European Organization for Particle Physics

Exploring the frontiers of knowledge

ZEEK AND THE BALANCE BETWEEN ACADEMIC FREEDOM, INDUSTRIAL OPERATIONS & SECURITY

Liviu Vâlsan
CERN Computer Security Team
25th of March 2026 - Zeek Workshop CERN 2026

Founded in 1954

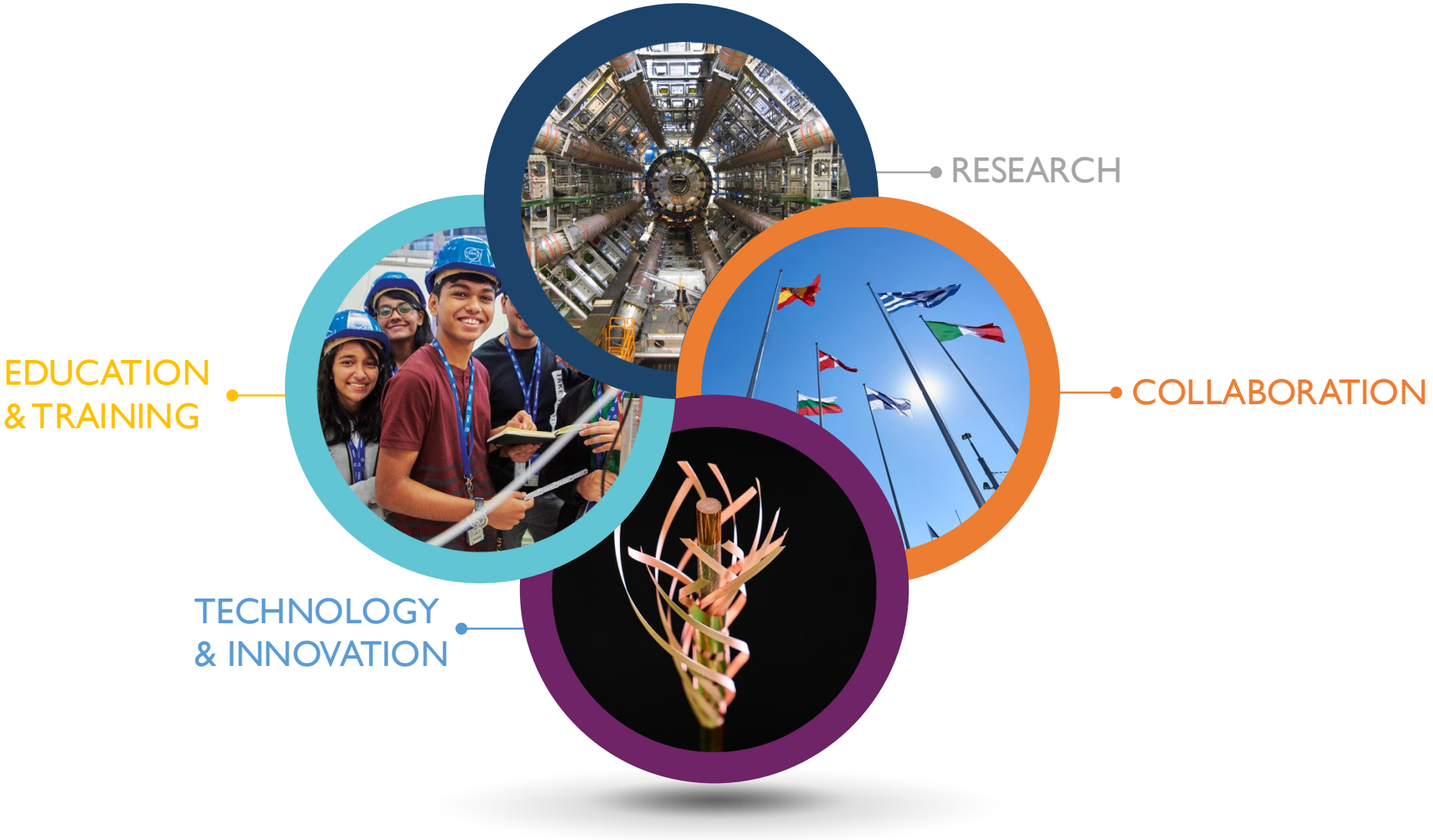
Science for Peace

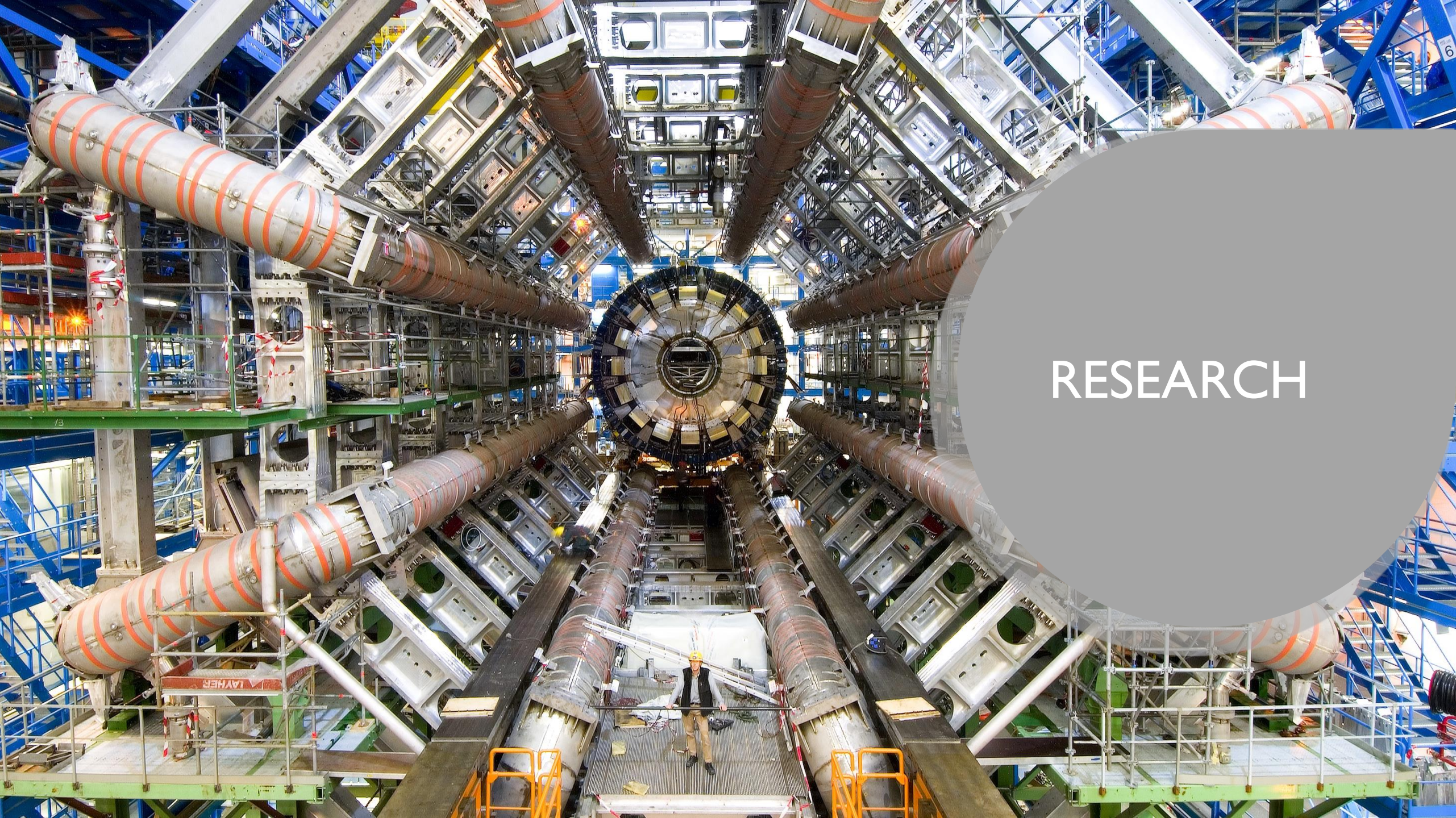
CERN is the European Laboratory for Particle Physics

Our goal is to understand the most fundamental particles and laws of the universe

Straddling the Franco-Swiss border near Geneva

Four pillars underpin CERN's mission

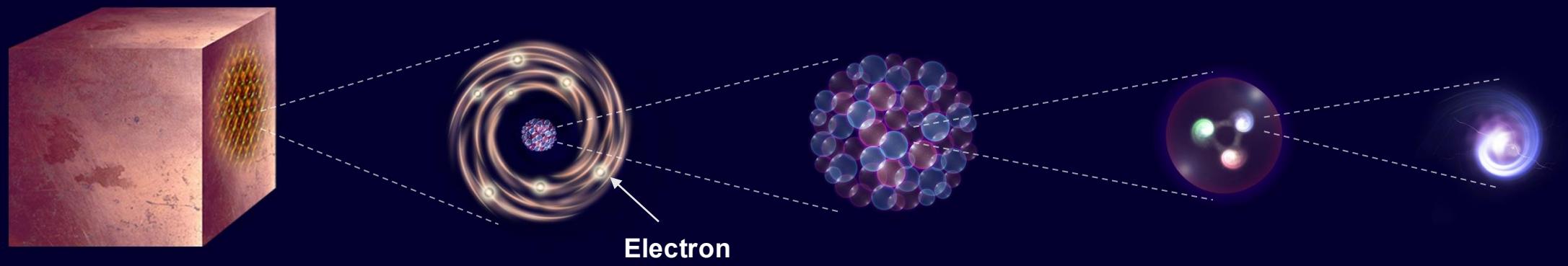


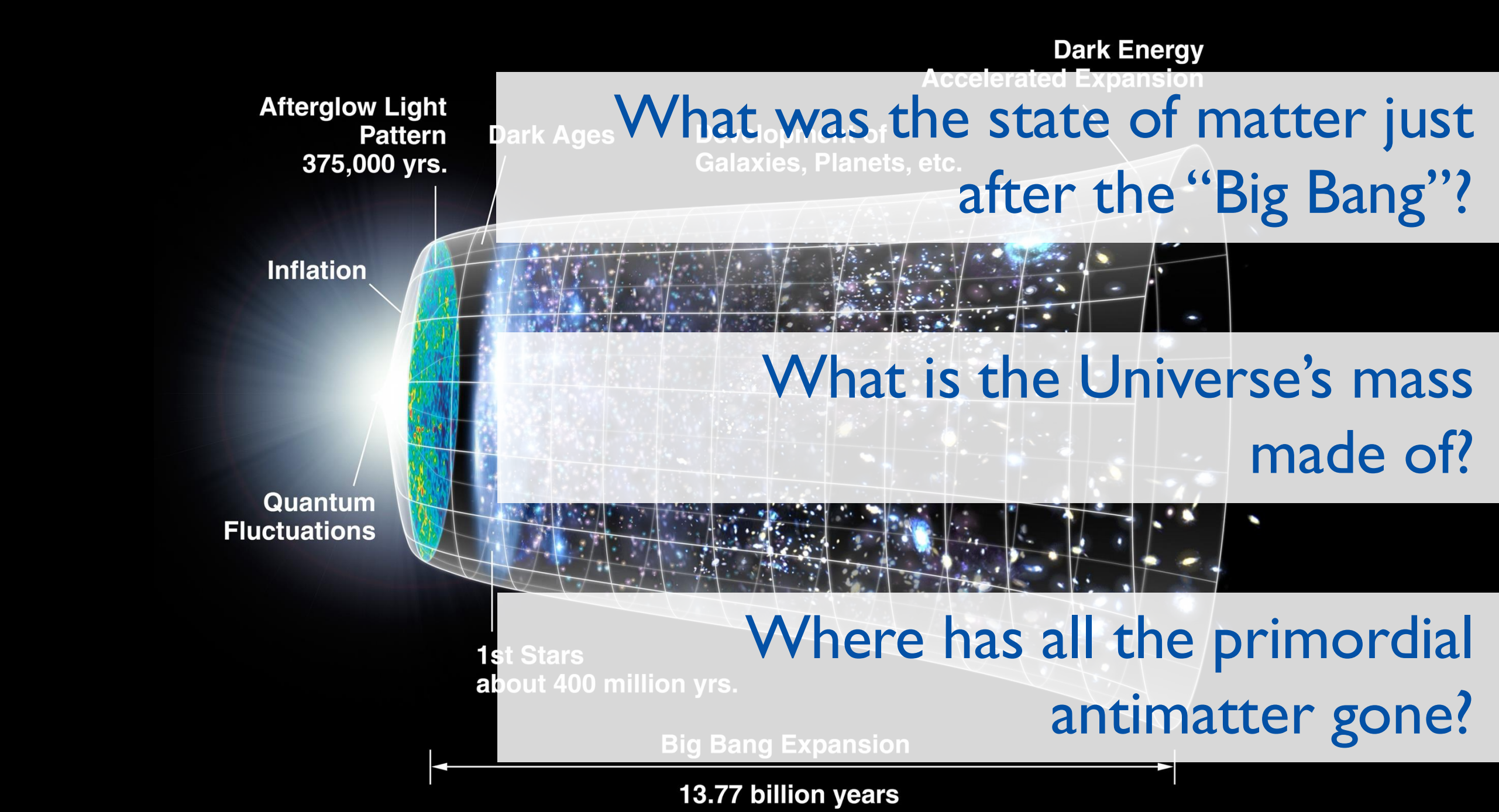


RESEARCH

What is the universe made of?

We study the elementary building blocks of matter and the forces that control their behaviour



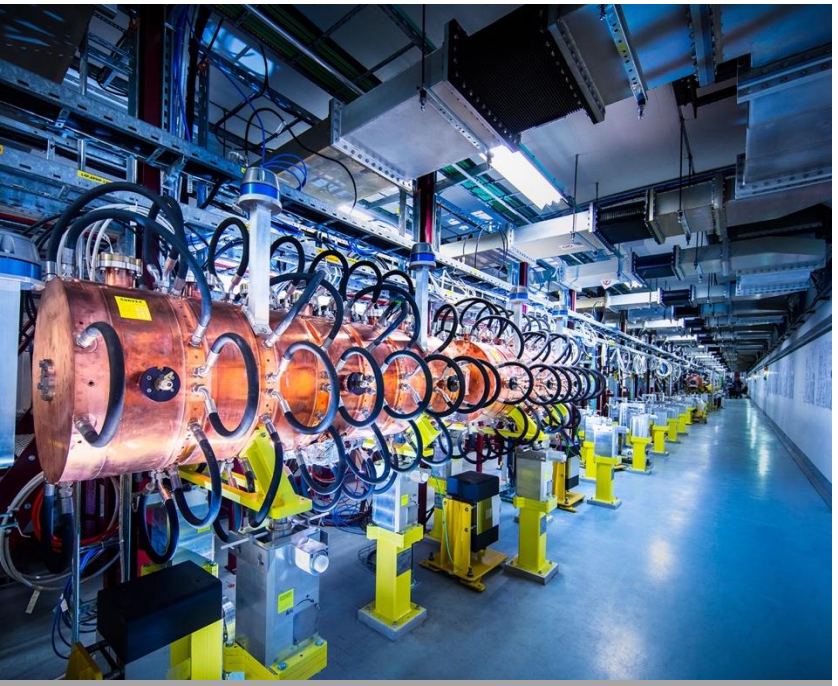


What was the state of matter just after the "Big Bang"?

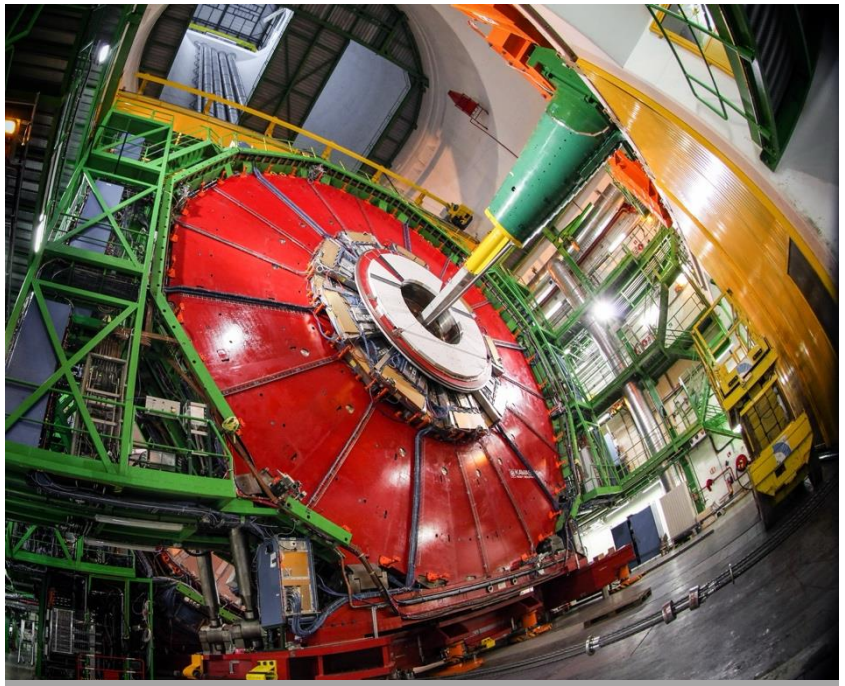
What is the Universe's mass made of?

Where has all the primordial antimatter gone?

To answer these questions, we develop technologies in three key areas

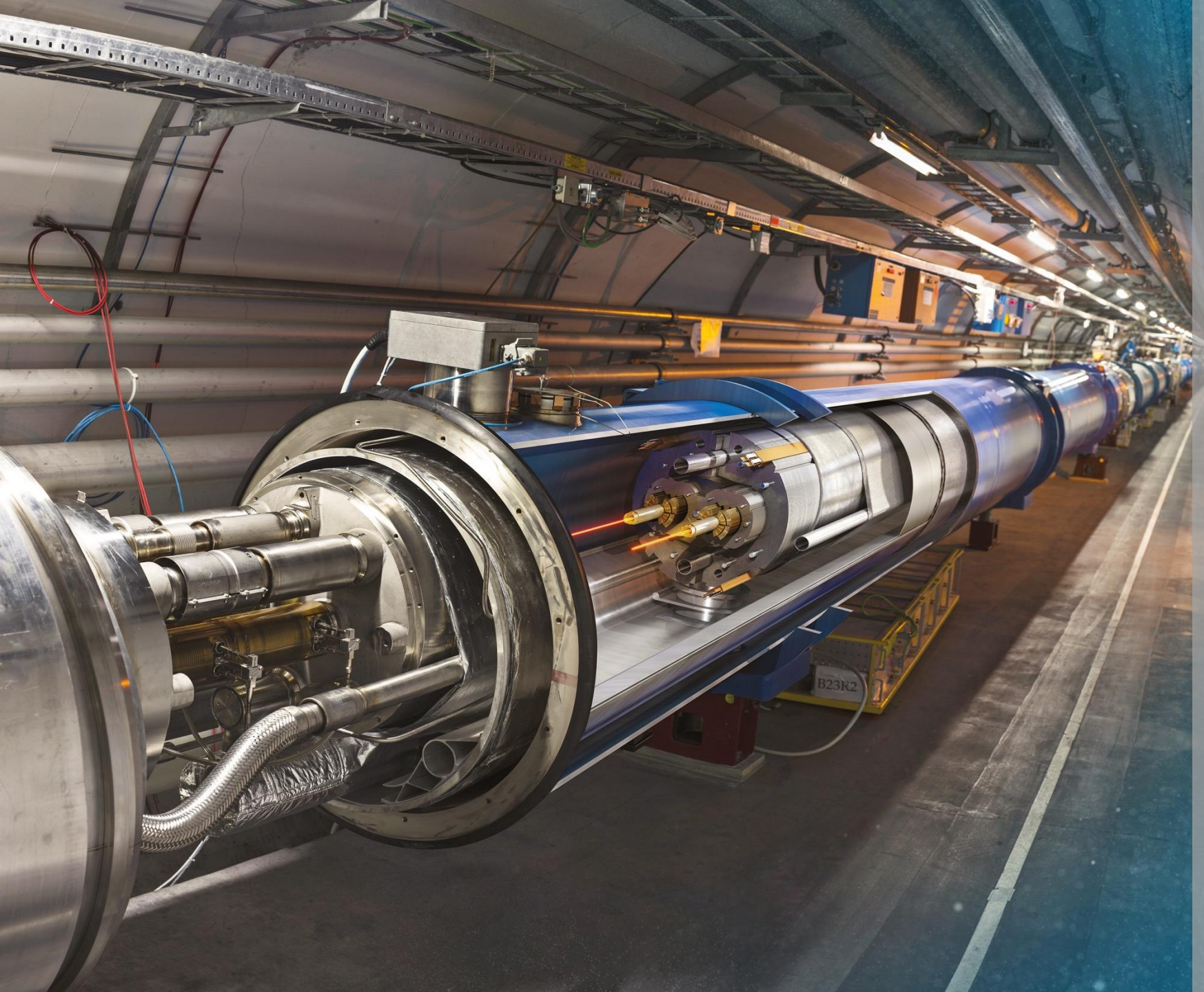


ACCELERATORS



DETECTORS

COMPUTING



Large Hadron Collider (LHC)

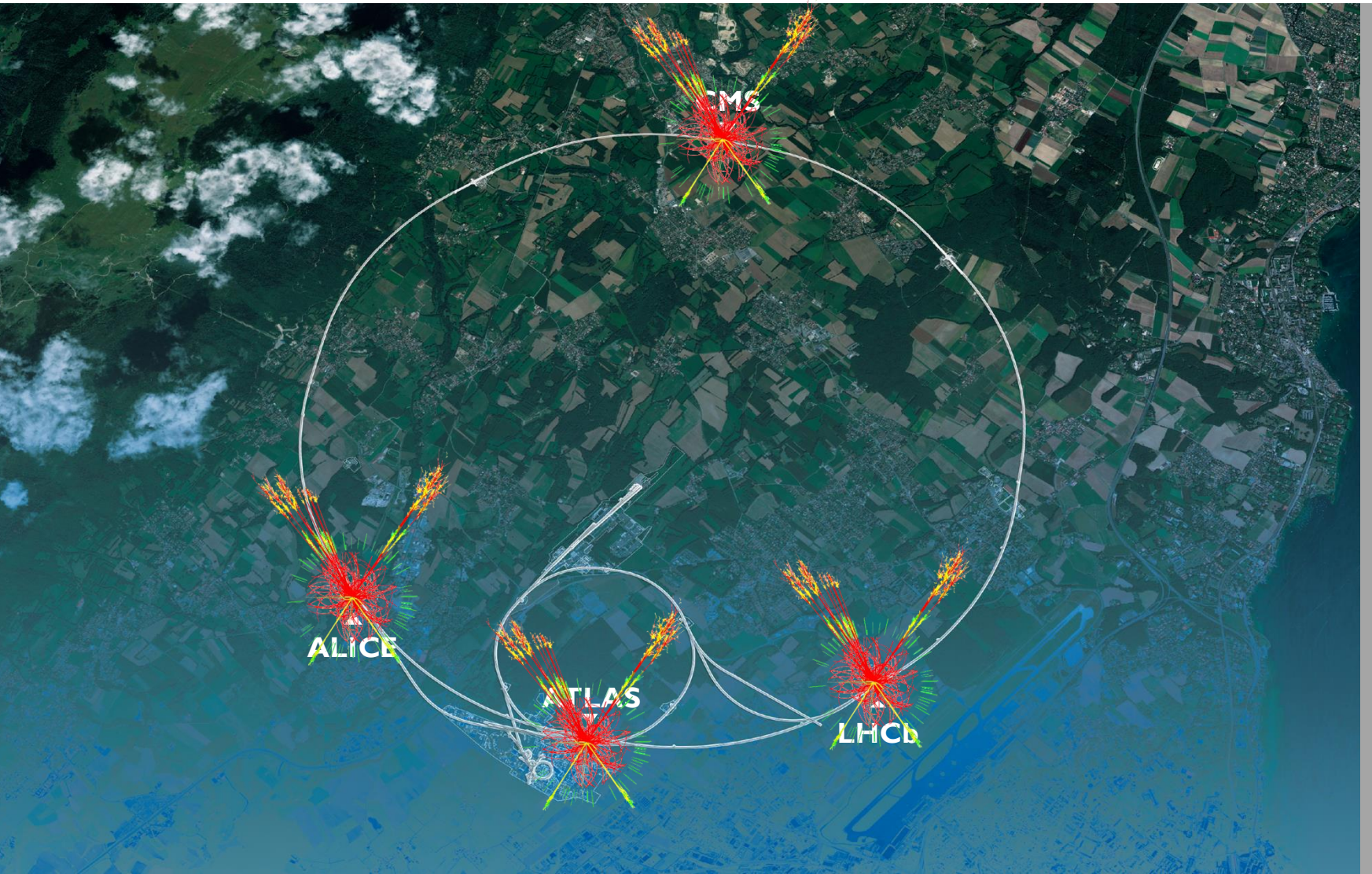
- 27 km in circumference
- About 100 m underground
- Superconducting magnets steer the particles around the ring
- Particles are accelerated to close to the speed of light
- ~ 11 000 turns / sec, 25 ns bunch spacing

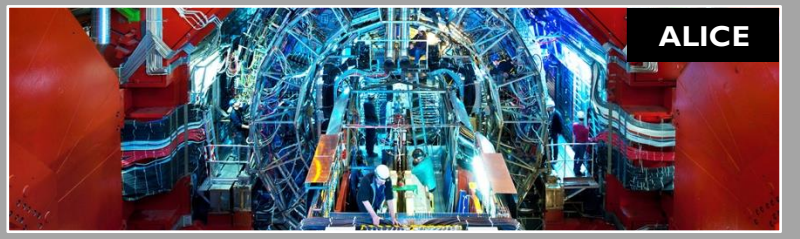
Current: 11,000 A

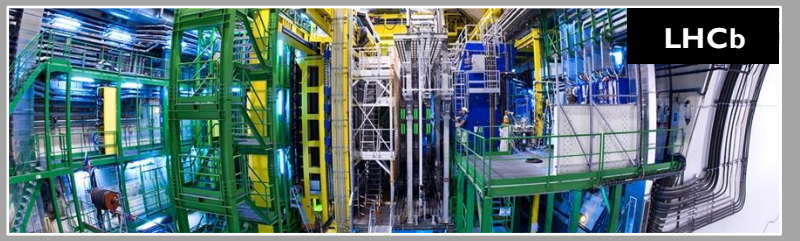
Superconducting: -271° C
(1.9 K) cold

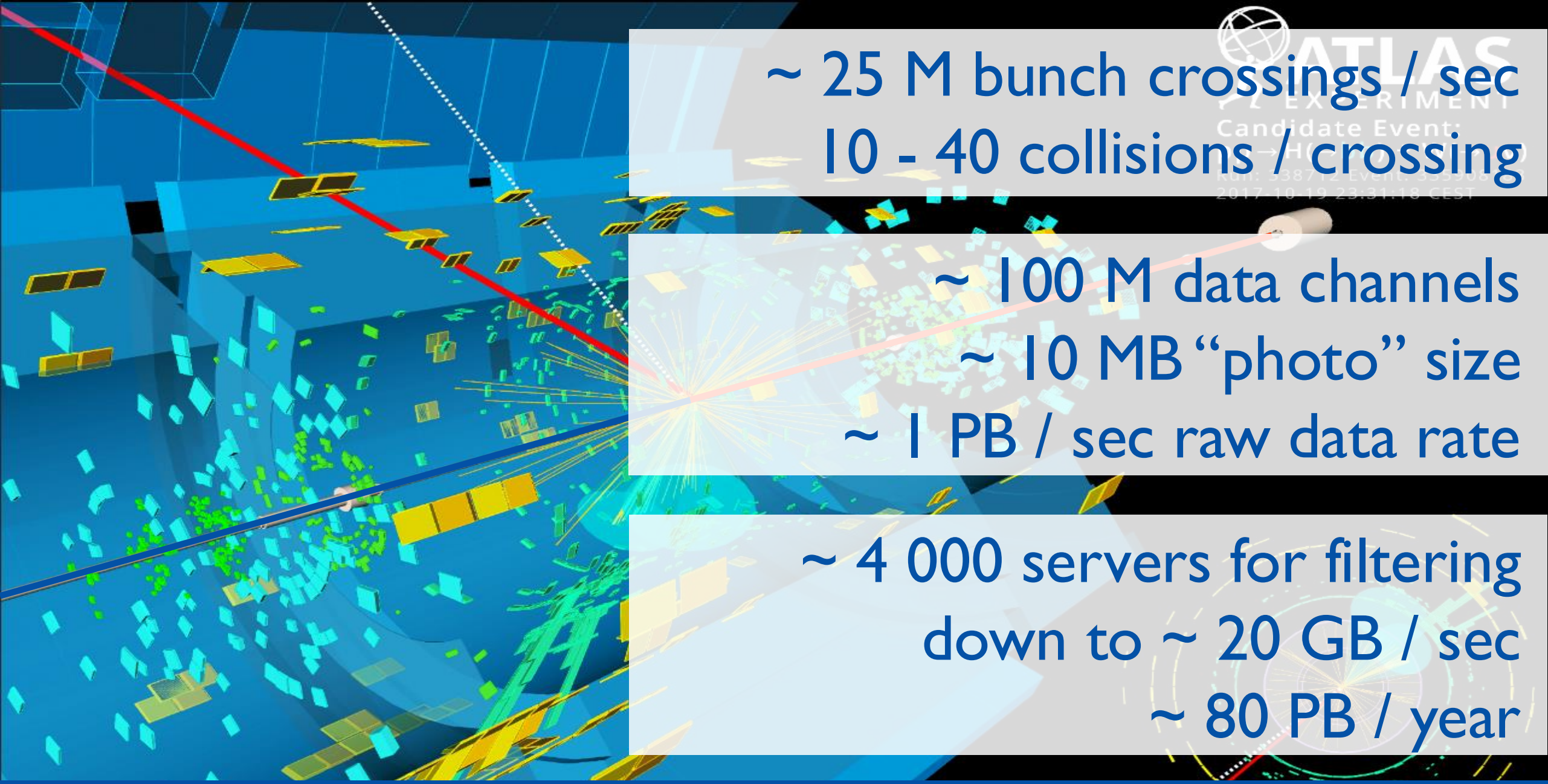
Stored energy:
2 × 80 kg of TNT equiv.

Giant detectors record the particles formed at the four collision points









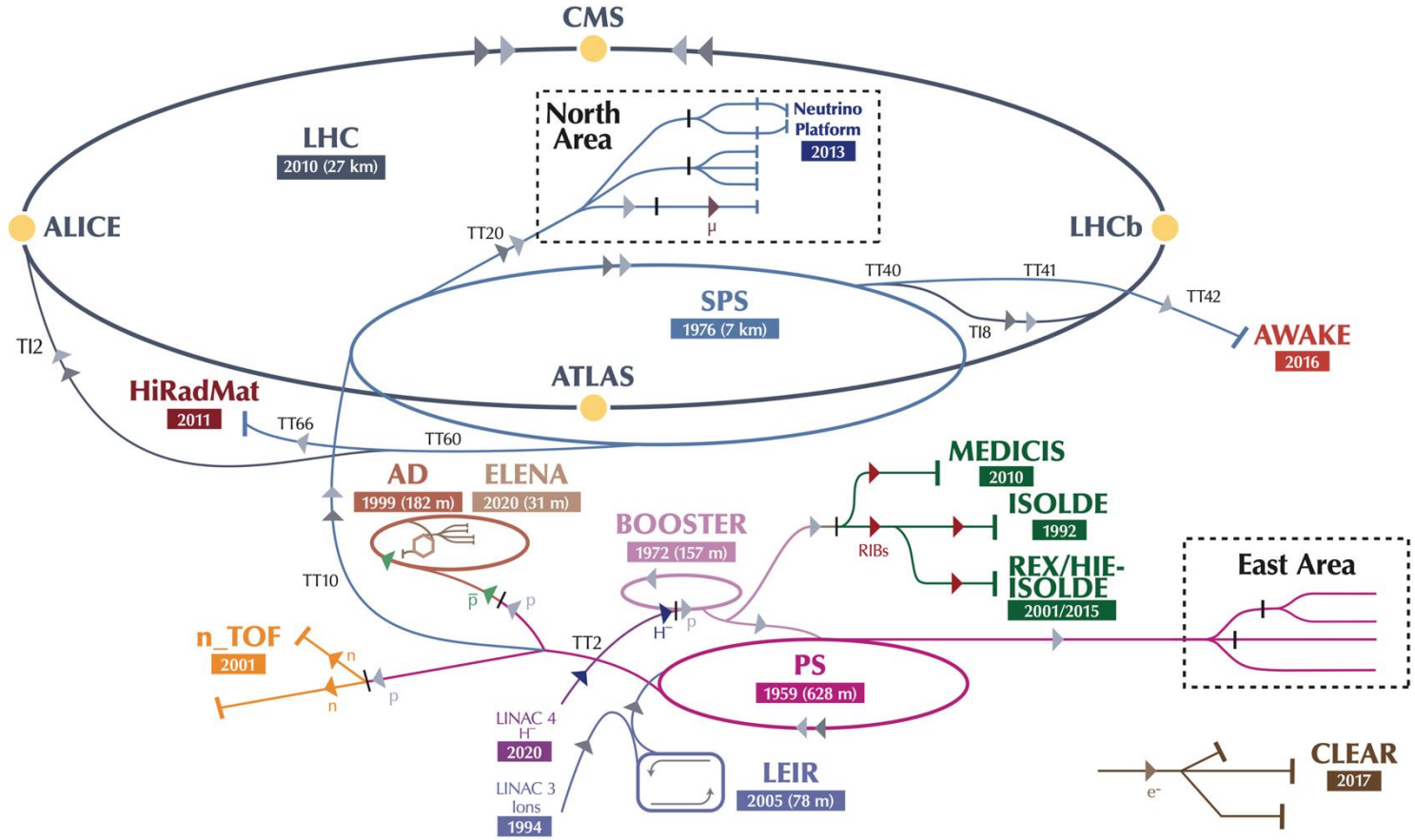
~ 25 M bunch crossings / sec
10 - 40 collisions / crossing

~ 100 M data channels
~ 10 MB "photo" size
~ 1 PB / sec raw data rate

~ 4 000 servers for filtering
down to ~ 20 GB / sec
~ 80 PB / year

3D "Photo" of a collision from the LHC

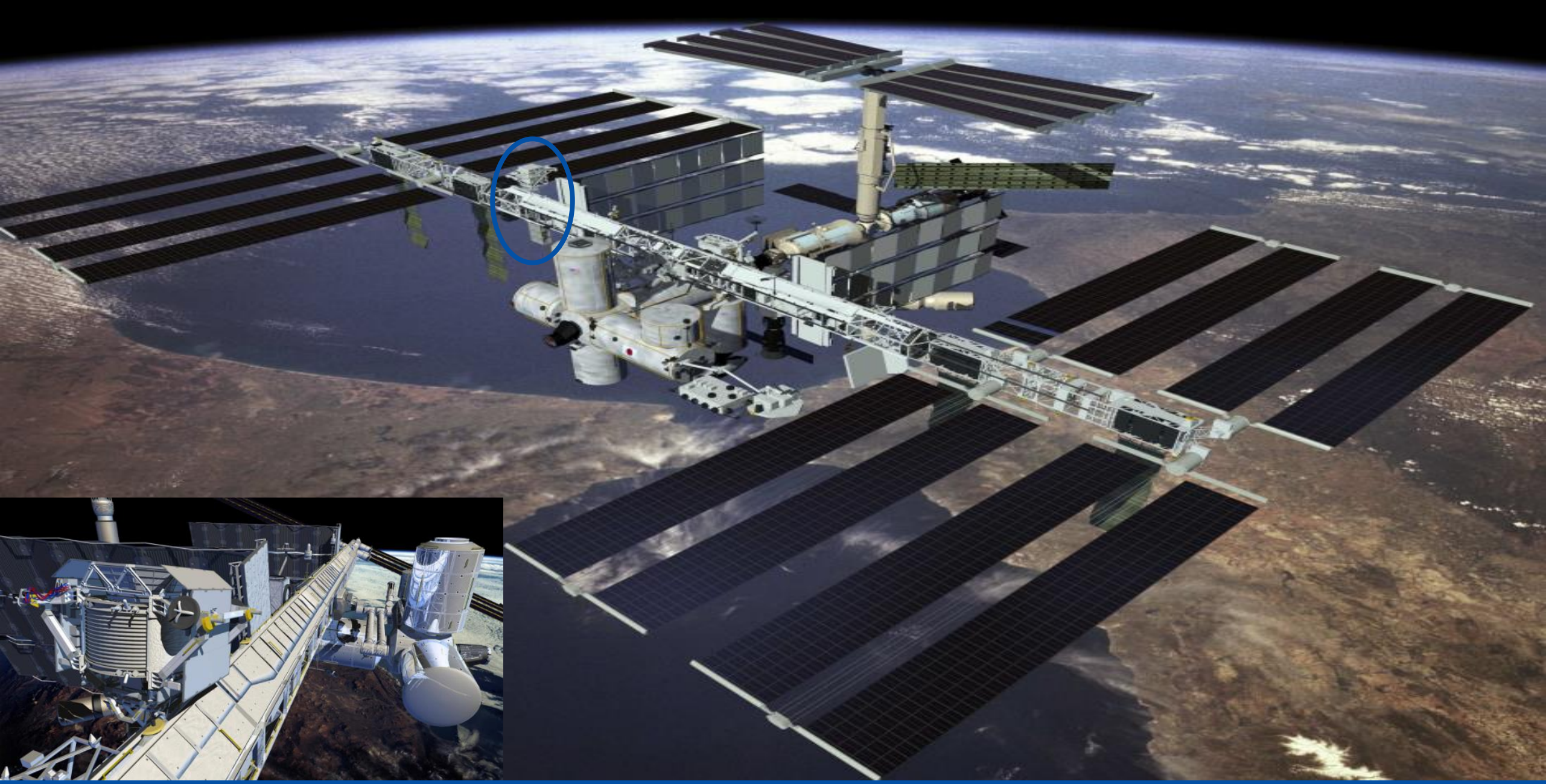
The CERN accelerator complex
Complexe des accélérateurs du CERN



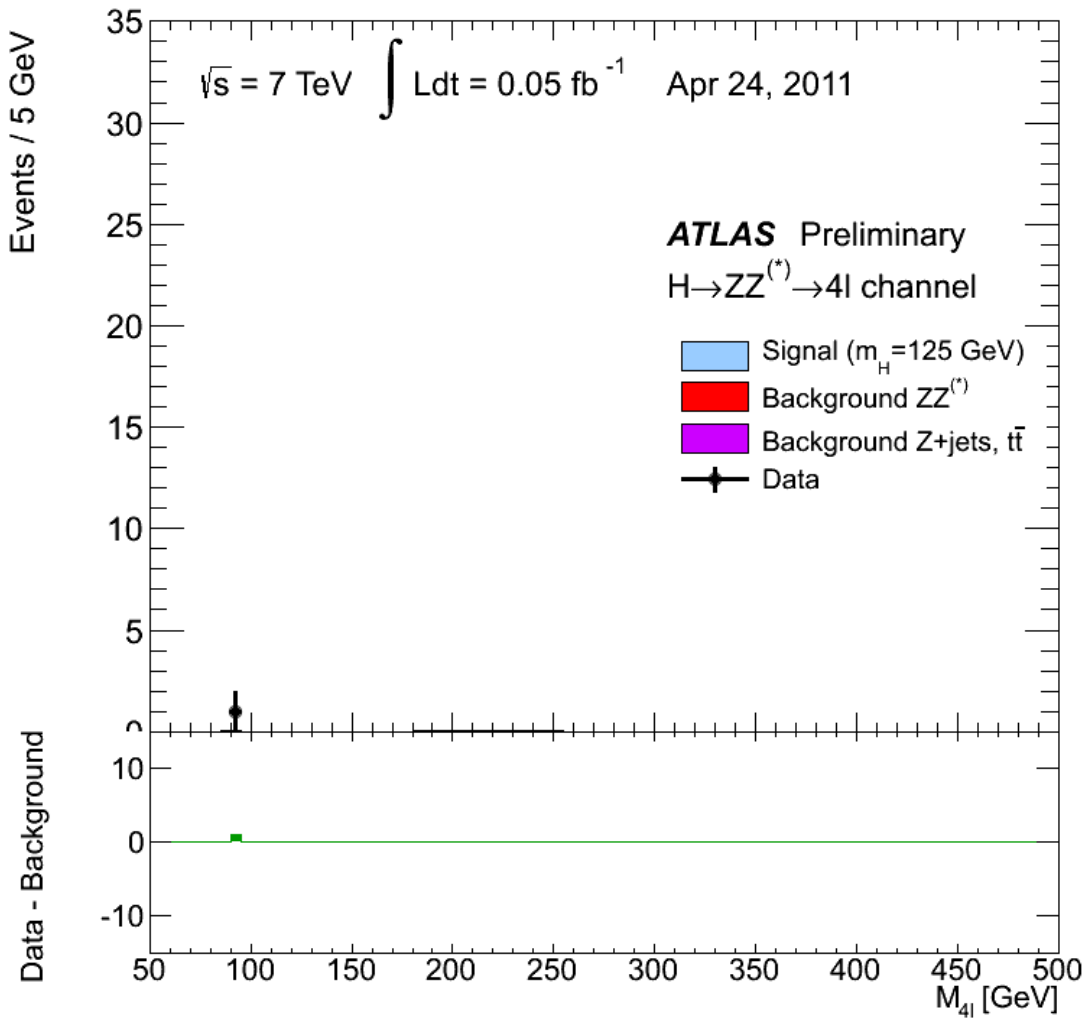
H⁻ (hydrogen anions) · p (protons) · ions · RIBs (Radioactive Ion Beams) · n (neutrons) · $\bar{p}$ (antiprotons) · e^- (electrons) · μ (muons)

LHC - Large Hadron Collider // SPS - Super Proton Synchrotron // PS - Proton Synchrotron // AD - Antiproton Decelerator // CLEAR - CERN Linear Electron Accelerator for Research // AWAKE - Advanced WAKefield Experiment // ISOLDE - Isotope Separator OnLine // REX/HIE-ISOLDE - Radioactive EXperiment/High Intensity and Energy ISOLDE // MEDICIS // LEIR - Low Energy Ion Ring // LINAC - LINear ACcelerator // n_TOF - Neutrons Time Of Flight // HiRadMat - High-Radiation to Materials // Neutrino Platform

January 2026

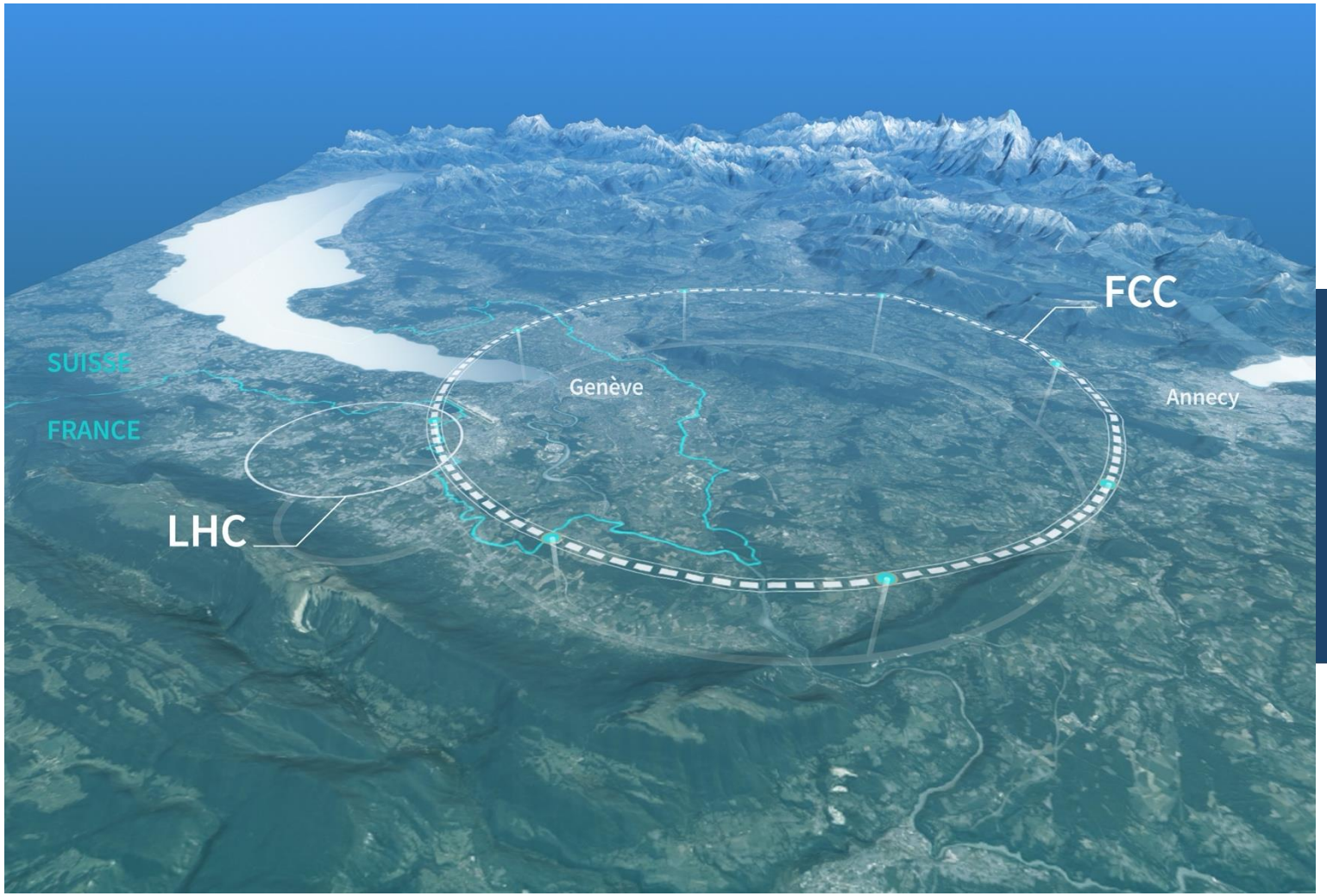


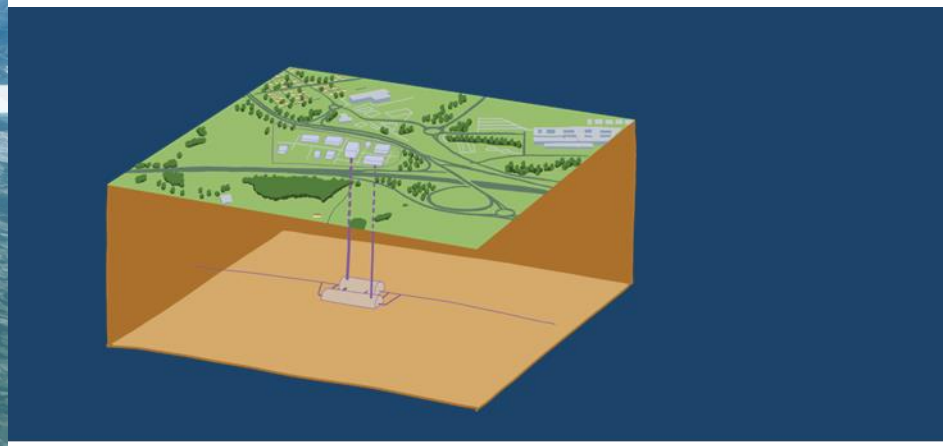
AMS: A Detector in Space



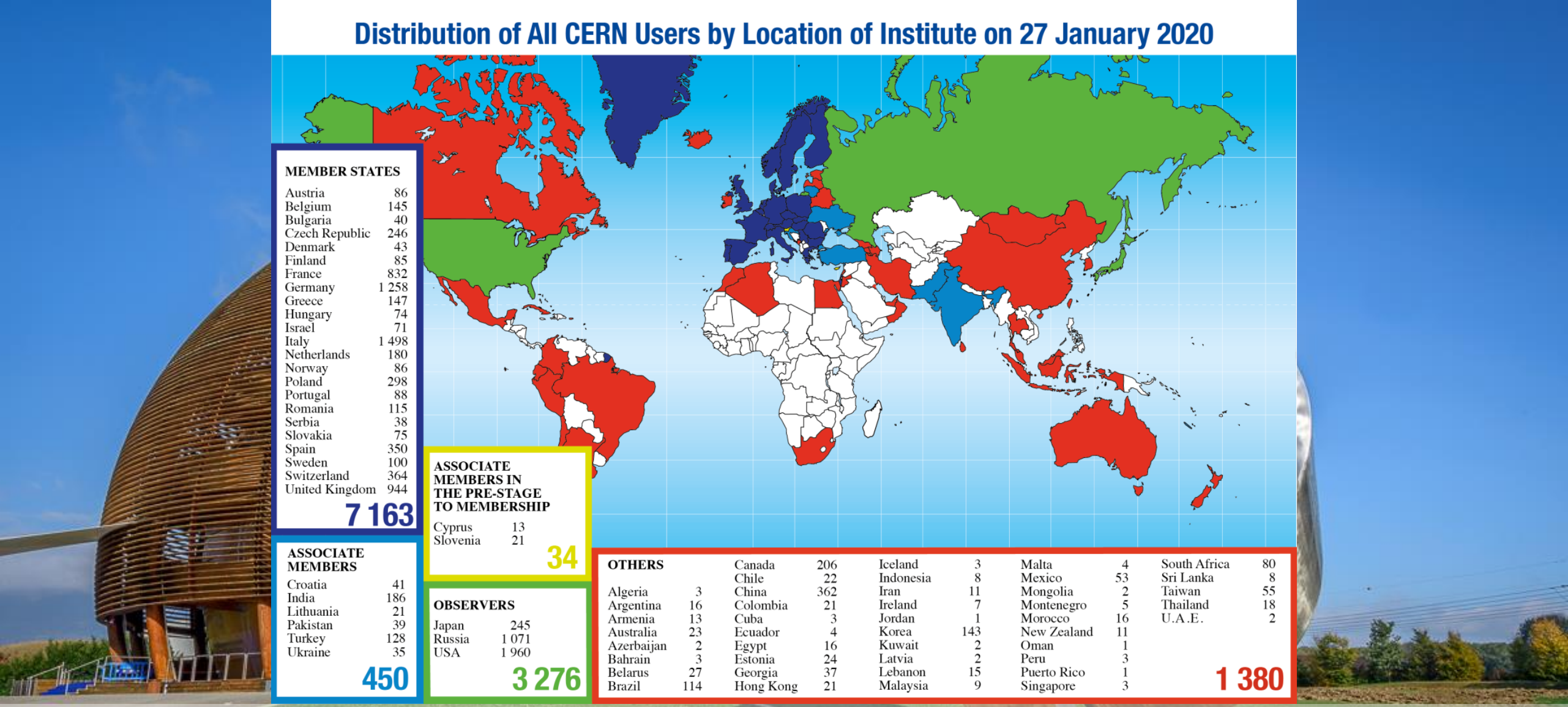
Return on Investment

Preparing CERN's future





COLLABORATION



CERN has 25 member states and supports a global community of 12 000 researchers

Science for peace

CERN was founded in 1954 with 12 European Member States

CERN's annual budget is 1200 MCHF (equivalent to a medium-sized European university)

Employees:
2704 staff,
1181 graduates and fellows
Associates:
12406 users, **1401** others

25 Member States

Austria – Belgium – Bulgaria – Czech Republic
Denmark – Estonia – Finland – France – Germany
Greece – Hungary – Israel – Italy – Netherlands
Norway – Poland – Portugal – Romania – Serbia
Slovakia – Slovenia – Spain – Sweden – Switzerland
United Kingdom

10 Associate Member States

Brazil – Croatia – Cyprus – India – Ireland – Latvia Lithuania – Pakistan – Türkiye – Ukraine

4 Observers

Japan – USA – European Union – UNESCO

~ 50 Cooperation Agreements

Albania – Algeria – Argentina – Armenia – Australia – Azerbaijan – Bahrain – Bangladesh – Bolivia – Bosnia and Herzegovina
Canada – Chile – Colombia – Costa Rica – Cuba – Ecuador – Egypt – Georgia – Ghana – Honduras – Hong Kong –Iceland
Indonesia – Iran – JINR – Jordan – Kazakhstan – Kuwait – Lebanon – Madagascar – Malaysia – Malta – Mexico – Mongolia
Montenegro – Morocco – Mozambique – Nepal – New Zealand – North Macedonia – Oman – Palestine – Paraguay
People's Republic of China – Peru – Philippines – Qatar – Republic of Korea – Rwanda – Saudi Arabia – Singapore
South Africa – Sri Lanka – Taiwan – Thailand – Tunisia – United Arab Emirates – Uruguay – Uzbekistan – Vietnam

Data as of 31 December 2024

A laboratory for people around the world

Distribution of all CERN Users by the location of their home institute

Geographical & cultural diversity
Users of **110 nationalities**
24.7 % women

Member States (7704)

Austria 88 – **Belgium** 142 – **Bulgaria** 49 – **Czech Republic** 250
Denmark 50 – **Estonia** 27 – **Finland** 88 – **France** 856 – **Germany** 1260
Greece 101 – **Hungary** 84 – **Israel** 75 – **Italy** 1657 – **Netherlands** 174
Norway 88 – **Poland** 363 – **Portugal** 110 – **Romania** 110 – **Serbia** 42
Slovakia 72 – **Slovenia** 29 – **Spain** 448 – **Sweden** 103 – **Switzerland** 409
United Kingdom 1029

Associate Member States (613)

Brazil 141 – **Croatia** 35 – **Cyprus** 12 – **India** 158 – **Ireland** 11
Latvia 22 – **Lithuania** 21 – **Pakistan** 35 – **Türkiye** 151 – **Ukraine** 27

Observers (2330)

Japan 229 – **United States of America** 2101

Data as of 31 December 2024

Cooperation Agreements (1759)

Albania 7 – **Algeria** 1 – **Argentina** 17 – **Armenia** 28 – **Australia** 31 – **Azerbaijan** 2 – **Bahrain** 10 – **Canada** 203
Chile 58 – **Colombia** 25 – **Costa Rica** 8 – **Cuba** 3 – **Ecuador** 4 – **Egypt** 22 – **Georgia** 36 – **Hong Kong** 17 – **Iceland** 3
Indonesia 8 – **Iran** 18 – **JINR** 305 – **Jordan** 2 – **Kazakhstan** 8 – **Kuwait** 2 – **Lebanon** 12 – **Madagascar** 1 – **Malaysia** 1 **Malta** 3
– **Mexico** 66 – **Montenegro** 4 – **Morocco** 22 – **New Zealand** 1 – **Nigeria** 1 – **Oman** 1 – **Palestine** 1
People's Republic of China 472 – **Peru** 3 – **Philippines** 1 – **Republic of Korea** 184 – **Saudi Arabia** 4 – **South Africa** 73
Sri Lanka 7 – **Taiwan** 49 – **Thailand** 17 – **Tunisia** 3 – **United Arab Emirates** 14 – **Vietnam** 1

TECHNOLOGY & INNOVATION

CERN DD/OC

Tim Berners-Lee, CERN/DD

Information Management: A Proposal

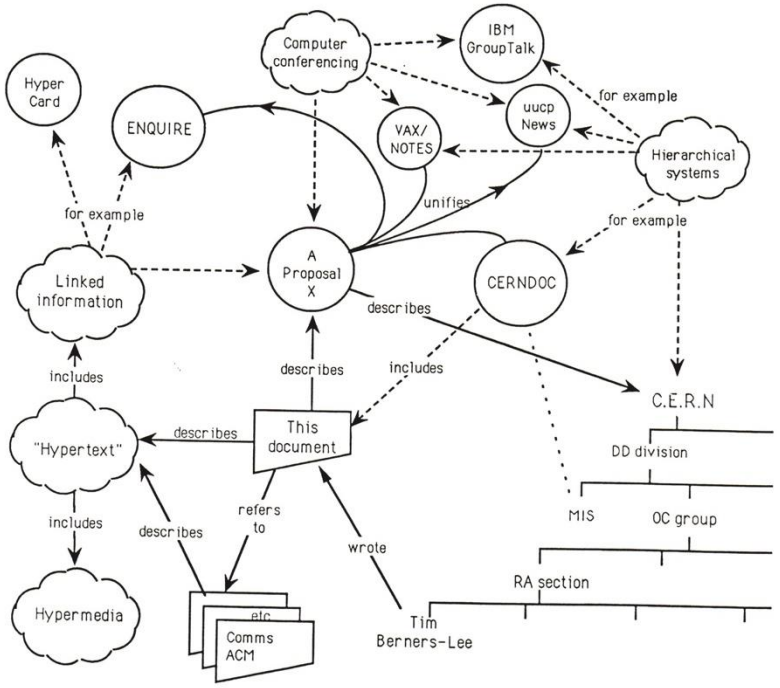
March 1989

Information Management: A Proposal

Abstract

This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext sytstem.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control



CERN is the birthplace of the World Wide Web

CERN's technological innovations have an important impact on society

Accelerator technologies for cancer radiotherapy with protons, ions and electrons.

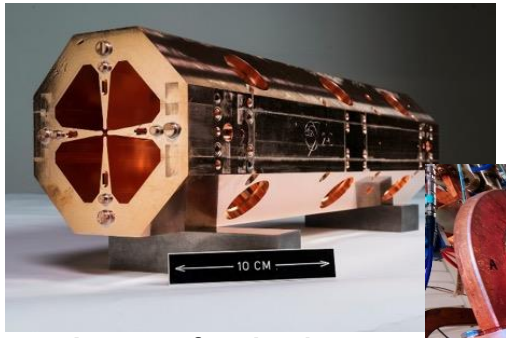
Pixel detector technologies for high-resolution 3D colour X-ray imaging.

Developing machine learning software for autonomous driving.

Cultural Heritage
InsightART

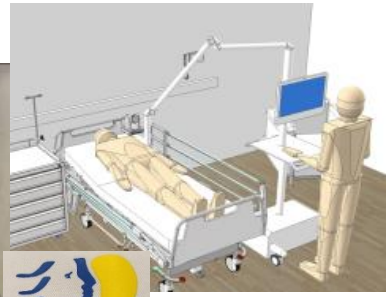
Measuring the DNA of your art.

Further Dissemination of our Technologies



Linacs for hadron therapy

Linacs for Very High Energy Electron Therapy



Patient monitoring

Medical ion sources

Open-Source

White Rabbit - timing through ethernet

Structured Laser Beams for Industry

Space Radiation Monitor

EDUCATION & TRAINING

CERN education and training programmes

1181 graduates
(including Research Fellows)

3 000 PhD students

300 Undergraduate students in Summer programmes

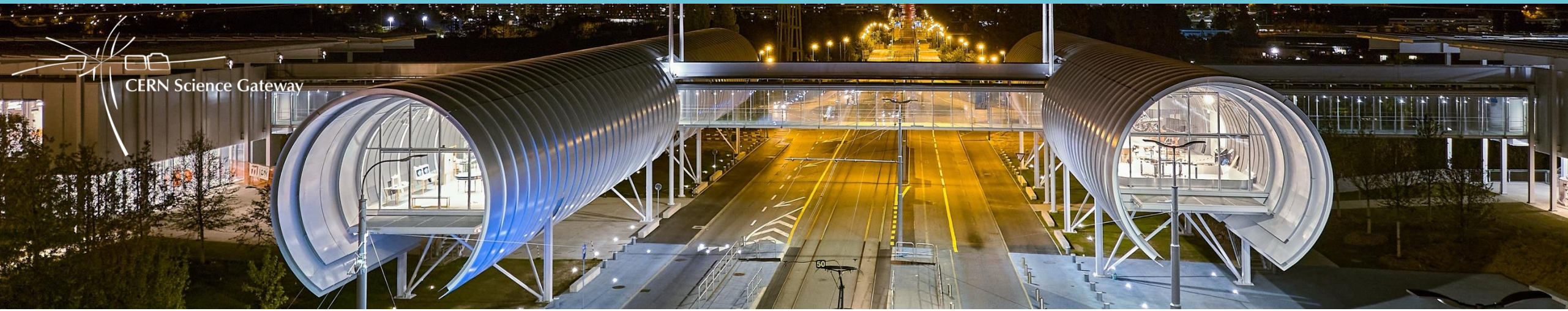
> 15 000 teachers participating in dedicated programmes, since 1998

2746 teams with more than 20 000 students in Beamline for Schools (BL4S) competition programme, since 2014

Visiting CERN https://visit.cern

The Science Gateway, inaugurated in October 2023. Free entry, open to everyone aged 5 and over.

400 000 visitors a year



Interactive exhibitions

Laboratory workshops

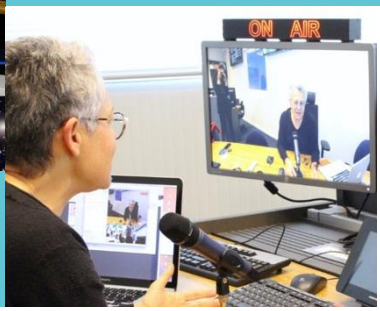
Science shows

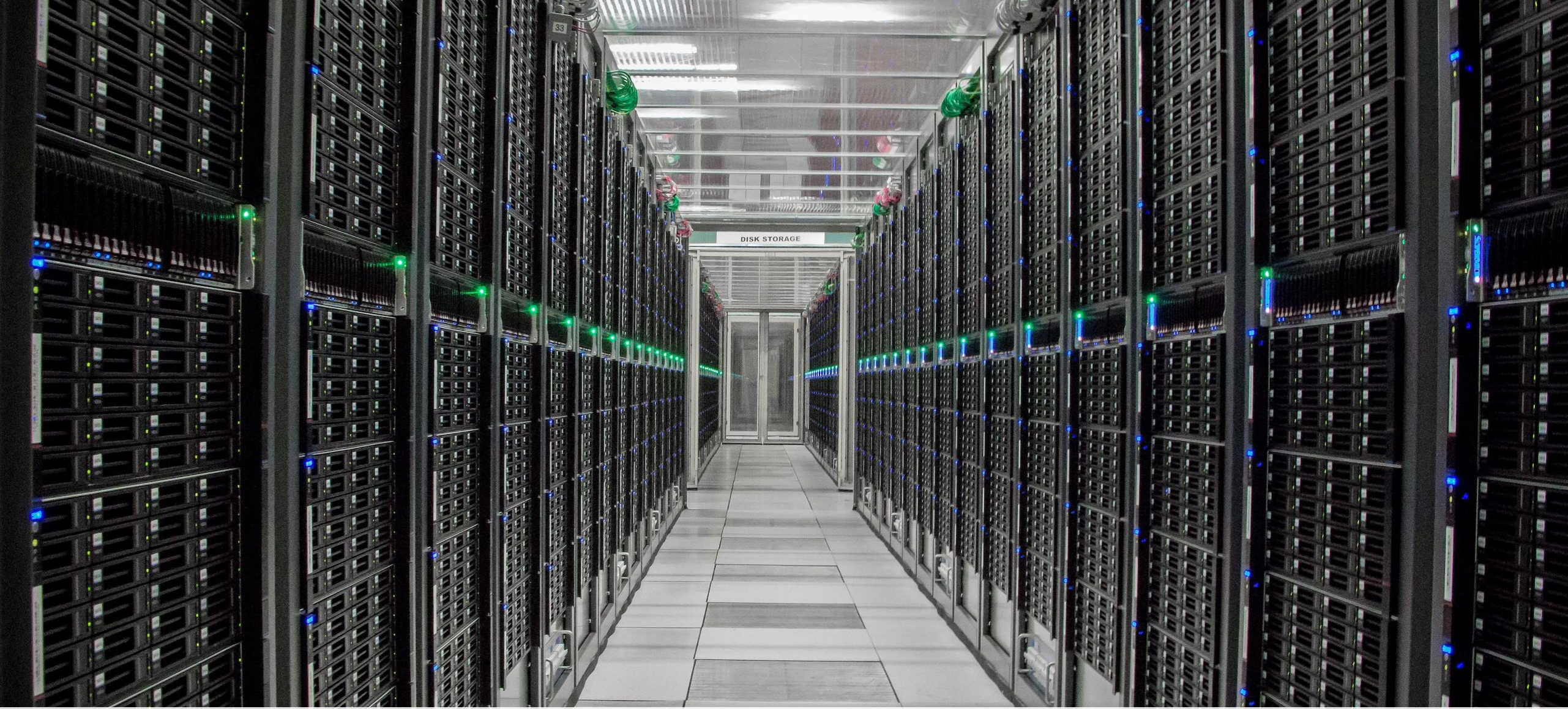
Guided tours

Science films

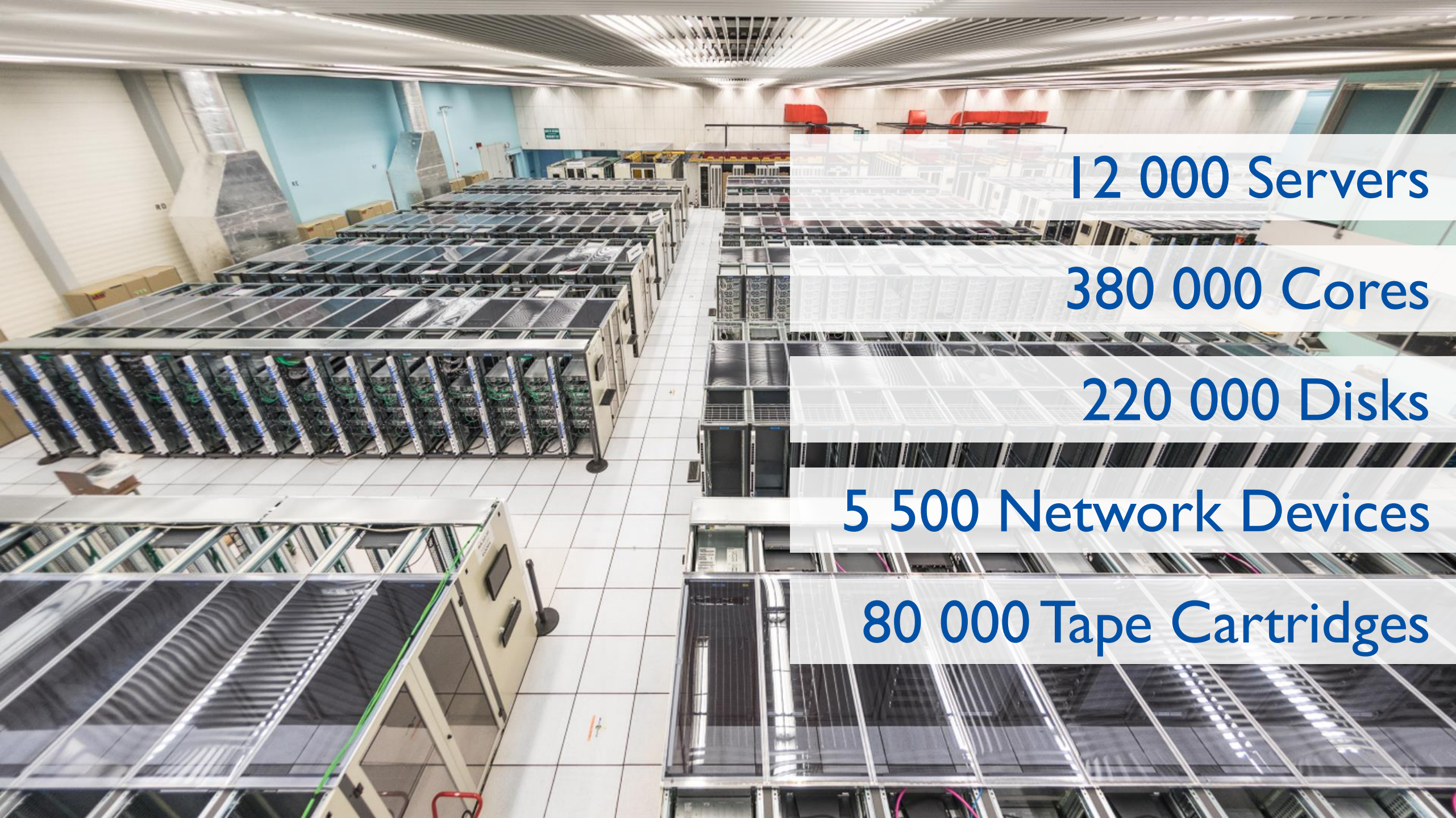
Public events

Virtual tours





Computing

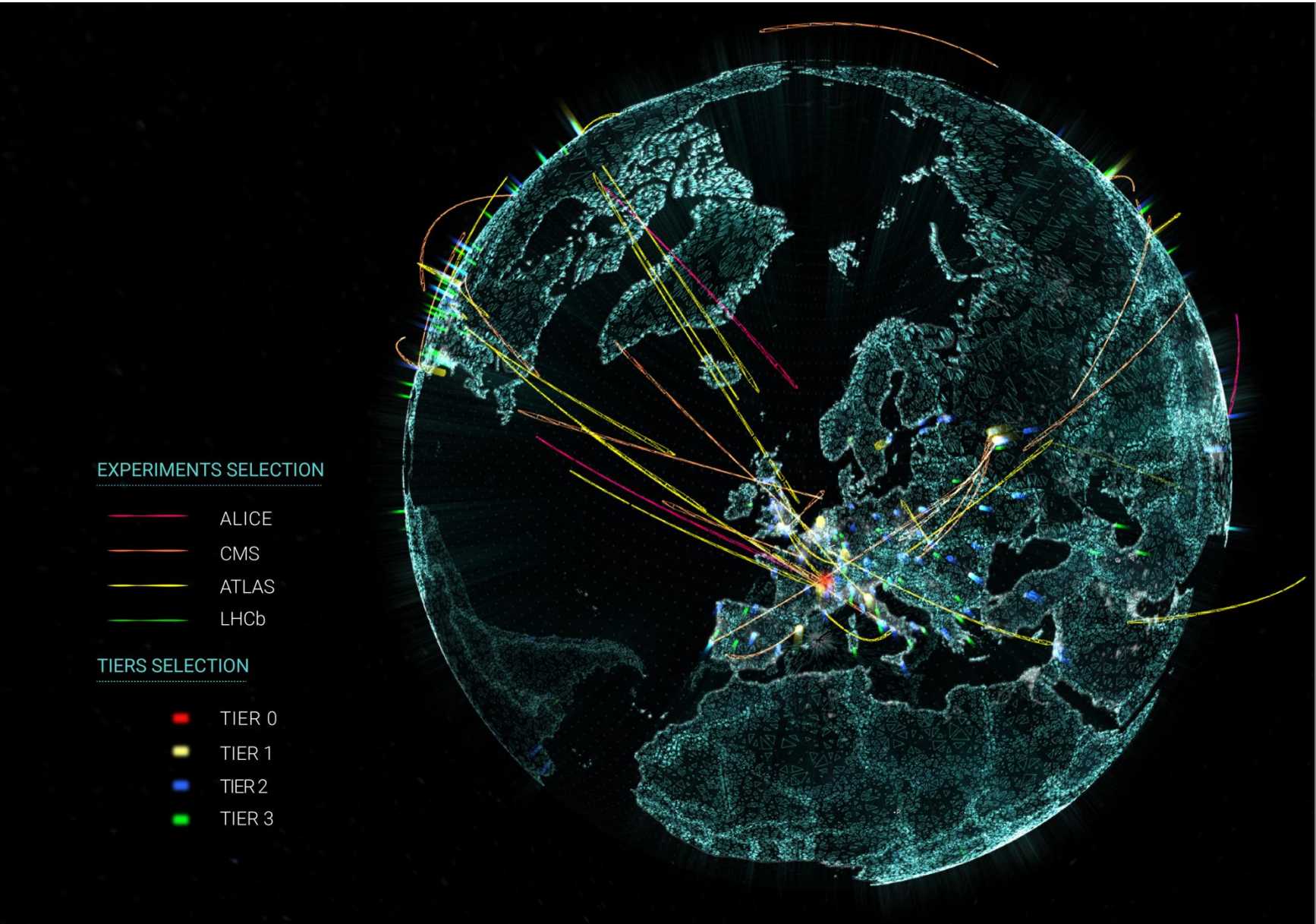

12 000 Servers
380 000 Cores
220 000 Disks
5 500 Network Devices
80 000 Tape Cartridges

> 1.3 EB stored on tape

Capacity of > 2 EB

Massive amounts of data

The Worldwide LHC Computing Grid (WLCG)



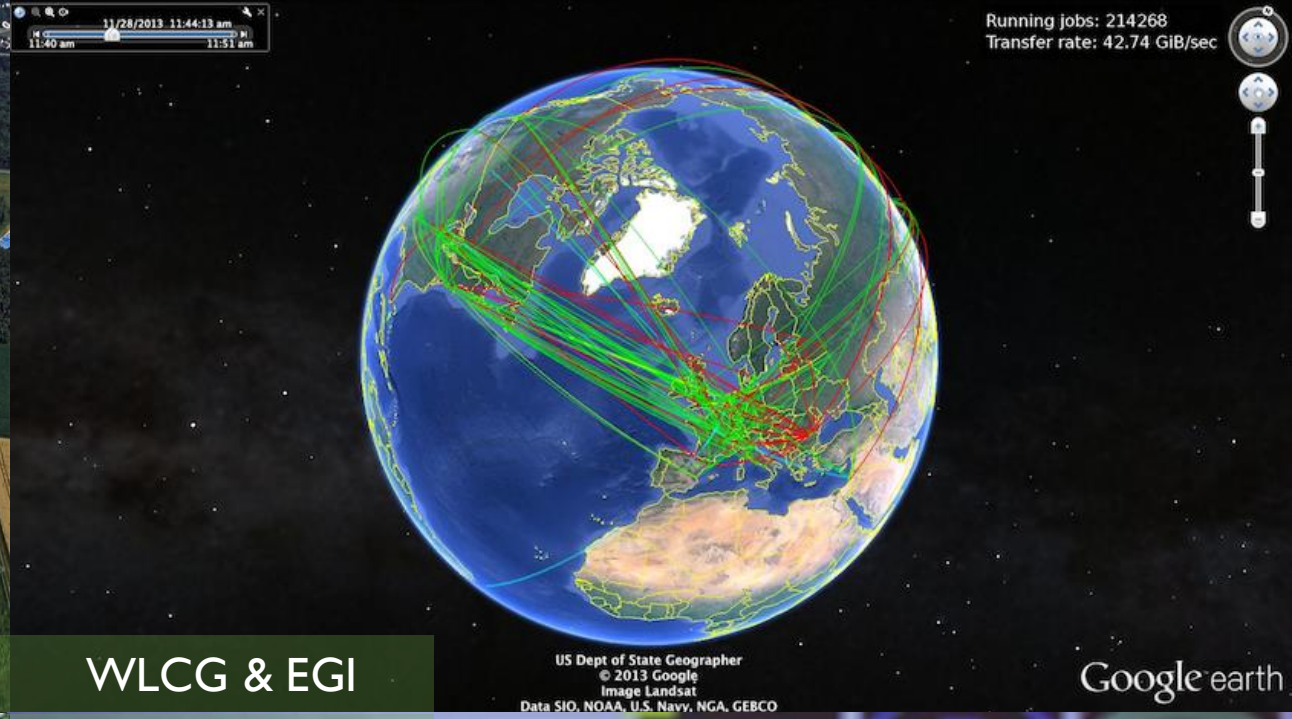
WLCG

- Stores, distributes, processes and analyses LHC experiments' data.
- 1.4 million processing cores in 170 data centres and more than 40 countries.
- 1.3 Exabytes of CERN data stored and analysed world-wide.

CERN Computer Security Team mandate

Protect the operations and reputation of CERN against computer security threats

Campus



WLCG & EGI

Data centre

Control systems

Like any other company, organisation or university, CERN is under permanent attack.

RISK MATRIX

Operational	Financial	Legal	Reputational
Sabotage	Violation of copyrights		
	License infringements		
	Financial fraud		
	Data theft		Attacking third parties
Misuse of compute power			Defacement
Impersonation			
Espionage			Water-Holing

08:49
◄ Mail

CERN RESEARCH ROOTED BY SIEGED
by SiegedSec - Thursday October 27, 2022 at 12:55 AM

SiegedSec

BreachForums User

MEMBER

Posts:
Threads:
Joined: Sep 2(
Reputation:

Yesterday, 12:55 AM (This post was last modified: Yesterday, 07:
AM by pompompurin.)

CERN RESEARCH ROOTED BY SIEGED

Hello hackers, needs, journalist, feds and eve
in between. This week at SiegedSec we breac
the CERN research centre and gained root ac
to a number of servers, exfiltrating around 20
of sexy breach data.

[redacted]

Report:
Hello, siegedsec welcomes our lovers and the ones who envy,
Today we have breached CERN with root access via an OOP lib by CERN web. so we bring to you a stunning 200 GB leak.

We don't have anything against you guys so we hadn't done much,youve just happened to be our next victim. (Joking cern rhymes with stern and Howard's stern sucks)

Until next time,
Ps fuck the feds

👍 8 ❤️ 3 🎉 1

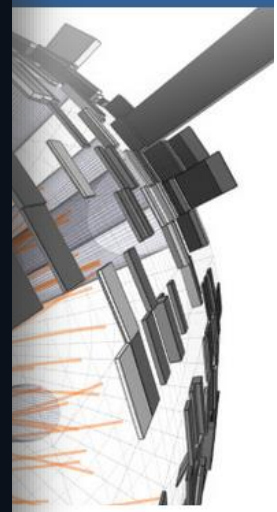
460 22:47

[redacted]

siegedsec__2_.txt
5.7 KB

431 22:48

Developers



Data Theft (…or not 🙂)

Европейская организация по ядерным исследованиям под кураторством США, вторая по размерам в мире лаборатория физики высоких энергий. Также иногда переводится как Европейский Центр ядерных исследований. Аббревиатура CERN произошла от Conseil Européen pour la Recherche Nucléaire.

❌ Официальный сайт ЦЕРН
☐ https://home.cern/
https://check-host.net/check-report/cfa62c4ka78
❌ WEB Директория ЦЕРН
☐ https://directory.web.cern.ch/
❌ Авторизация для сотрудников ЦЕРН
☐ https://auth.cern.ch/
☐ https://login.cern.ch/

14.7K edited 06:28

KillMilk
Все отладили, всё работает. ЦЕРН без обид, ты был тестом🤦‍♂️

10.3K 18:50

KillMilk
Я так долго ждал этого дня ребята🥹

10.4K 18:51

	min	max	avg
GF1P Active Sessions	73998	85747	79380
GF2P Active Sessions	327460	6414111	3033365
GF1P Data Plane load (right-y)	0.700%	1.95%	1.07%
GF2P Data Plane load (right-y)	3.25%	44.2%	23.0%

Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported


By Greg Wallace, Sean Lyngaas, Pete Muntean and Michelle Watson, CNN
Updated 11:50 AM EDT, Mon October 10, 2022

DDOS-ing CERN (for tests)

Computer Security Officer: Mandated by DG; generally *not* person responsible; independent in terms of decisions; part of IT management; ties with BC/DR lead, crisis management, Host Relations, legal, ODP, risk management, STEPS ("CIO")

Computer Security Team: 6 staff+students; many in-kind contributions and shared responsibilities with IT service managers (AD, EDR, firewall, IAA, …)

Standard: Audited 2023 against CISv8 (our choice)
82 findings (0 critical, 15 major, 33 moderate, 34 minor): no surprises, all expected; 50% under CSO, 50% under IT department/STEPS
https://www.ciscurity.org/controls/v8

Governance

Policies: Maintaining CERN Computing Rules (OC5). Improving governance and enforcement of "security".
https://cern.ch/ComputingRules

Basic Training: Giving regular awareness/on-boarding sessions. Plus online security courses. Plus "*Bulletin*" articles. Plus "clicking campaigns".
1+ session per month; 300+ articles published in total; 2k+ out of 22k+ people phished
https://security.web.cern.ch/training/en/CERN%20Articles%20On%20Computer%20Security.pdf

Dedicated Training: Providing in-depth training on security practices incl. programming. Plus "*Serious Gaming*" and "*WhiteHat Challenges*".
5 "*Zebra*" table-top exercises, one with real policemen from Geneva & Pays de Gex; ~100 CERN *WhiteHats* trained, plus many more students from external universities
"Thanks for cleaning up" – Bulletin article to come

Awareness, Training & Policies

2FA: Deploying extra protection to SSO/SSH.
9500+ accounts already enrolled. More to come
https://home.cern/news/news/computing/computer-security-log-click-be-secure

"*Gotham*": Notifying "unusual" logins.
~4770 notifications per month
https://home.cern/news/news/computing/computer-security-your-remote-logins

Dumps of Exposed Passwords: Notifying when used outside. Ditto for our community. Forcing reset when used at CERN.
Monitoring ~9k communities; reporting ~11k exposed passwords per day (~4/day for CERN)
https://home.cern/news/news/computing/computer-security-password-revolutions

Account Protection

***EOP – xorlab – MDO* eMail-Filtering:** Quarantining SPAM & malware.
~115k analyzed per day; 10% SPAM; 2% quarantined; >12/d manually checked (MDO: >50% FP)
https://home.cern/news/news/computing/computer-security-fighting-spam-boss-level

***ESET* Anti-Virus/Anti-Malware:** Providing endpoint detection & response software for BYOD and CERN-owned devices.
~600 Bring-your-own-devices (BYOD) and 200+ CERN-managed devices
https://home.cern/news/news/computing/computer-security-winter-season-virus-time-one-free-pill-your-device

***Threatray* Memory Hashing:** Detecting anomalies on CERN-managed devices.
~5500 CERN-managed devices enrolled

Endpoint Protection

Automatic Vulnerability Scanning: Identifying weaknesses of endpoints & servers, unused firewall openings, as well as exposed secrets.
~24k devices scanned per month; ~210 issues per month
https://home.cern/news/news/computing/computer-security-time-spring-clean

Security Consultancy & Reviews: Improving CERN's security posture (via *Cloud/Software License Office, IT consultants, IT Architecture Review Board*).
20-30 in-depth reviews per year

Self-Security Assessment for Cloud Services: Providing metrics, guidelines & controls for better security.
Based on CISv8 standard. Prototype ready. Web-portal in development

PenTests, Reviews & Consulting

***PaloAlto* Firewalling:** Performing deep packet inspection and policy-based IP, domain & URL blocking.
>2x 200Gbps (ingress+egress) IPv4&v6 monitored in-line
https://home.cern/news/news/computing/computer-security-cerns-new-first-line-defence

DNS RPZ & Firewall: Blocking malicious & typo-squatting domains (with SWITCH). Ditto for 50+ CH & F hospitals.
~800 domains blocked by CERN, >100/day by SWITCH. No hospital got ransomwared so far
https://home.cern/news/news/computing/computer-security-when-cernch-not-cern

pDNS Containers: Helping WLCG sites to do alike.

Network Protection

Code / Container Scanning: Deploying *GitLab/GitCI* and *Harbor* security features (SAST/DAST/…).
https://home.cern/news/news/computing/computer-security-avoiding-salmonella-your-code

Software-Bill-of-Materials (SBOM): Pushing for a curation service to avoid (automatic) downloading of malicious libraries, packages, containers & VMs. Document dependency trees and license constraints.
https://home.cern/news/news/computing/computer-security-when-your-restaurant-turns-sour

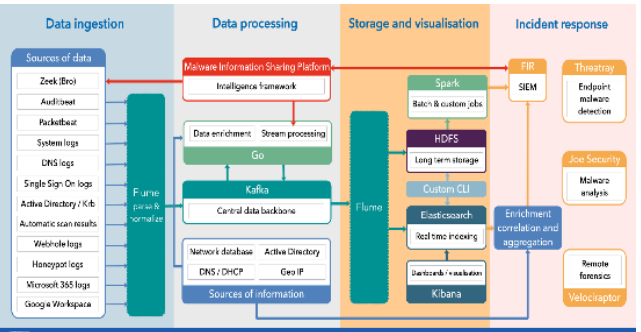
Software Security

ThreatIntel: Obtaining high-quality Indicators of Compromise.

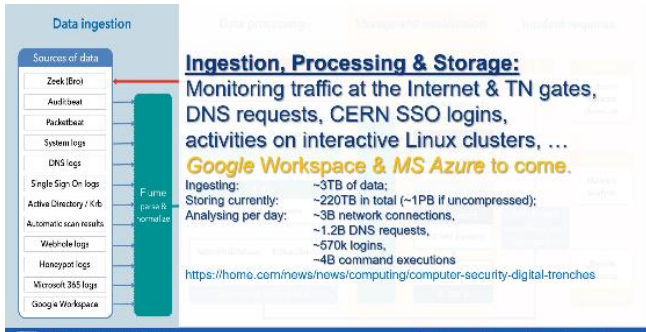
e.g. IPs, domains, file hashes from our peers and *Prodaft*, plus the *IWF* on CSAM (child sexual abuse material).
~15M IoCs shared with 1000+ peer organizations; 100k+ IoCs currently actively monitored
https://home.cern/news/news/computing/computer-security-protective-intelligence

Collaboration: Acting as a trusted, neutral broker, aiming at fostering cooperation and trust in our community: *WLCG/EGI/OSG*, *SWITCH* (CH), *REN-ISAC* (5-eyes); +Governments: *MELANI* (CH), *ANSSI* (F), *CH-CERTs*; +Law enforcement: *Interpol*, *Europol*, *FBI*, *CISA*, local police; +Int'l org's: *GISSIG/UNISSIG*; and with security vendors.
P.ex. 120+ universities world-wide notified this year of ransomware preparations in their IT infrastructure

Threat Intelligence



Orchestration (the "SOC")



Ingestion, Processing & Storage: Monitoring traffic at the Internet & TN gates, DNS requests, CERN SSO logins, activities on interactive Linux clusters, … *Google* Workspace & *MS Azure* to come.

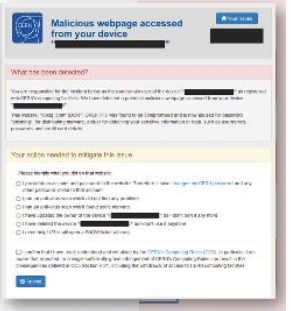
Ingesting:	~3TB of data;
Storing currently:	~220TB in total (~1PB if uncompressed);
Analysing per day:	~3B network connections, ~1.2B DNS requests, ~670k logins, ~4B command executions

https://home.cern/news/news/computing/computer-security-digital-trenches

Intrusion Detection

"*Auto-Notify*": Notifying resource owners (devices, accounts, websites, …) of problems with their resources.
~300 reports per month (plus ~4700 "*Gotham*")
https://home.cern/news/news/computing/computer-security-our-findings-your-problem

Forensics: Providing capabilities and tools like *Prodaft*, *Threatray*, *Velociraptor*.
https://home.cern/news/news/computing/computer-security-catch-me-if-you-can

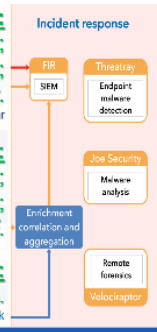


Incident Response

CERN Computer Security Rota: Providing 2nd line Guys-on-Duty ("GoD"); 3rd line Security Escalation Cordinator ("SEC"); 4th line Computer Security Officer.
~150 SNOW and ~36 FIR tickets handled per month; 5-10 "heavy" incidents per year

Grid Security Rota: Leading the WLCG Security Office; Leading *EGI* Incident Response Taskforce; Leading *EOSCfuture* Incident Response TF.

"*SAFER*" Community Security: Providing world-wide incident response.
https://home.cern/news/news/computing/computer-security-safer-teamwork



CERN & HEP CSIRT

A Comprehensive Portfolio

The CERN Security Operations Center

SYSTEM DESIGN OF THE CERN SOC

- Unified platform for:
  - Data ingress
  - Storage
  - Analytics
- Multiple data access / view patterns:
  - Web based dynamic dashboards for querying and reporting
  - Command line interface that can be easily scripted
- Extensible, pluggable, modular architecture
- Unified data access control policies

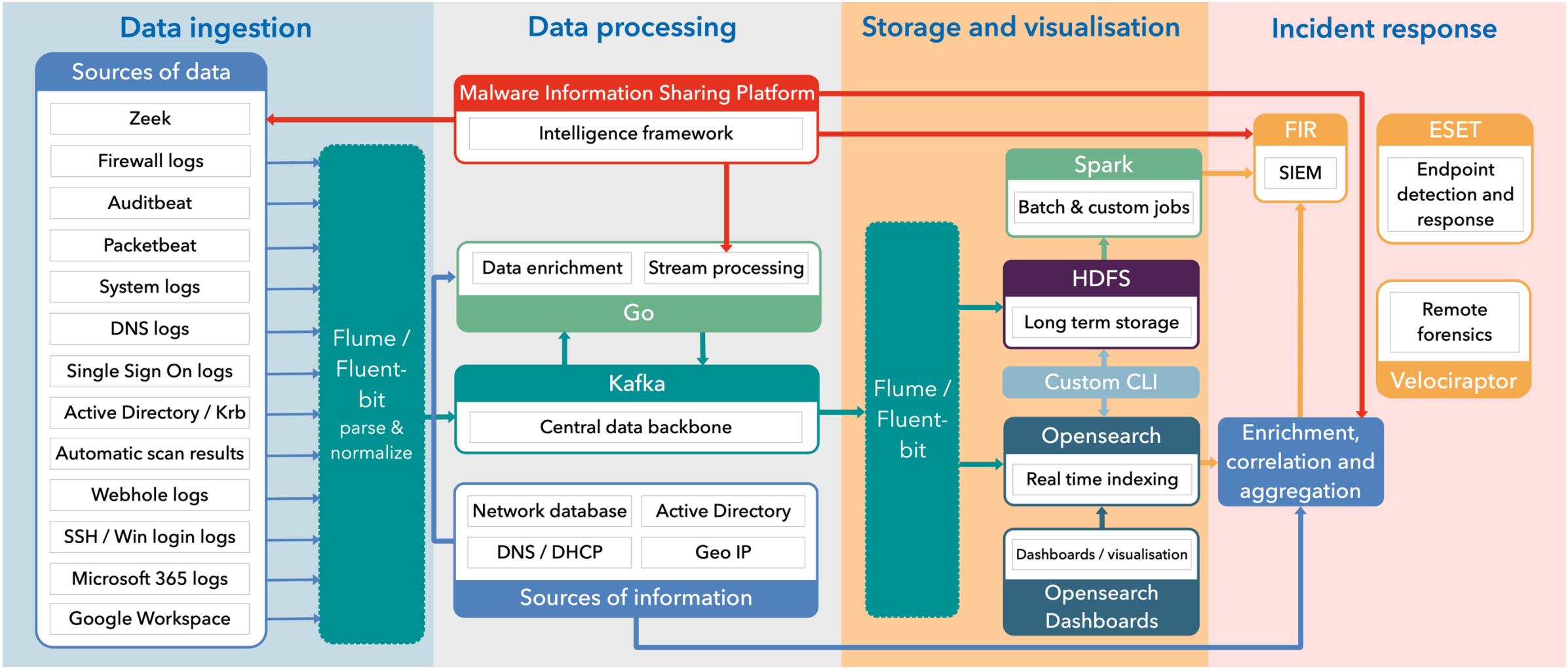
TECHNOLOGY GOALS

- Scale out, not scale up
- Integrated with the rest of the CERN IT ecosystem
- Use of commodity hardware (as much as possible)
- Use of cheap, massively-scalable storage (standard disk arrays)
- Deployment inside OpenStack (whenever possible)
- Configuration management done via Puppet

PRIVACY/SECURITY CONCERNS

- Every component follows strong security requirements:
  - Data transfers encrypted
    - Using TLS
  - Authentication used for all data accesses
    - Mostly Kerberos, password for Elasticsearch
  - Authorization & ACLs
    - Data only accessible to the Computer Security Team & Service Managers
  - Spark master-executors communications are protected

SYSTEM ARCHITECTURE



TECHNOLOGY STACK USED

- **Intrusion Detection:** Zeek
- **Telemetry Capture Layer:** Apache Flume & Fluentbit
- **Data Bus (Transport):** Apache Kafka
- **Analytics:** Apache Spark & Go
- **Long-Term Data Store:** Hadoop HDFS
- **Real-Time Index & Search:** Opensearch
- **Visualisation:** Opensearch Dashboards & CLI
- **Web frontends:** OpenShift

ZEEK USAGE AT CERN

- Cornerstone of the CERN SOC
- Cluster of 16 nodes (12 production, 4 QA)
- ~2.5 billion daily connections
- ~1.2 TB of daily Zeek logs
- Building RHEL RPMs and sharing them
- > 3 million Indicators of Compromise used for active detection via the Zeek intel framework
- Tens of thousands of daily raw Zeek alerts being distilled to only a few dozen alerts that a SOC analyst needs to handle (via automatic removal of false positives, aggregation and correlation)


CERN