Where security research and standardization meet

Claire Vishik

BACKGROUND

Premise

Security and adjacent areas have benefited from standardization to a very large degree. But the evolving technology environment, different distribution of expertise and competing endeavors call for new approaches to standardization in security that can focus and speed up the standardization process without jeopardizing the key ingredients and achievements of open standardization.

A broad field: cybersecurity

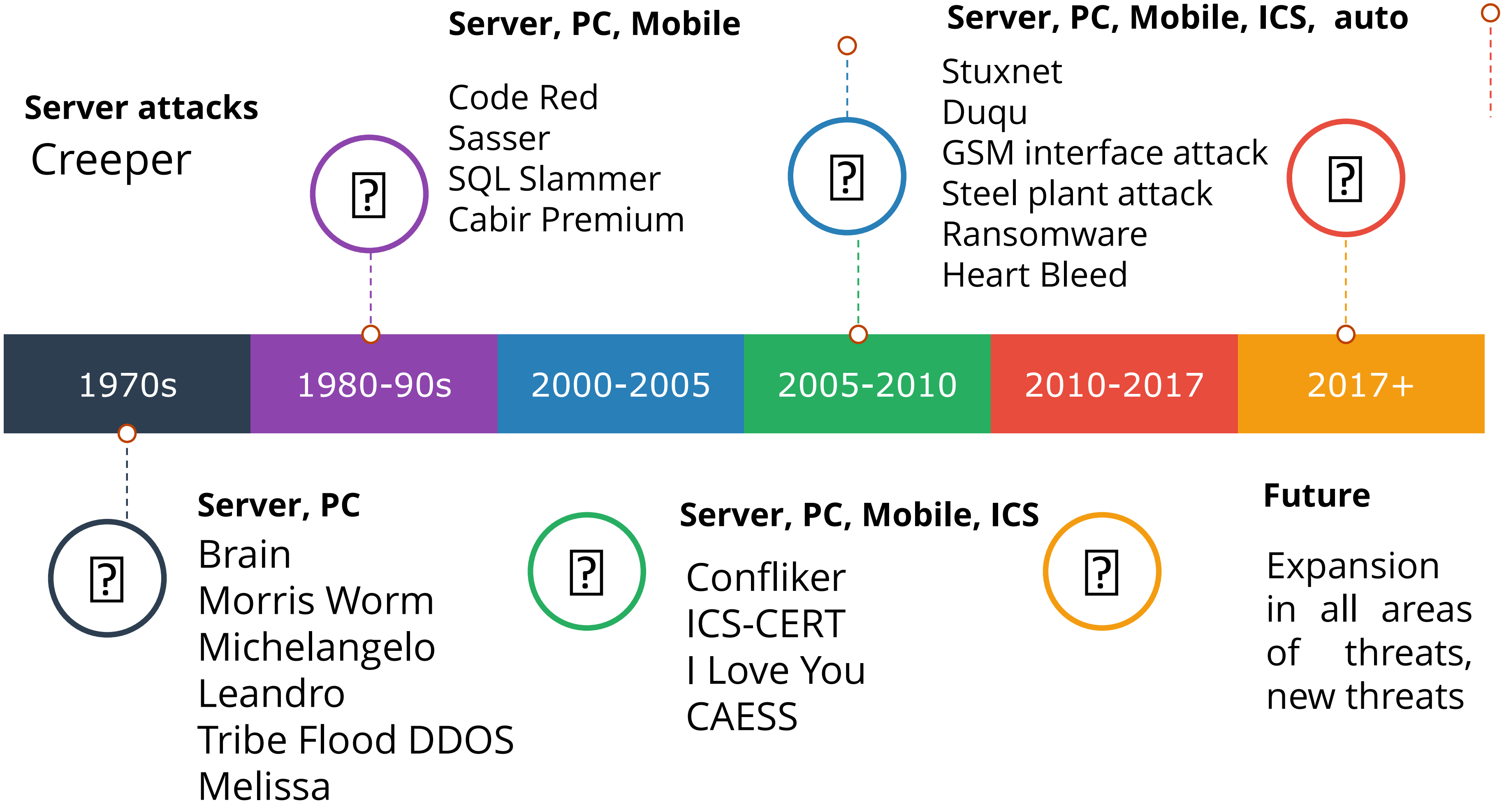
Complex space requiring collaboration of a multi-disciplinary global community for success – and standards

Narrow Definition	Broad Definition
Activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected...	Strategy, policy, and standards for security of and operations in cyberspace. Includes international engagement, incident response policies, law enforcement, information assurance, diplomacy, and other areas fundamental for security and stability of the global information infrastructure…

http://niccs.us-cert.gov/glossary#letter_c

National Initiative for Cybersecurity Careers & Studies

Reach of cyberattacks is expanding



1970s

1980-90s

2000-2005

2005-2010

2010-2017

2017+

Server attacks

Creeper

Server, PC

Brain
Morris Worm
Michelangelo
Leandro
Tribe Flood DDOS
Melissa

Server, PC, Mobile

Code Red
Sasser
SQL Slammer
Cabir Premium

Server, PC, Mobile, ICS

Confliker
ICS-CERT
I Love You
CAESS

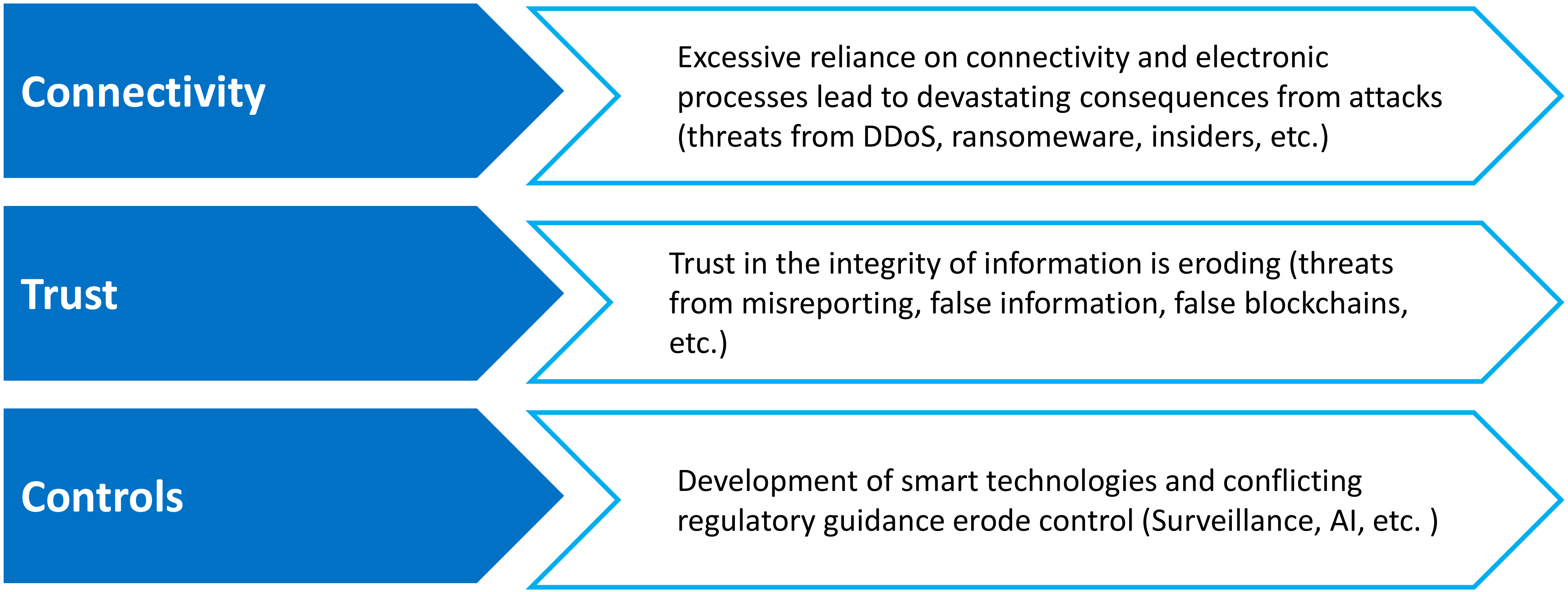
Server, PC, Mobile, ICS, auto

Stuxnet
Duqu
GSM interface attack
Steel plant attack
Ransomware
Heart Bleed

Future

Expansion in all areas of threats, new threats

Key threat areas (from the 2017 ISF Threat Horizon)



Connectivity

Excessive reliance on connectivity and electronic processes lead to devastating consequences from attacks (threats from DDoS, ransomeware, insiders, etc.)

Trust

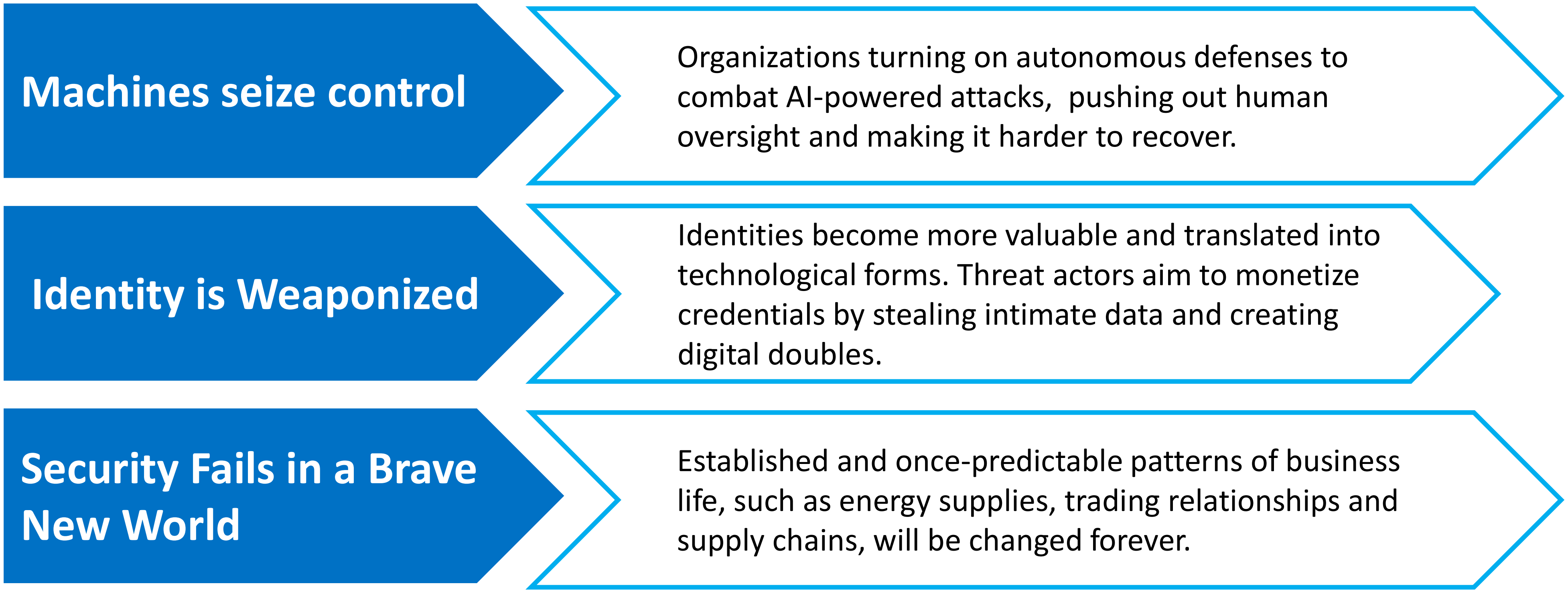
Trust in the integrity of information is eroding (threats from misreporting, false information, false blockchains, etc.)

Controls

Development of smart technologies and conflicting regulatory guidance erode control (Surveillance, AI, etc.)

Focus on trust and integrity

Key threat 2023: nothing much has changed



Machines seize control

Organizations turning on autonomous defenses to combat AI-powered attacks, pushing out human oversight and making it harder to recover.

Identity is Weaponized

Identities become more valuable and translated into technological forms. Threat actors aim to monetize credentials by stealing intimate data and creating digital doubles.

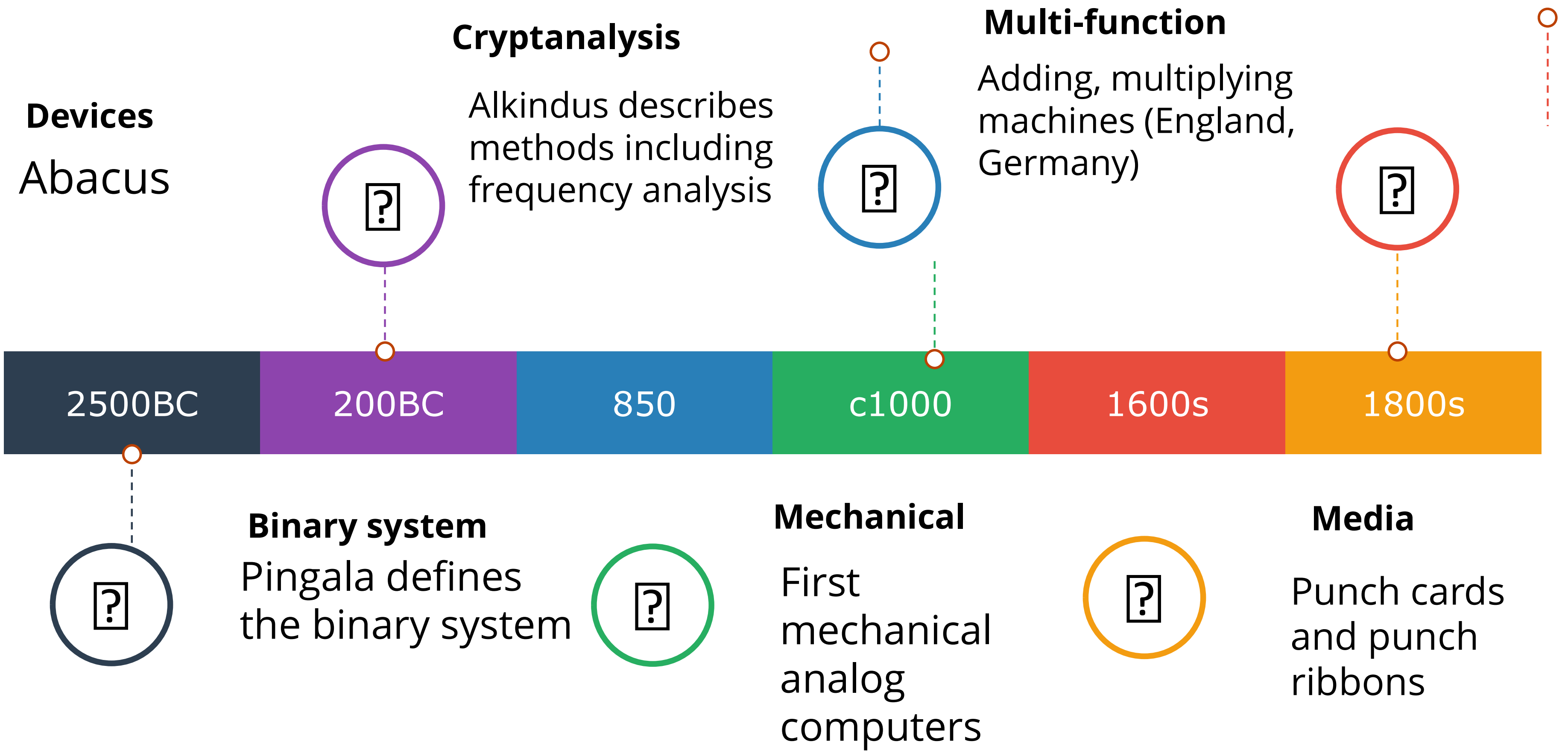
Security Fails in a Brave New World

Established and once-predictable patterns of business life, such as energy supplies, trading relationships and supply chains, will be changed forever.

Adapted from https://www.newswire.com/news/threat-horizon-2023-report-by-isf-claims-artificial-intelligence-will-21349871

ACCELERATION OF THE INNOVATION CYCLE

Earliest computing



Devices

Abacus

Binary system

Pingala defines the binary system

Cryptanalysis

Alkindus describes methods including frequency analysis

Mechanical

First mechanical analog computers

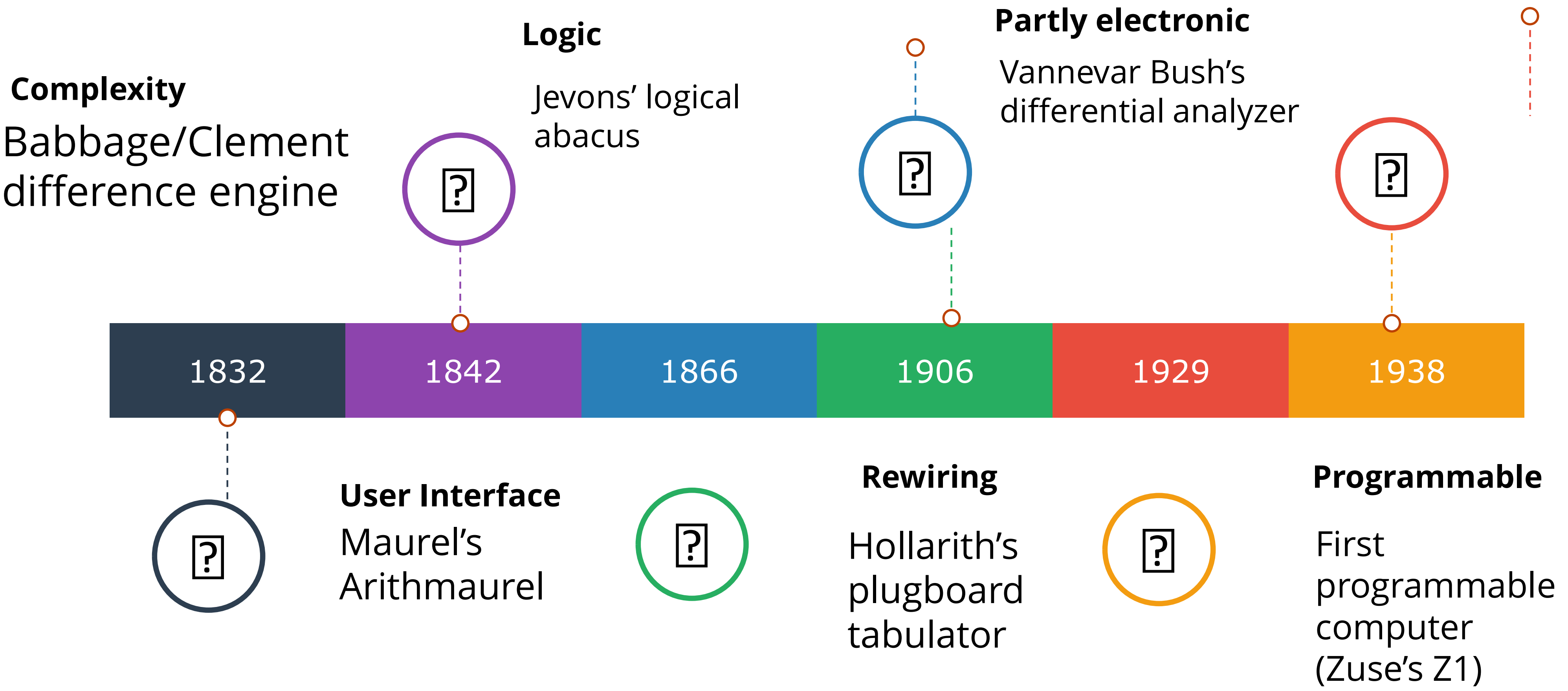
Multi-function

Adding, multiplying machines (England, Germany)

Media

Punch cards and punch ribbons

Early computing



Complexity

Babbage/Clement difference engine

Logic

Jevons' logical abacus

Partly electronic

Vannevar Bush's differential analyzer

User Interface

Maurel's Arithmaurel

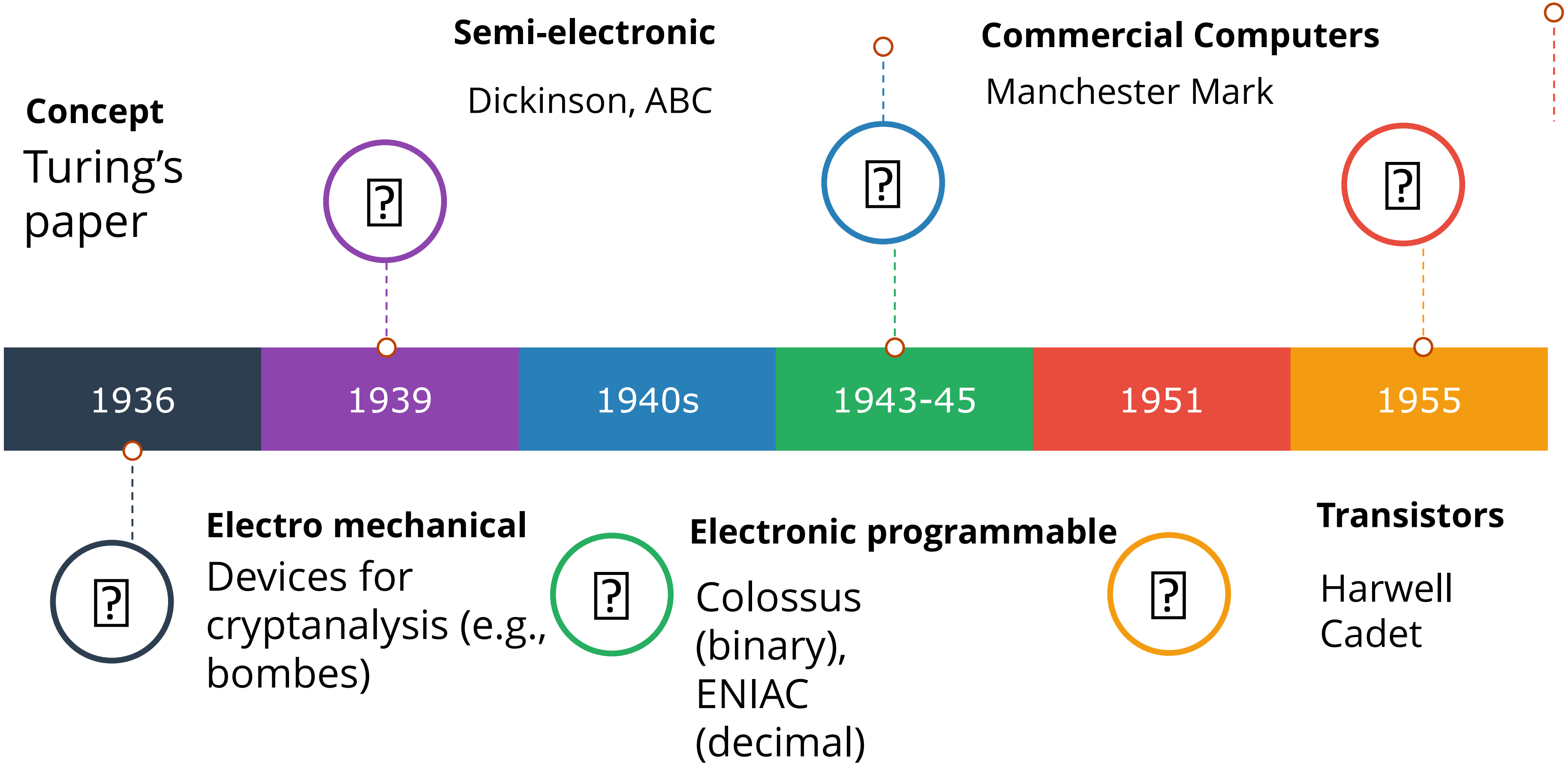
Rewiring

Hollarith's plugboard tabulator

Programmable

First programmable computer (Zuse's Z1)

Digital Computing



1936

1939

1940s

1943-45

1951

1955

Concept

Turing's paper

Electro mechanical

Devices for cryptanalysis (e.g., bombes)

Semi-electronic

Dickinson, ABC

Electronic programmable

Colossus (binary), ENIAC (decimal)

Commercial Computers

Manchester Mark

Transistors

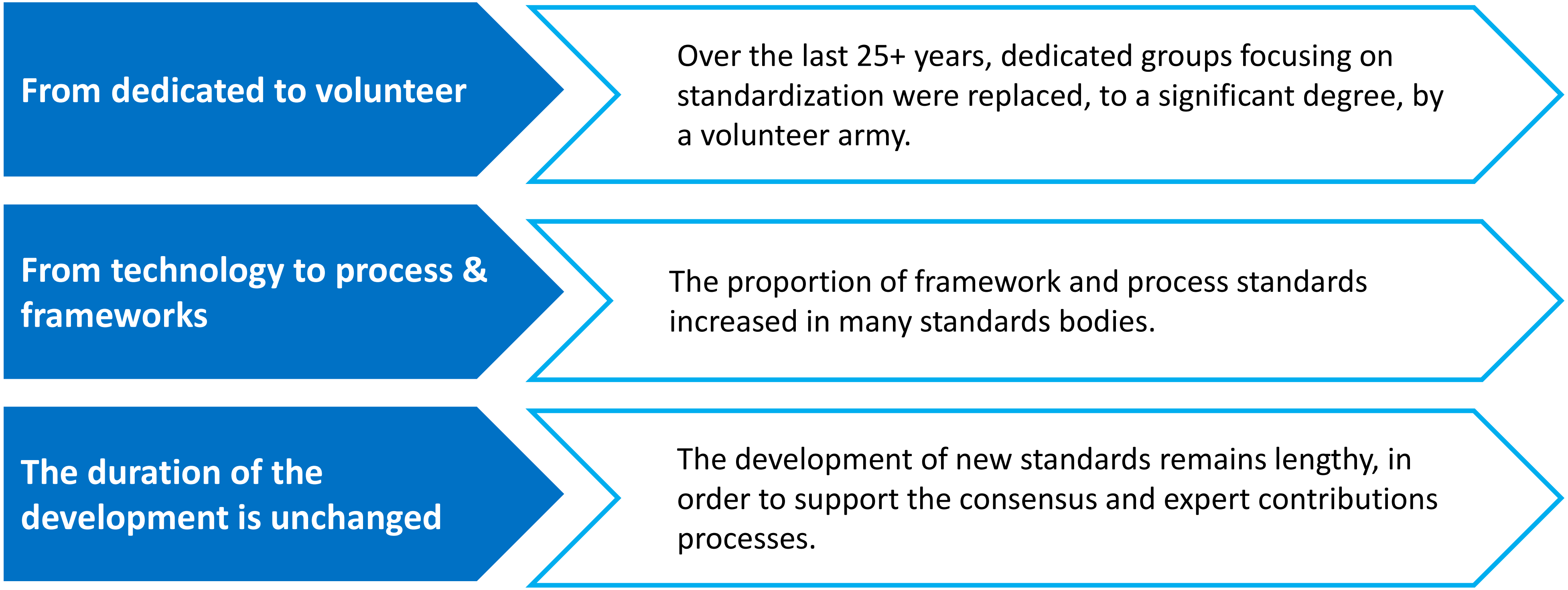
Harwell Cadet

Innovation cycle

1. Simple aids for practical tasks
2. Theoretical extensions
3. Specialization
4. Transfer into an adjacent field
5. Commercialization
6. Generalization (where standardization typically takes place)
7. Usability
8. Complexity

CHANGES IN SECURITY STANDARDIZATION ENVIRONMENT

New realities of security standardization



From dedicated to volunteer

Over the last 25+ years, dedicated groups focusing on standardization were replaced, to a significant degree, by a volunteer army.

From technology to process & frameworks

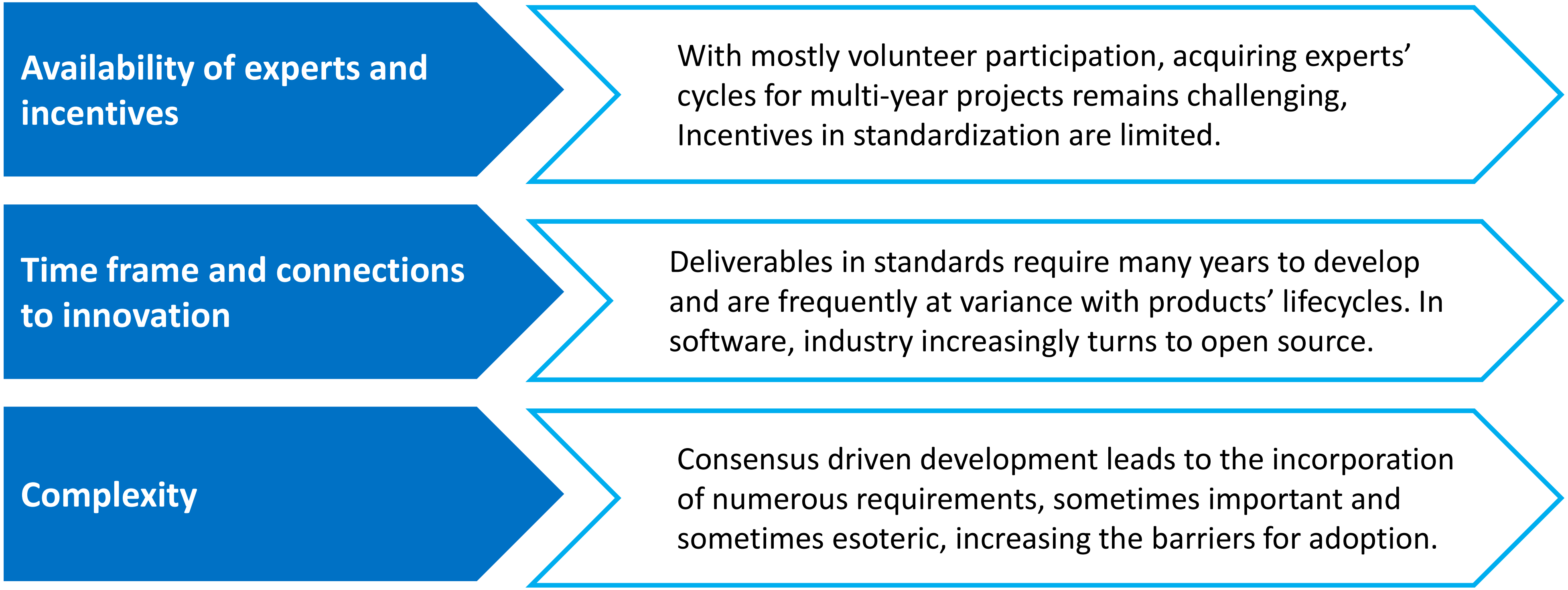
The proportion of framework and process standards increased in many standards bodies.

The duration of the development is unchanged

The development of new standards remains lengthy, in order to support the consensus and expert contributions processes.

In some areas, the length of the development of standards (especially in security) is in opposition to the shortening of the innovation cycles.

Difficulties for industry



Availability of experts and incentives

With mostly volunteer participation, acquiring experts' cycles for multi-year projects remains challenging, Incentives in standardization are limited.

Time frame and connections to innovation

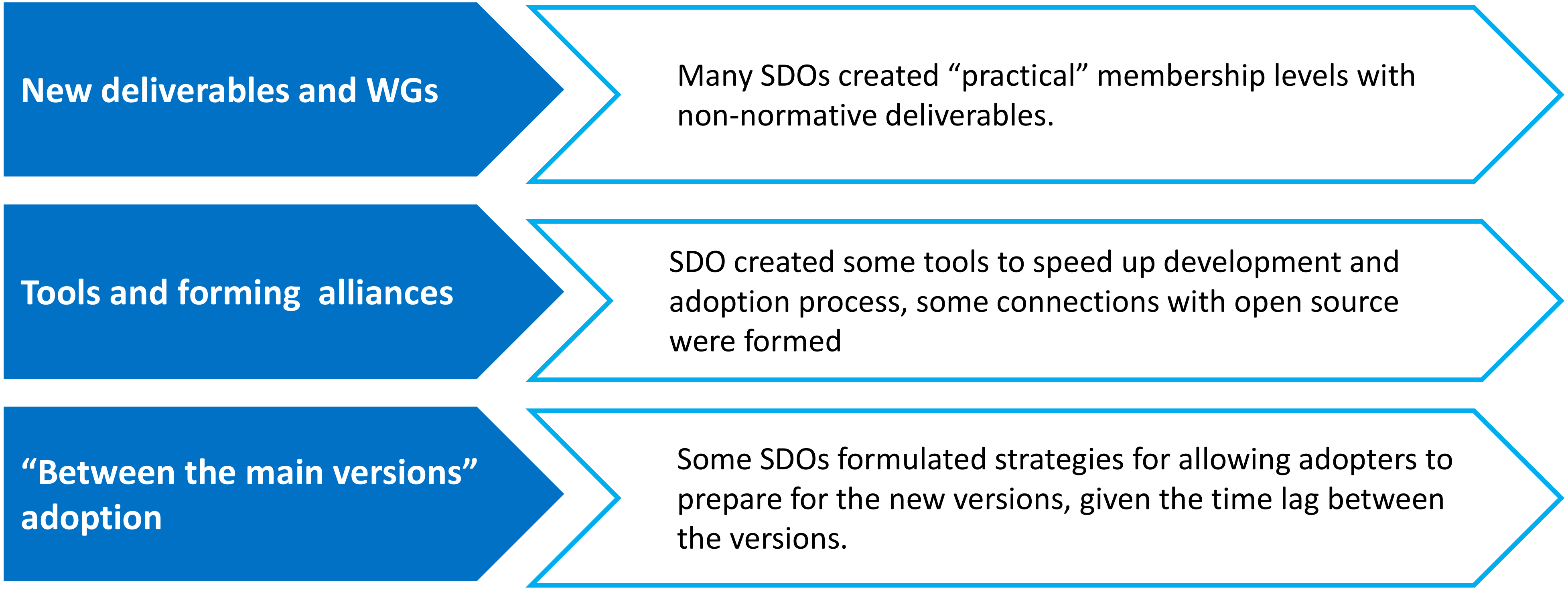
Deliverables in standards require many years to develop and are frequently at variance with products' lifecycles. In software, industry increasingly turns to open source.

Complexity

Consensus driven development leads to the incorporation of numerous requirements, sometimes important and sometimes esoteric, increasing the barriers for adoption.

The dichotomy between the product development and standard development is not new. But the speed of innovation led to new dilemmas.

New approaches in SDOs



New deliverables and WGs

Many SDOs created “practical” membership levels with non-normative deliverables.

Tools and forming alliances

SDO created some tools to speed up development and adoption process, some connections with open source were formed

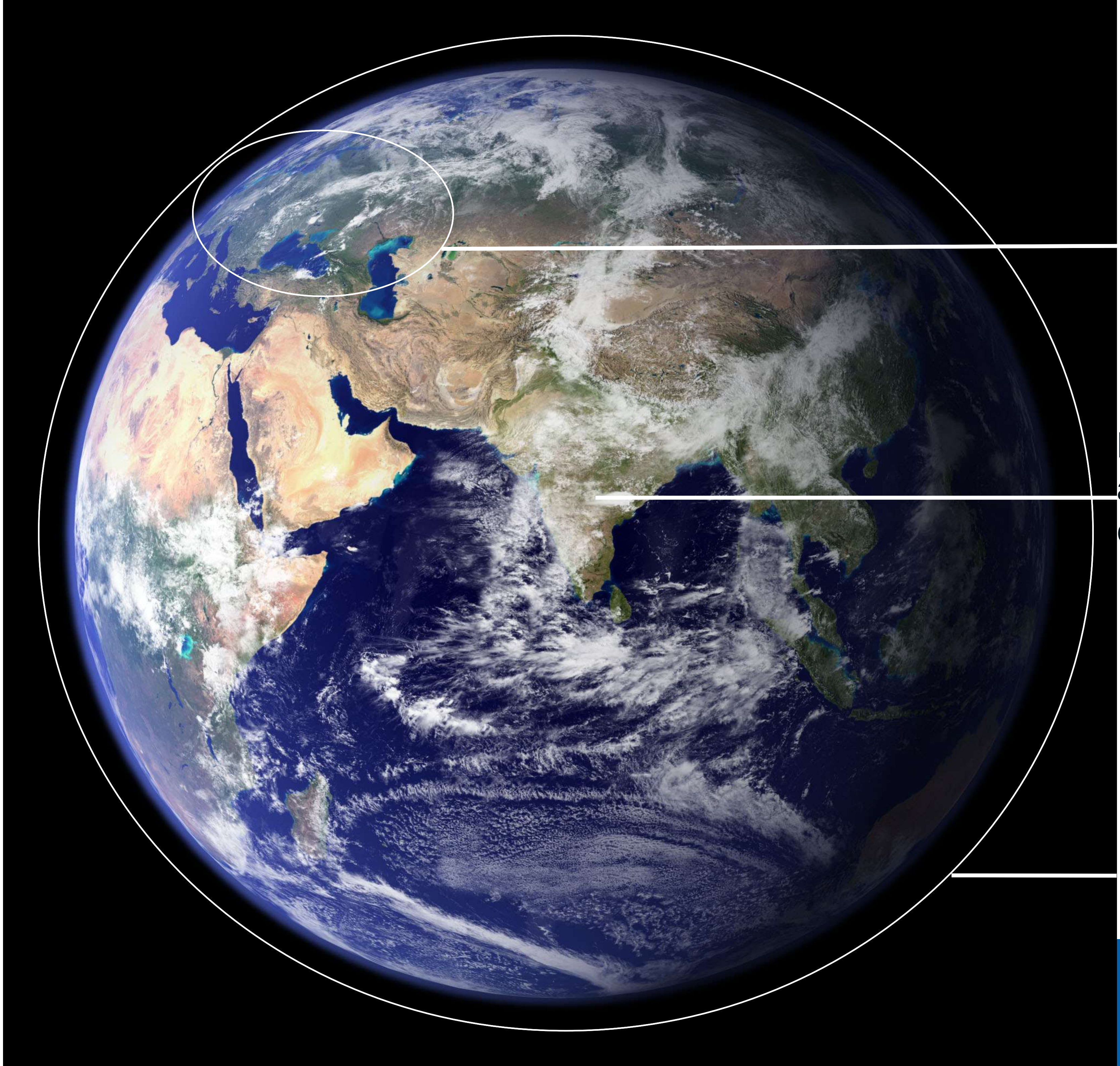
“Between the main versions” adoption

Some SDOs formulated strategies for allowing adopters to prepare for the new versions, given the time lag between the versions.

SDOs are supporting new strategies to adapt to new realities in standardization.

Global Standards

Changing geopolitical situation and regulatory requirements lead to the increasing number of adaptations of international standards that are sometimes incompatible among themselves. This is increasingly frequent in security.



Regional cooperation is more complex

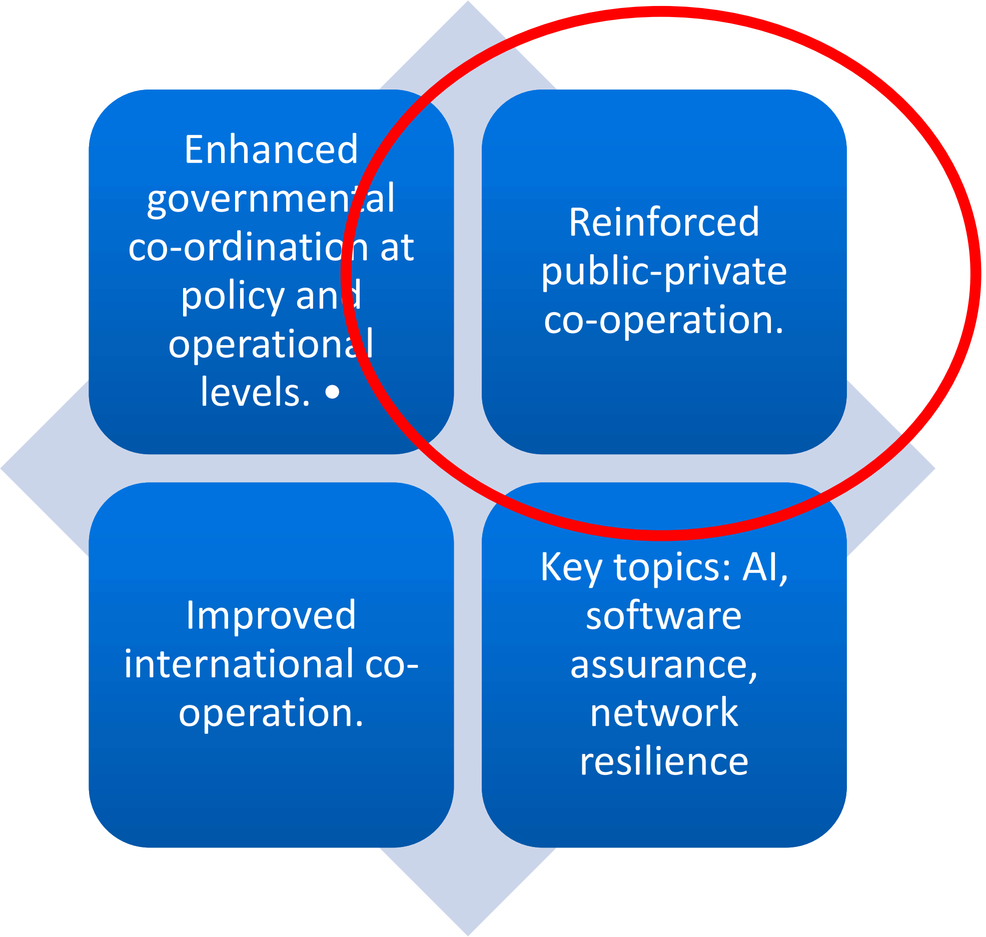
Local initiatives are increasingly diverse

Global mechanisms work most of the time

WHAT IS WORKING AND POTENTIAL NEXT STEPS

Commonality & differences in security strategies and R&D focus areas

Shared concepts



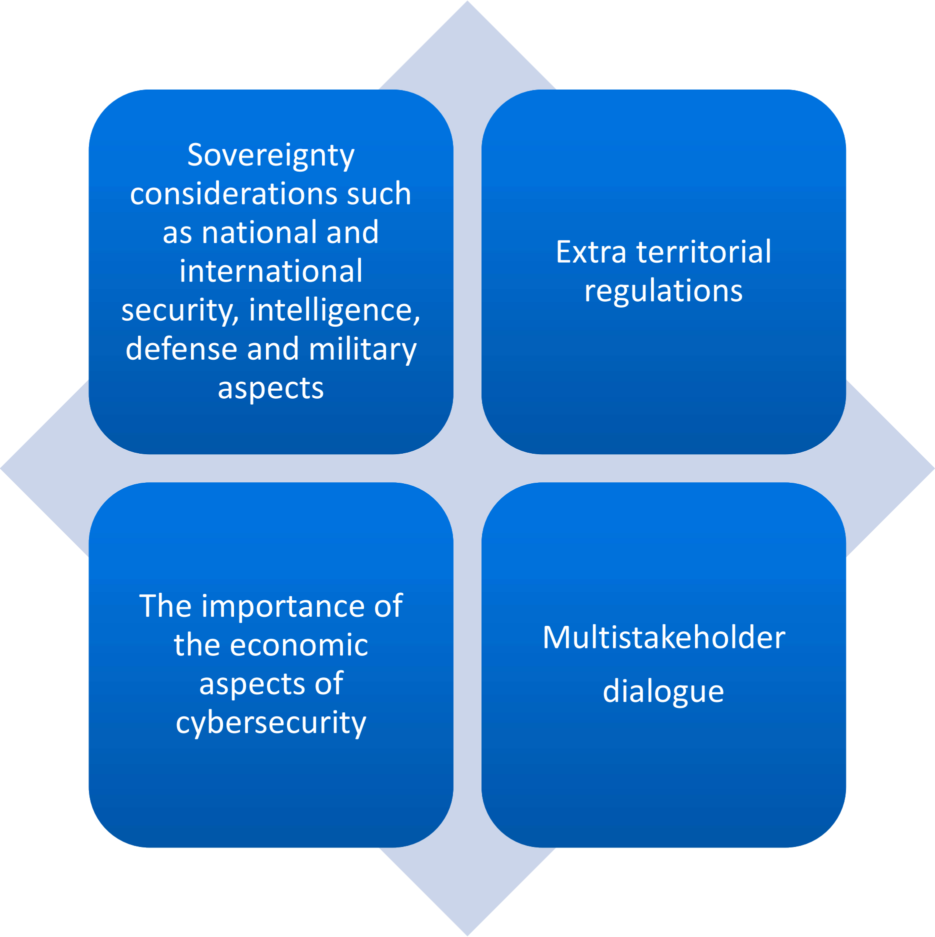
Enhanced governmental co-ordination at policy and operational levels. •

Reinforced public-private co-operation.

Improved international co-operation.

Key topics: AI, software assurance, network resilience

Emerging trends



Sovereignty considerations such as national and international security, intelligence, defense and military aspects

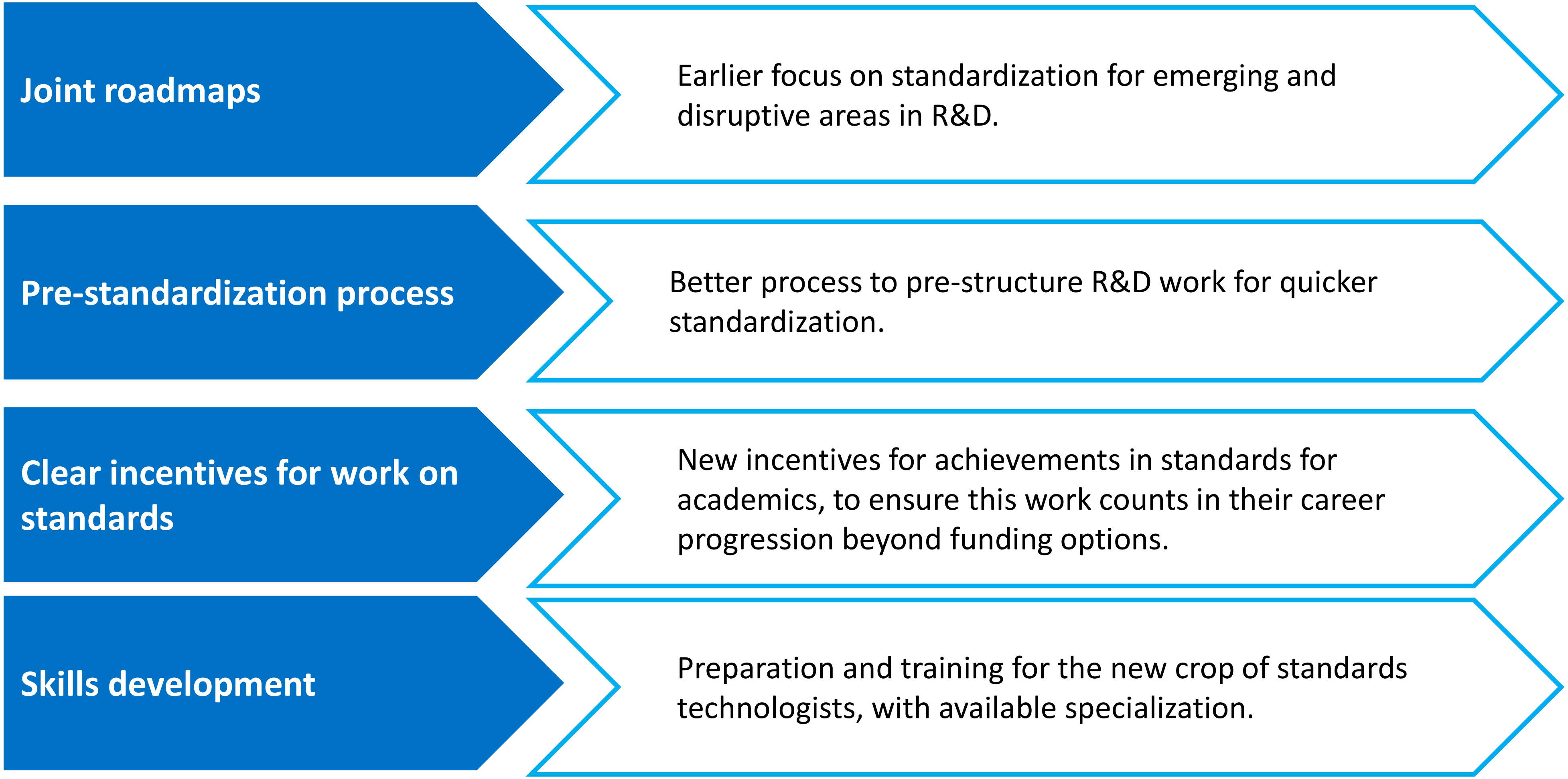
Extra territorial regulations

The importance of the economic aspects of cybersecurity

Multistakeholder dialogue

Information is based on the analysis of cybersecurity and R&D strategies

R&D and Standards Cooperation



Joint roadmaps

Earlier focus on standardization for emerging and disruptive areas in R&D.

Pre-standardization process

Better process to pre-structure R&D work for quicker standardization.

Clear incentives for work on standards

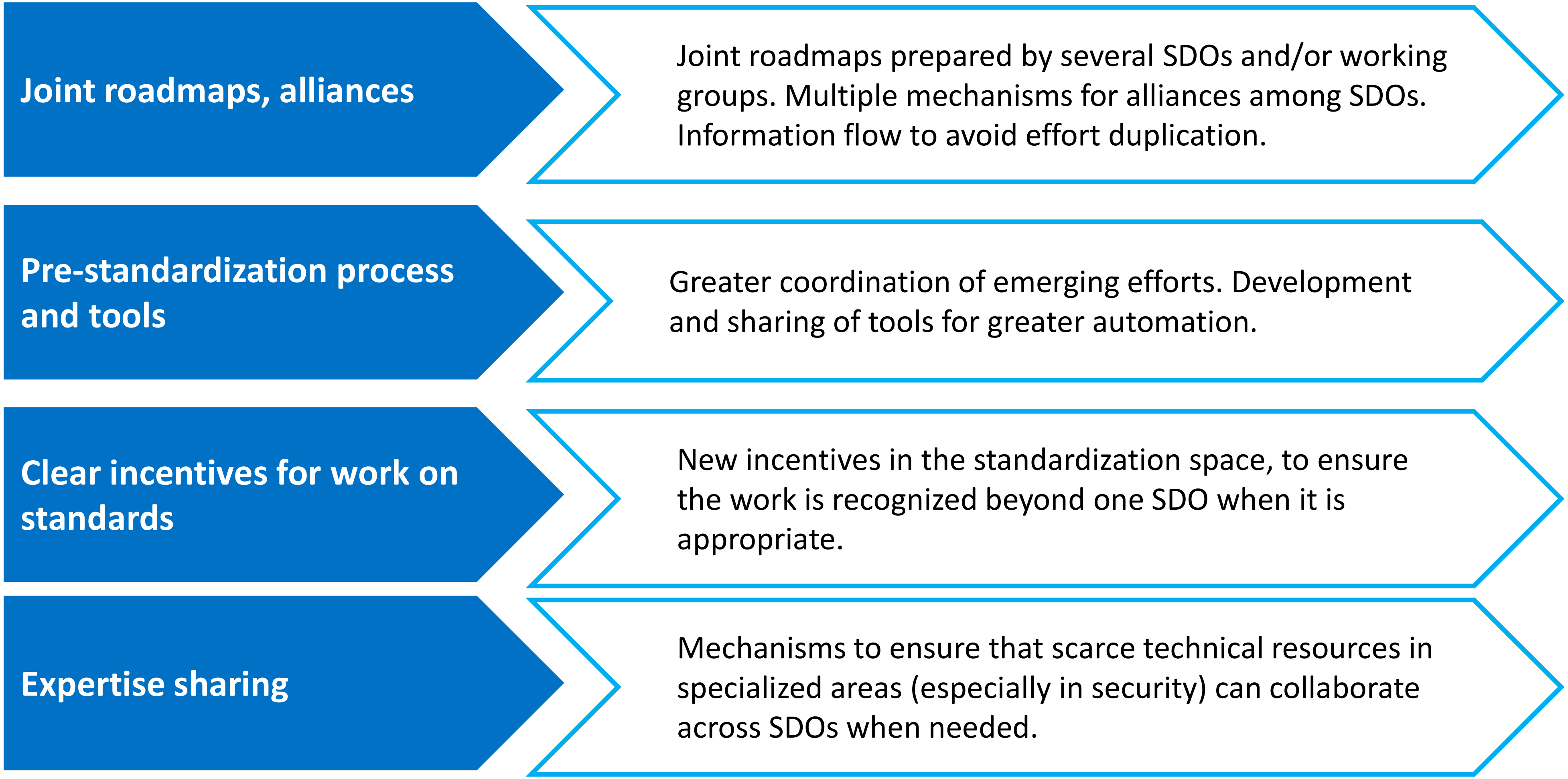
New incentives for achievements in standards for academics, to ensure this work counts in their career progression beyond funding options.

Skills development

Preparation and training for the new crop of standards technologists, with available specialization.

Academia, industrial research, and standardization already benefit from collaboration. But more opportunities exist.

Greater collaboration within the SDO space



Joint roadmaps, alliances

Joint roadmaps prepared by several SDOs and/or working groups. Multiple mechanisms for alliances among SDOs. Information flow to avoid effort duplication.

Pre-standardization process and tools

Greater coordination of emerging efforts. Development and sharing of tools for greater automation.

Clear incentives for work on standards

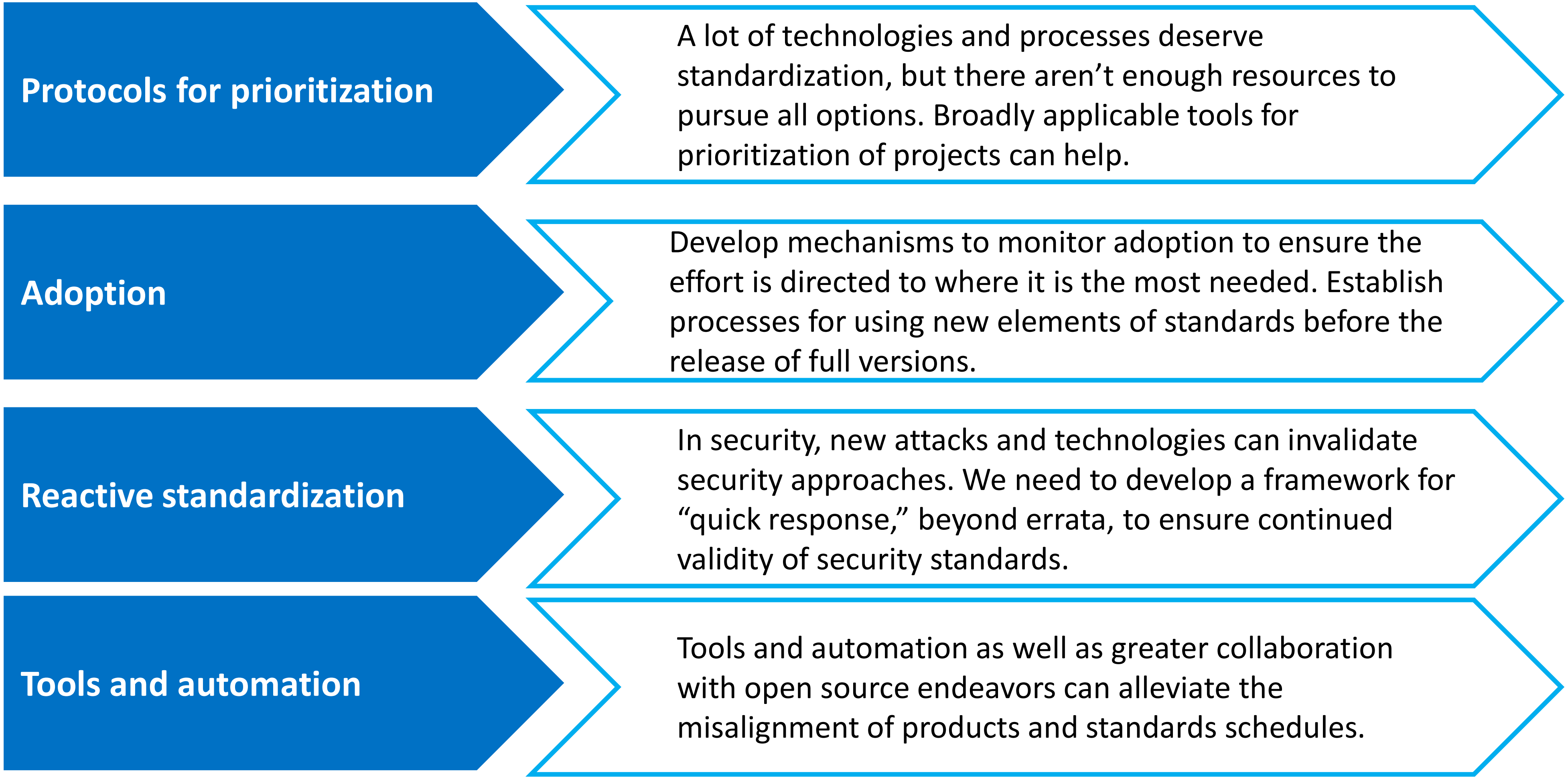
New incentives in the standardization space, to ensure the work is recognized beyond one SDO when it is appropriate.

Expertise sharing

Mechanisms to ensure that scarce technical resources in specialized areas (especially in security) can collaborate across SDOs when needed.

Greater collaboration among SDOs can lead to greater availability of technical resources, especially in security, and less duplication.

Shared perspective for the future



Protocols for prioritization

A lot of technologies and processes deserve standardization, but there aren’t enough resources to pursue all options. Broadly applicable tools for prioritization of projects can help.

Adoption

Develop mechanisms to monitor adoption to ensure the effort is directed to where it is the most needed. Establish processes for using new elements of standards before the release of full versions.

Reactive standardization

In security, new attacks and technologies can invalidate security approaches. We need to develop a framework for “quick response,” beyond errata, to ensure continued validity of security standards.

Tools and automation

Tools and automation as well as greater collaboration with open source endeavors can alleviate the misalignment of products and standards schedules.

There are many more potential light weight next steps that ths standardization community needs to discuss.

THANK YOU!