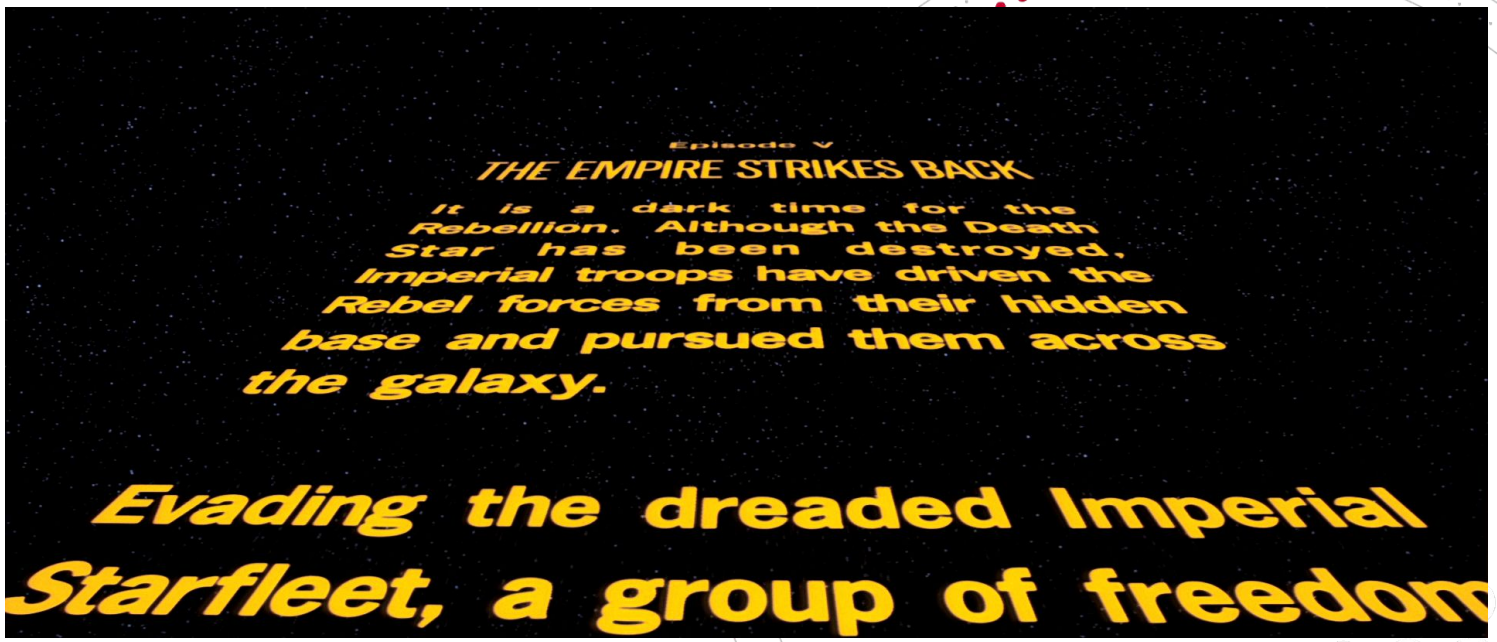
Symantec by Broadcom

# Why is cybersecurity standardization broken?

Arnaud Taddei
Global Security Strategist

22nd of March 2024

# As counter intuitive as it is cybersecurity standardization is broken




# Cybersecurity standardization in the context of regulation …

Symantec™ by Broadcom

# And unfortunately there is a huge industry engagement issue!

## And not just on “the West” … and in fact not just on the industry!

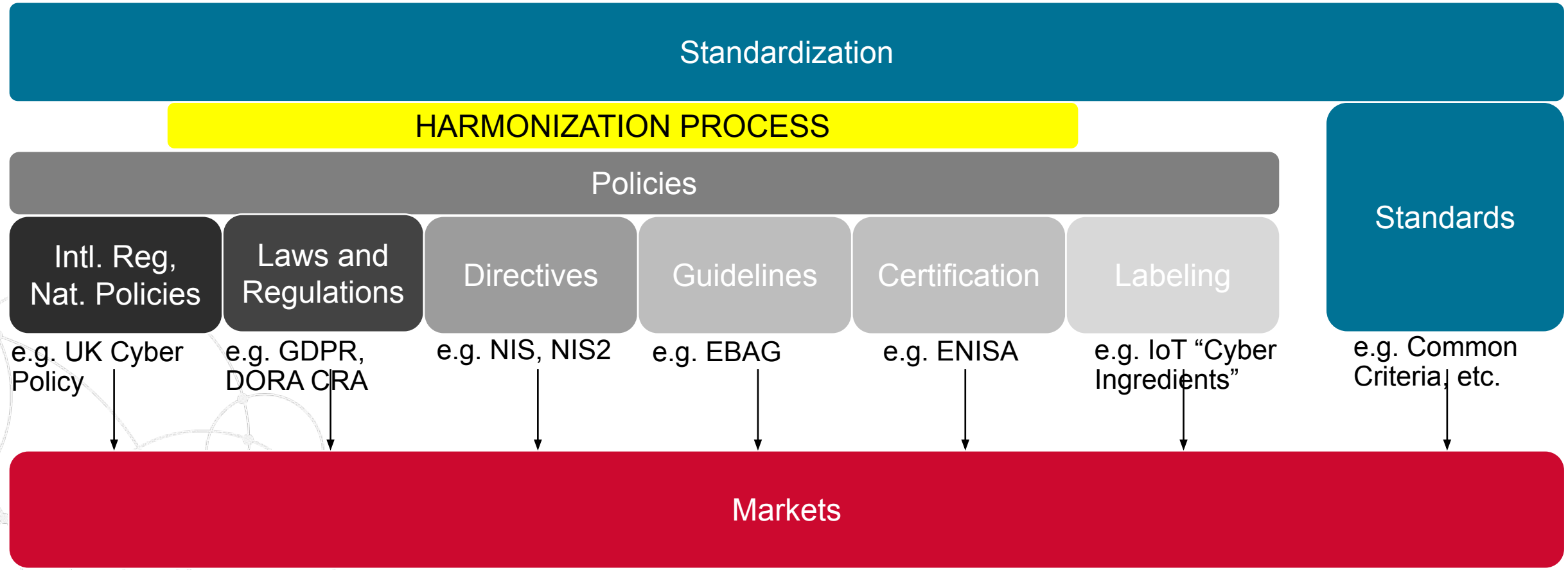
- Everyone is struggling with engaging in standardization
  - 20 years ago:
    - You: “Hey boss I need $2m to do all of this standardization work, meetings, etc.”
    - Boss: “Sure, the money is here”
  - 10 years ago:
    - You: “Hey boss I need $2m to do all of this standardization work, meetings, etc.”
    - Boss: “Hmmm, let’s scrutinize these $2m, looks like it is more $0.5m!”
  - Now:
    - You: “Hey boss I need $2m to do all of this standardization work, meetings, etc.”
    - Boss: “what ‘standardization’ mean? is it the same as opensource?”
- Key reasons
  - This is 20 years that in some areas, standardization is not taught in MBA and leadership course
  - Opensource is seen as much more tangible by industry leaders → leads to a product
  - What is the ROI?
  - Do we still need standardization in a world that is fragmenting?
    - “Physics has its laws”: here this is geopolitics
  - Do we still need standardization in a world dominated by public clouds?
    - “Physics has its laws”: inter-cloud connectivity doesn’t work → destroys interoperability

Symantec by Broadcom

# Why standardization matters?

## An unrecognized mechanism that shapes markets

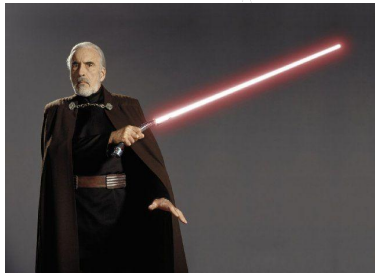


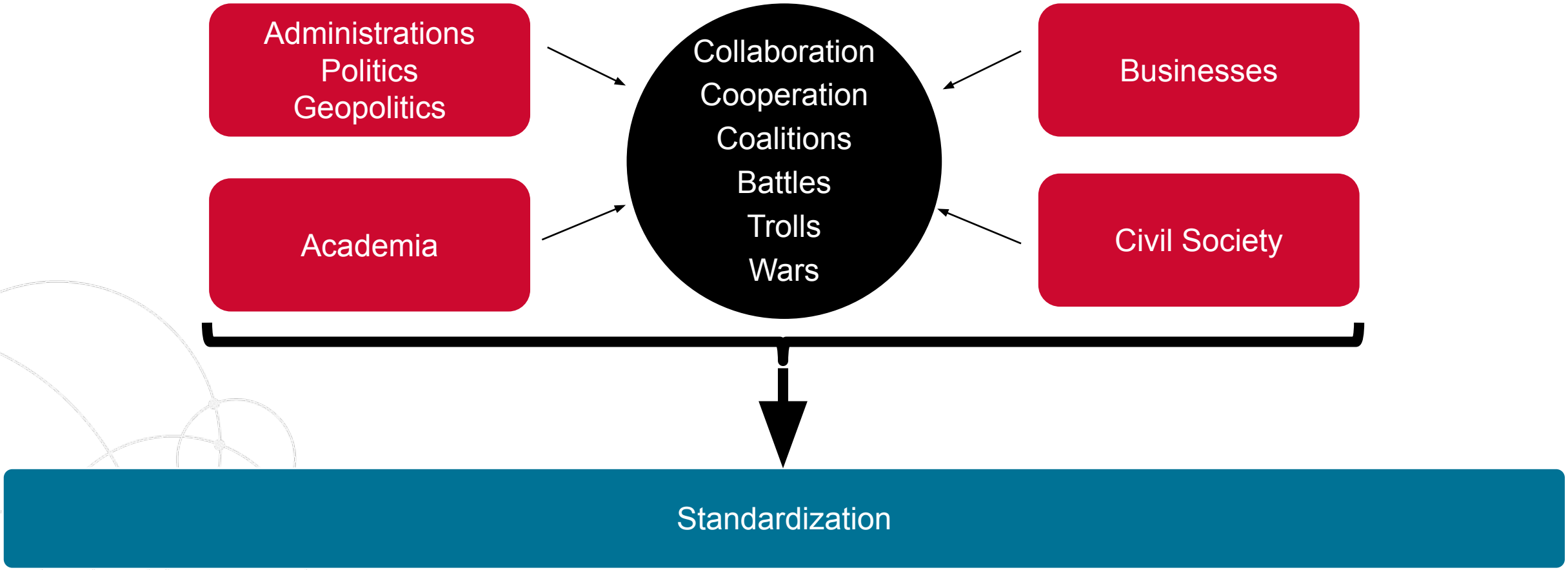

 

Symantec by Broadcom

# The problem – “The dark matter” behind Standardization

“My Lord I have a good news: the war has started”



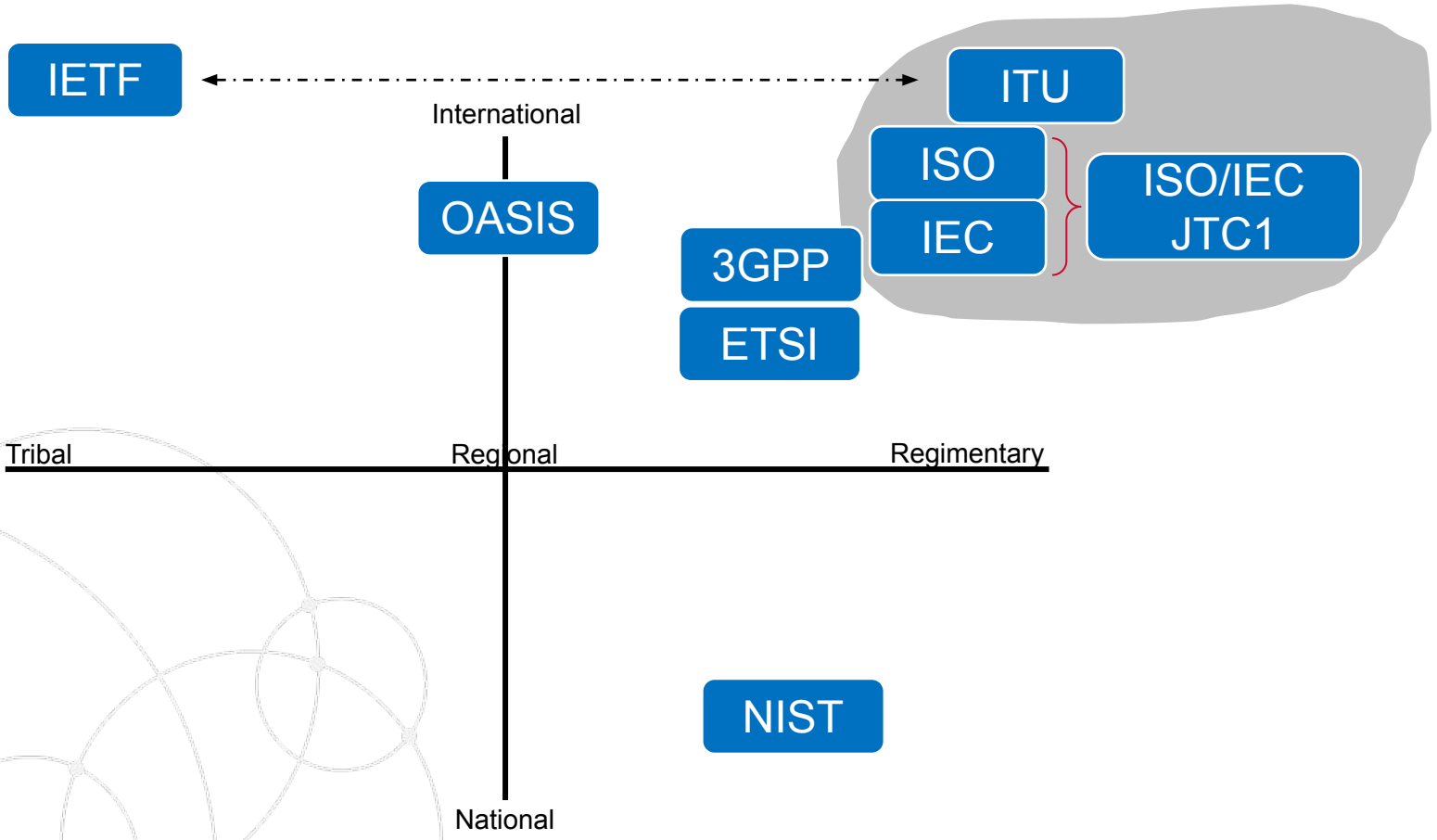


Symantec by Broadcom

# Decrypting the Cybersecurity Standardization Landscape

## An experimental **extremely simplified** analysis




- The story is way more complicated!
- Many other fora not on that list:
  - Identity focused organizations
  - By vertical organizations
  - A cohort of specific relevant organizations: CIS, NATO, GSMA, CA/B Forum, ENISA and EU nebulae, CSA, etc.
  - Vast spectrum of styles
  - The hardest one by far is 3GPP

Symantec by Broadcom

# As counter intuitive as it is cybersecurity is in a big Tower of Babel

## Cybersecurity is taken as hostage

Symantec by Broadcom

# GENERAL CONTEXT

Arms Race Example

**Defense Landscape**
Defenders are disorganized


**Attack Landscape**
In military terms
**THEY HAVE THE INITIATIVE**

We managed WannaCry with damage
Total loss from attacks potentially at **$T** level soon

**Explosion of the attack surface**

But creates new conditions

**Innovation**

Gives conditions to …

**Digitalization**

Both too slow and too fast (lack of ethics view) to adopt innovation

Very fast to adopt innovation against “us”; good intelligence of market and industry dynamics

But Accelerates too

Accelerates

**COVID19 non neutral!**

Symantec by Broadcom

# GLOBAL SECURITY STANDARDIZATION

**A lot of Dark Matter: 4 Stakeholders engaged in a huge battlefield**

Administrations

Academia

Business

Civil Society

Stakeholders "Dark Matter"

Frames

Structures

Security Standardization "Universe"

ISO IEC IETF 3GPP

ITU

ETSI

OASIS

GSMA

IEEE NIST

+ National Standard Bodies
Regional Standard Bodies
Industry Associations, etc.
NATO, MEF,

**Coordination and collaboration exist but improvements are required**

**Security Standardization is increasingly fractalized**

UNITED NATIONS

ITU

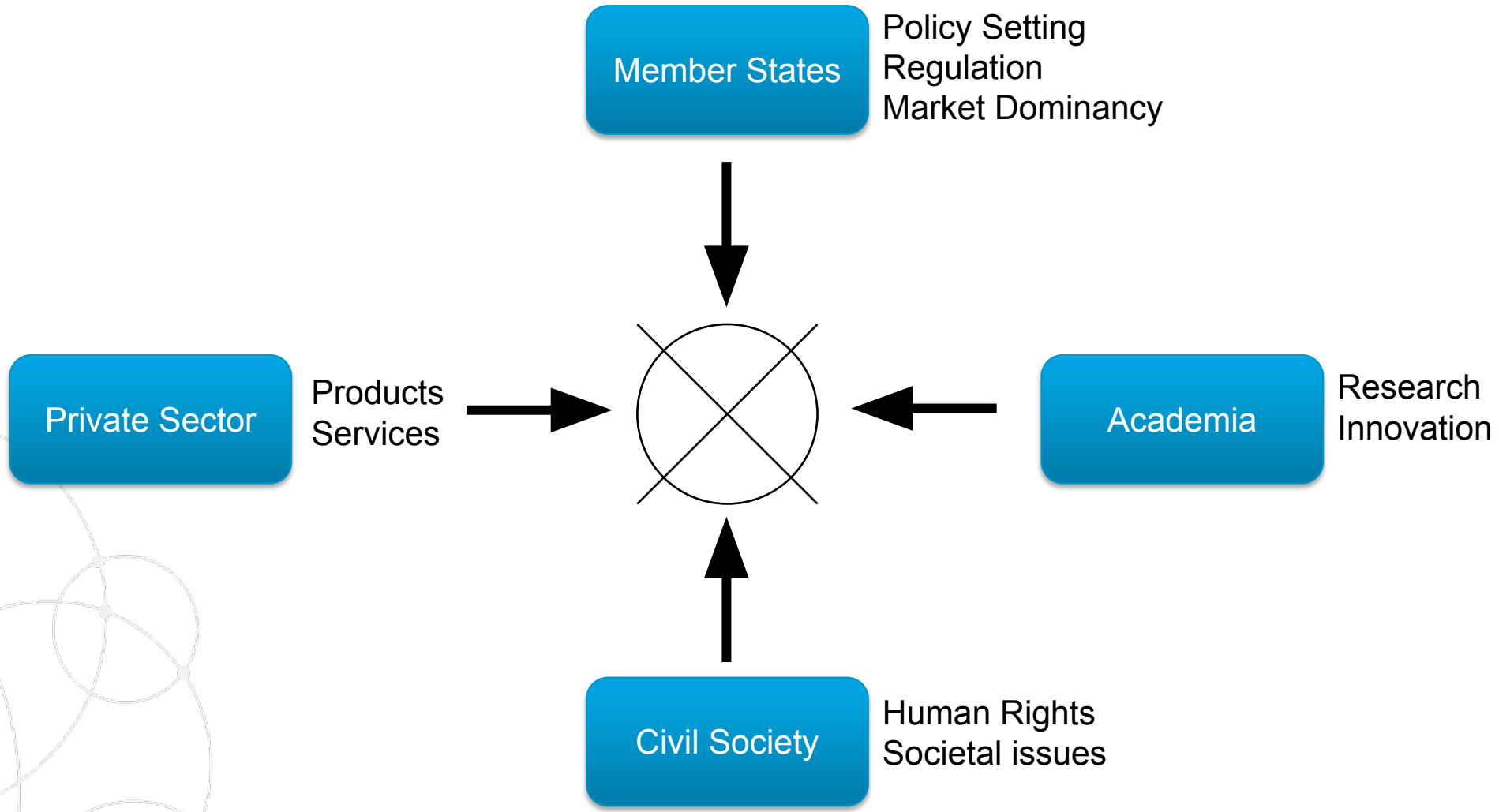
ITU-T

SG17

Symantec by Broadcom

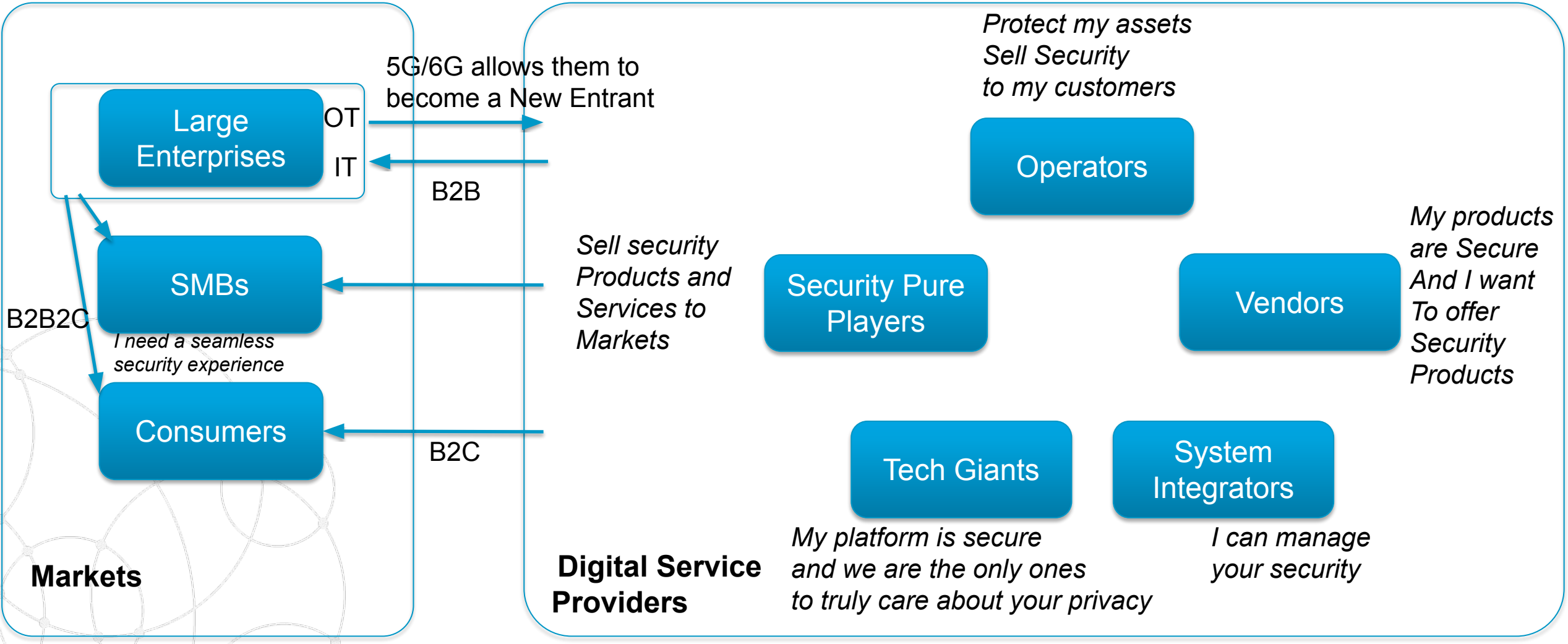
# Babel Tower terminology example: Privacy



Symantec by Broadcom

# Cybersecurity in Digital Service Providers Market Dynamics



Symantec by Broadcom

# What is happening?

- Diktat of the “platform” as a new business model
- Powered by a move from the (operating) system approach to the “cloud” as new operating system
- Rise of the hyperscalers on the west and then on the east
  - Ferocious adoption/addiction force è consumerization of IT
- CSPs cornerized down to 5G and now 6G
- Innovation under explosion and approaching singularity, many good, bad and ugly side effects
- Interlaced with a change of culture (movement to “Agile”, not just IT)
- More and more intrication with the 4 knights hidden in the dark matter
  - Administrations, business, academia and civil society
  - STRONG geopolitical, military, societal, sustainability (SDG, ) agenda, etc.
- Acceleration of regulation aspects
  - national/regional/”international” policies, directives, laws, certification, labelling, and market regulation
- Cybersecurity now clearly taken as an hostage of a completely different story
- And COVID Accelerates everything!!

Symantec by Broadcom

# And now more than ever!

2 examples to illustrate threat landscape changes and attack surface explosion

- Generative AI will scale social engineering and attack automation
  - LLMs are about finding statistically the next words
  - Harder and harder for specialists to make the difference
  - So how hard it is for non-specialists or when specialists are under stress?

- IoT explosion to 1T devices will explode the attack surface down to 5G/6G
  - In particular how to deal with Constrained devices?
  - How to deal with securing those trillions of clouds supporting IoT communication to IoT platforms?
  - IoT or IoE?

Symantec by Broadcom

# And even more

2 examples of what is making conditions worse every day

- Fragmentation will aggravate:
  - under the weight of geopolitics
  - Regulation will contract on ‘borders’
  - All levels of assets will be affected: Internet, Clouds, Infrastructures, Hardware, Software, IPR

- We don’t document our security architectures!
  - Design and Architecture methodologies are simply not there
  - Leading to no way to even understand complex triads:

    Privacy / Security / Safety

    - Just on Privacy / Security: Superposition of two states with no approach to healing the Privacy zealots and the Security zealots

Symantec by Broadcom

# First Conclusion

Security as we know it today won’t work in the future

Even rebalancing Software Supply Chain Security vs Security Controls
(SBOM School vs ZT School)
won’t be sufficient

Attackers will have a solid and growing advantage in short and mid term

Symantec by Broadcom

# What does it mean for standardization?

This calls for:

1) Where is the current ‘cybersecurity standardization’ map?
2) Where is the future ‘cybersecurity standardization’ map?
3) Which SDO is doing what?
4) What are the gaps?
5) Where best those gaps should be pursued?

Symantec by Broadcom

# Considerations for the future

Symantec™ by Broadcom

# The ‘clinic’ story → Biology metaphor

How a small group of people is trying to rethink the story

Before pandemic, a small group of people realized the issue and thought this way:

*“If we were in health, and if we needed to establish a clinic, we would have all parameters to establish one be in the Sahara desert or in the posh area of Cologny in Geneva.*

*But in cyber it would be close to impossible as Wannacry showed and it is not better today as a number of key constituencies are missing, nor do we have a model!”*

The pandemic showed that hospitals could be raised in 24 hours, we doubt we are able to still achieve this in cyber!

From this metaphor, ‘we’ started to develop against key gaps and a Common Security Model

# Some success stories

## Fixing some urgencies

The first ever standard on Cyber Defence Centers was delivered as X.1060 @ITU

The first ever standard on collaborative playbooks is in a good way as CACAO @OASIS

The first ever “standard” on cybersecurity events cross industry is in V1.0 as OCSF … and paired with X.icd-schemas @ITU

The ITU-T WTSA20 Resolution 50 gives 2 key instructions to SG17: 5 and 6 which allows SG17 CG-SECAPA to continue from CG-SECAD in the last study period: Goal to establish a Common Security Model

A KEY work item on security for AI was established in SG17 Q15 X.sr-ai

Key work on simulation in progress in the incubation queue of SG17

PKI is being revisited: Constraint Devices, DPKI

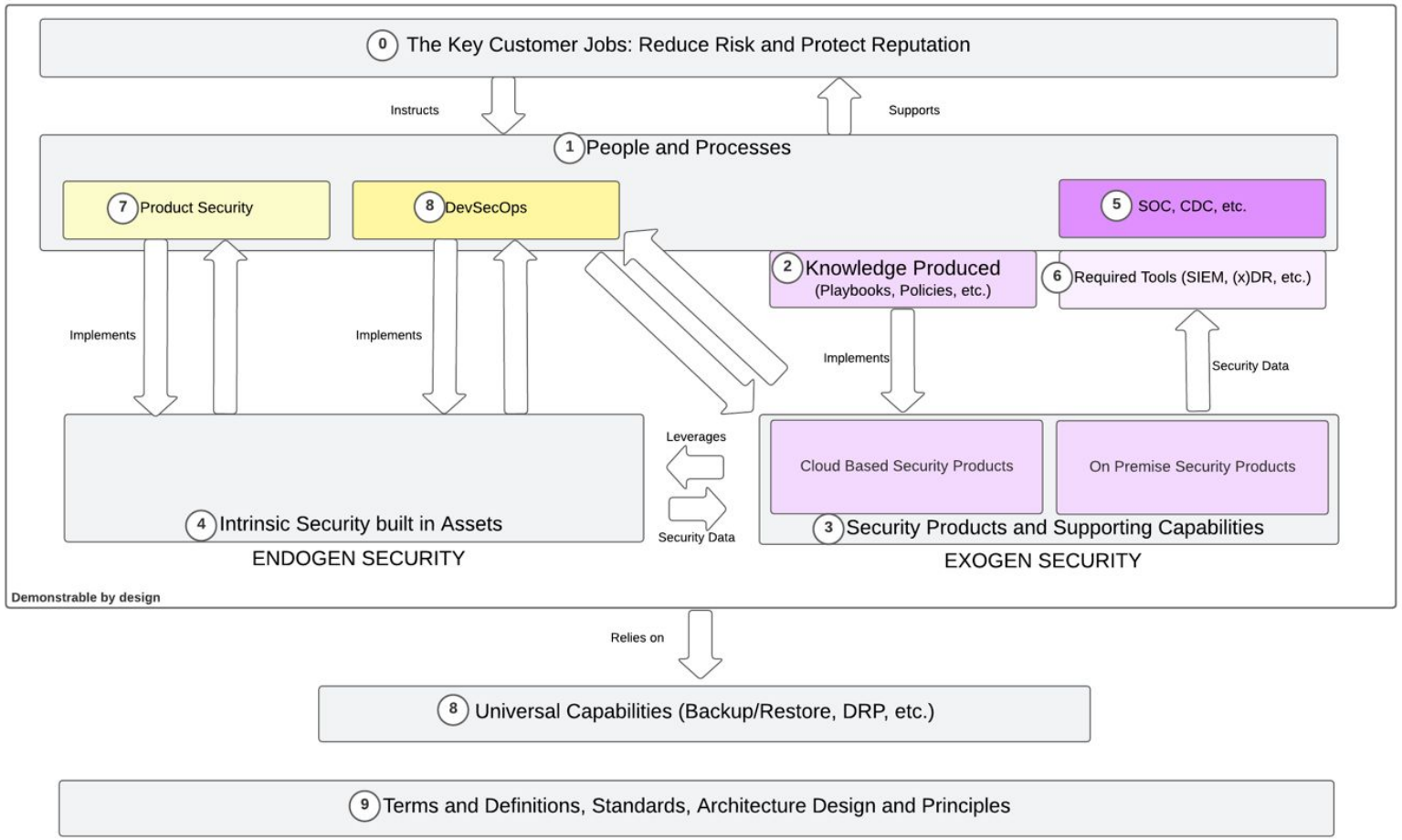
 

Symantec by Broadcom

# ITU-T SG17 Common Foundation?

Work in Progress

## Work in Progress - Discussion for an ”OSI model for cybersecurity”




Narrative: “if all the job is to reduce risk and protect reputation then what are the key constituencies for a reasonable operational security:

- People and process …
- … who extract their knowledge …
- … to instruct a product stack …
- … to protect assets”

This narrative already transformed an entire community, changed national cybersecurity policies, added two new instructions by UN Resolution, agreement to establish new Compendium … several key contributions expected by Fall 2023

Symantec by Broadcom

# An OSI Model for Security

## Simple enough but not simplistic

BUT IT FAILED → Forced us to go one order of magnitude deeper

People and Processes

Knowledge | Tools

Endogen Stack | Exogen Stack

On Premise | Cloud Based | Cloud Based | On Premise

Universal Capabilities

Terms, Definitions, Design Principles, Architecture Methodolgy, etc.

Symantec by Broadcom

# Conclusions

Cybersecurity standardisation is not in a good shape

It requires:

- a strong analysis
- an alignment between many parties
- a colossal amount of work for the next 10 years

At the moment an ad-hoc group approached it on a very selective basis

- delivered already a number of new and unexpected gaps
- with a metaphor in mind coming from health and biology
- determination to change cybersecurity to address the next 20 years challenge
- perhaps one view out of many others to seize this elephant … and opportunity

Symantec by Broadcom

Symantec by Broadcom

# Thank You

Symantec™

by Broadcom