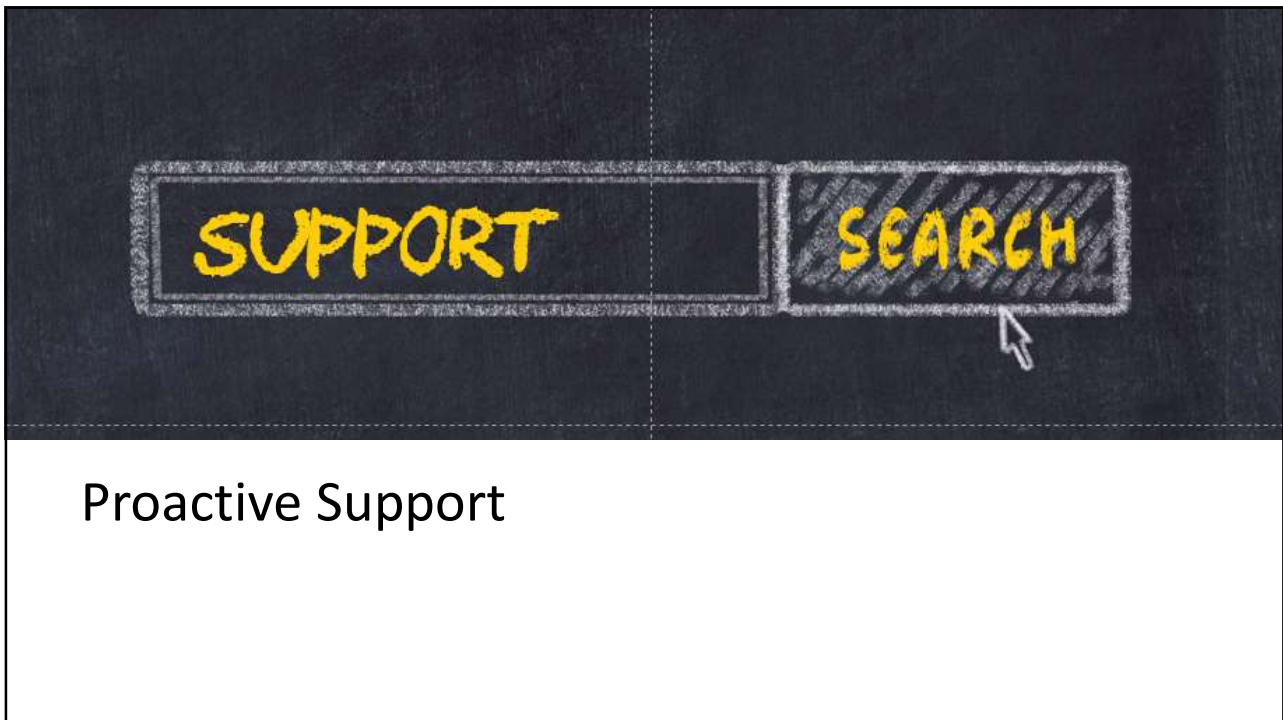


TRACK 01 Secure Software & Applications	TRACK 02 Security Services	TRACK 03 System & Infrastructure Security	TRACK 04 Technology Building Blocks
Secure SDLC – Secure Software Development Life Cycle	Identity Management and Authentication	System Security	Secure Hardware: Roots of Trust Anchored into Technology Foundations
(RA 1.1.1) Cybersecurity Requirements	(RA 2.1.1) Identity	(RA 3.1.1) Protection Against Software-Controlled Side-Channel Attacks (on general purpose hardware)	(RA 4.1.1) Developing PUFs
(RA 1.1.2) Cybersecurity-by-Design Solutions	(RA 2.1.2) Frictionless Authentication: Collaborative and Continuous	(RA 3.1.2) Processor Extension to Support New System Security Models	(RA 4.1.2) True Random Number Generators
(RA 1.1.3) Security Analysis for Existing Applications	(RA 2.1.3) Privacy-preserving Identity and Authentication	(RA 3.1.3) Security and Safety In Mixed Criticality Systems	(RA 4.1.3) Technology Solutions to Secure Circular Economy
Program Verification	Authorization and Audit	(RA 3.1.4) Diversity-based Multi-Variant Execution Mitigation Techniques for System Defense	Cryptographic Algorithms
(RA 1.2.1) Formal Program Verification	(RA 2.2.1) Enhancing Authorization Capabilities	Network Security	(RA 4.2.1) Symmetric-key Algorithms
(RA 1.2.2) Incremental Static Application Security Testing (SAST) for Distributed Applications	(RA 2.2.2) Intelligent Audit	(RA 3.2.1) Study of Critical Internet Components and Protocols	(RA 4.2.2) Public-key Algorithms
(RA 1.2.3) Efficient Runtime Application Security Protection (RASP) for Distributed Applications	(RA 2.2.3) Synergy between Audit and Authorization	(RA 3.2.2) Secure Communication Protocols for the IoT	(RA 4.2.3) Proofs and Validation
Secure Programming Languages and Secure Compilation	Advanced Encryption Techniques and Data Access Middleware	(RA 3.2.3) Analysis of Protocol Implementations	Cryptographic Protocols
(RA 1.3.1) Mechanically-verified Security Proofs for Capability Machine Programs	(RA 2.3.1) Secure Outsourced Data Processing	Security Monitoring and Management	(RA 4.3.1) Cryptographic Protocols for Distance Bounding
(RA 1.3.2) Specifying and Proving Security Properties of Side-Effecting Programs	(RA 2.3.2) Secure Collaborative Data Processing	(RA 3.3.1) Intelligence Gathering and Identification of Security State	(RA 4.3.2) Cryptographic Protocols Design for MPC Applications
(RA 1.3.3) Language-embedded Security Policies for Distributed Micro-services.	(RA 2.3.3) Data Access Middleware	(RA 3.3.2) Methods and Tools for Secure Deployment	(RA 4.3.3) Cryptographic Protocols for Blockchain
	Policy and Regulation	(RA 3.3.3) Detection and Response for IoT and Industrial Control Systems	(RA 4.3.4) Cryptographic Protocols for Mix Networks
	(RA 2.4.1) Legal Compliance Analysis		(RA 4.3.5) Security Analysis of Cryptographic Protocols
	(RA 2.4.2) Policy Analysis		Secure and Efficient Cryptographic Implementations
	(RA 2.4.3) Legal Engineering Analysis		(RA 4.4.1) Implementation Challenges of Post-quantum, FHE, Lightweight Crypto on Novel Compute Platforms
			(RA 4.4.2) Side-Channel and Fault Attacks
			(RA 4.4.3) White-Box Cryptography

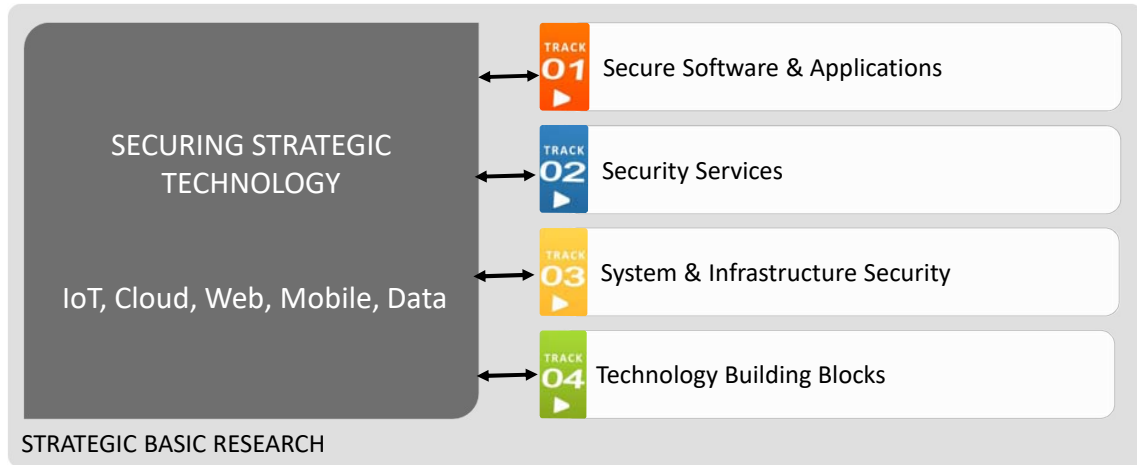








Prototypes and environments that combine multiple results



ICON and O&O

Danny De Cock, Bert Lagaisse, Sam Michiels, Svetla Nikova, Dave Singelée, Bjorn De Sutter, Coen De Roover, Peggy Valcke, Els Kindt



Danny De Cock



Bert Lagaisse



Sam Michiels



Svetla Nikova



Dave Singelée



Bjorn De Sutter



Coen De Roover



Els Kindt



COOCK

L-SEC, B-Hive, Sirris, ...

Lieven Desmet, Svetla Nikova



Lieven Desmet



Svetla Nikova



27

TETRA

Nele Mentens, Vincent Naessens
& Stijn Volckaert



Nele Mentens



Vincent Naessens



Stijn volckaert



28

Baekeland

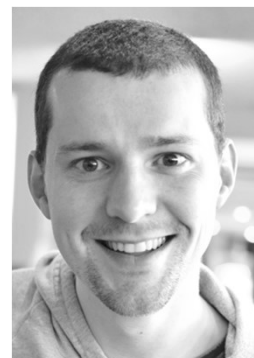
Bart Preneel & Wouter Joosen



29

Specialized Education and Industry Training

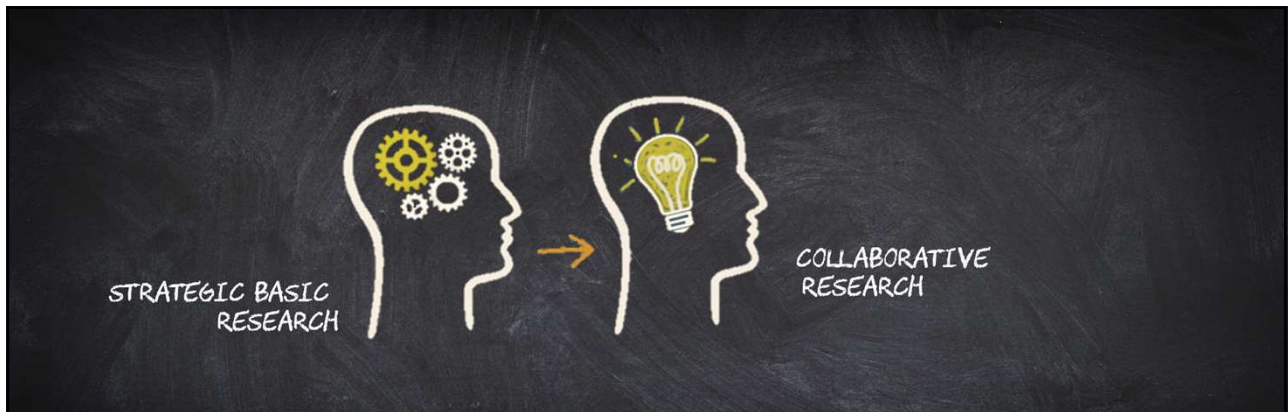
Pieter Philippaerts, Wouter Joosen, Bart Preneel



Pieter Philippaerts



30



THANK YOU