GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

Second Annual Event

Encouraging Digital Security Innovation

TÜV SÜD

OECD

BETTER POLICIES FOR BETTER LIVES

Cyber Israel
National Cyber Directorate

The Israeli Eco System
National Risk Management & Innovation

REFAEL FRANCO
Deputy Director General
Head of Robustness Division


CERT
IL

Israeli CERT Alert

התרעה דחופה: פגיעויות קריטיות בציוד VPN של מספר יצרנים [עדכון]

תקציר

1. לאחרונה פורסם כי ציוד VPN של מספר יצרנים מוכרים (Palo-Alto, Fortinet, Pulse Secure) חשוף לפגיעויות העלולות לאפשר לתוקף מרוחק ובלתי-מזוהה הרצת קוד על הציוד, או קריאה של קבצים מהציוד, כולל פרטי הזדהות של משתמשים.
2. לחלק מהפגיעויות קיים POC ברשת, וחלקן ניתנות לניצול באמצעות גישה ל- URL מסוים על ציוד ה- VPN.
3. מומלץ לכל ארגון העושה שימוש בציוד VPN שנמצא פגיעה, לבחון ולהתקין את עדכוני האבטחה הרלוונטיים בהקדם האפשרי.

ALERT

פרטים

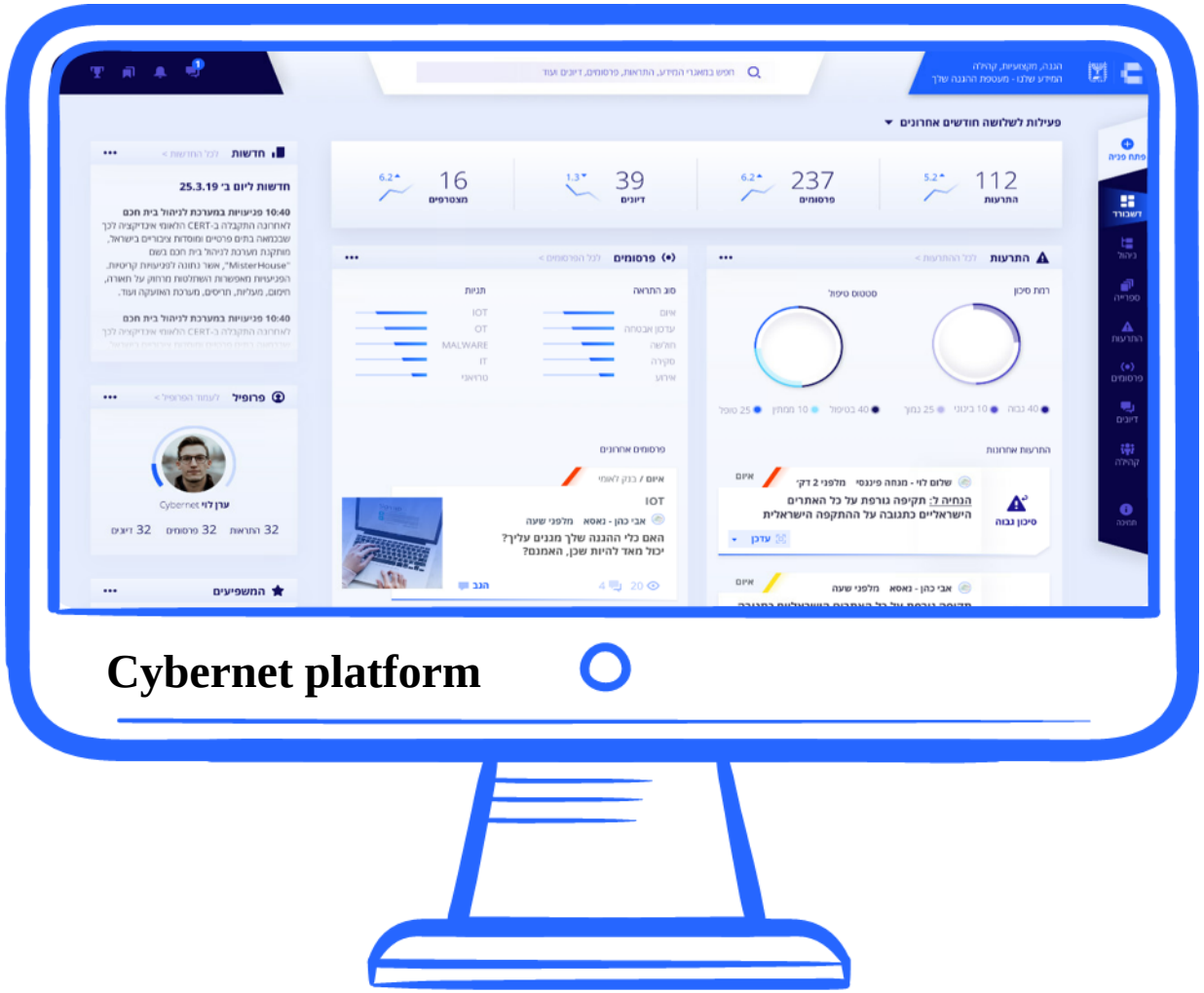
1. המוצרים בגרסאות הם:

Palo Alto Networks GlobalProtect portal and GlobalProtect Gateway
- PAN-OS 7.1.18 and earlier
- PAN-OS 8.0.11-h1 and earlier
- PAN-OS 8.1.2 and earlier

Pulse Connect Secure and Pulse Policy Secure
- Pulse Connect Secure 9.0R1 - 9.0R3.3
- Pulse Connect Secure 8.3R1 - 8.3R7

למרכז לדיווח על אירועי סייבר: 119 team@cyber.gov.il cyber.gov.il מערך הסייבר הלאומי ב-

1



Cyber Israel
National Cyber Directorate

Sharing information & tools via vpn ssl event

From: [redacted]
Sent: [redacted]
To: C[redacted]
Subject: [redacted]

Dea[redacted]

Recently, a research describing various vulnerabilities in some SSL VPN offerings was presented at Black Ha
Proof of concept code for some of the vulnerabilities was posted on the Internet, and are now actively exp
CERT-IL published an urgent alert to all users of Palo-Alto, Fortinet & Pulse Secure SSL VPNs, urging them t
Due to our national responsibility to protect the Israeli cyber sphere, and our main concern regarding this p
I would like to invite you to participate at a conference call with other trusted CERTs, to share with you our

Samoor tool - INCD "on demand scan tool" to detect vulnerable VPN SSL devices

Dear Colleagues,

1. Please find attached a zip file which includes "Samoor", ("the scan tool") along with its operating "readme" technical file.

Invite you to participate at a conference call with other trusted CERT's

ISRAEL CYBER JOURNEY

- SECURING ISRAEL'S CYBERSPACE
- SECURING ISRAEL'S LEADING POSITION IN CYBERSPACE

Human Capital – Cyber journey

Academia - Cyber Research Centers

Technion

Engineering Oriented

Haifa University

Inter-Disciplinary

Tel Aviv University

Inter-Disciplinary

Bar Ilan U

Cryptography

Hebrew University

Network and Protocols

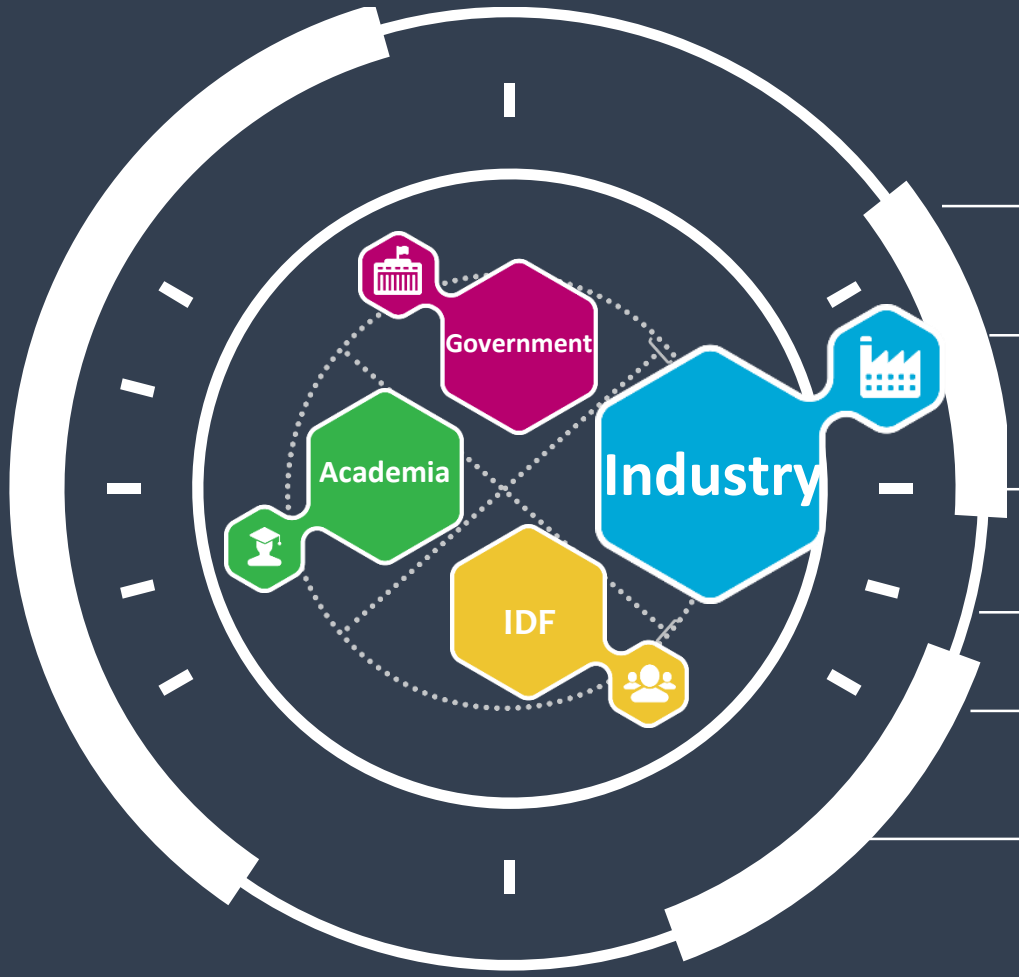
Ben-Gurion University

Applicative Research

6 Academic Cyber Research Centers:

- **~180 researchers**
- **~330 graduate students**

Innovation Labs

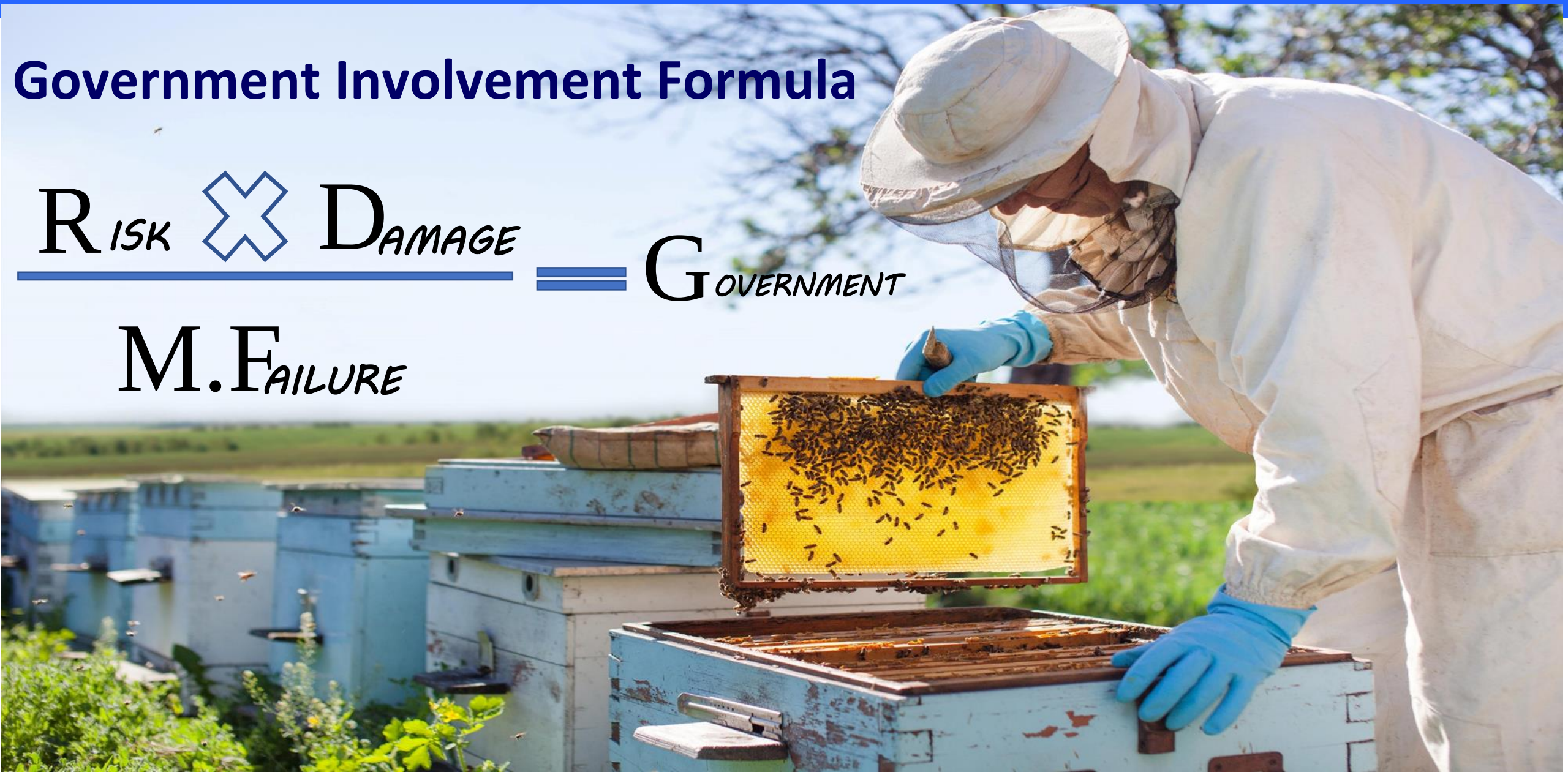


- Energy – SCADA / ICS
- Fintech security
- Smart transportation
- Medisec
- POC
- AI, 5G

Cyber Israel
National Cyber Directorate

Government Involvement Formula

$$\frac{\text{Risk} \times \text{Damage}}{\text{M.Failure}} = \text{Government}$$



Cyber Israel
National Cyber Directorate

Robustness

Cyber robustness is aimed to reducing the attack surface and creating a more difficult environment for offensive rivals actions, at the Israeli cyber space.

Cyber Israel
National Cyber Directorate

Government Involvement

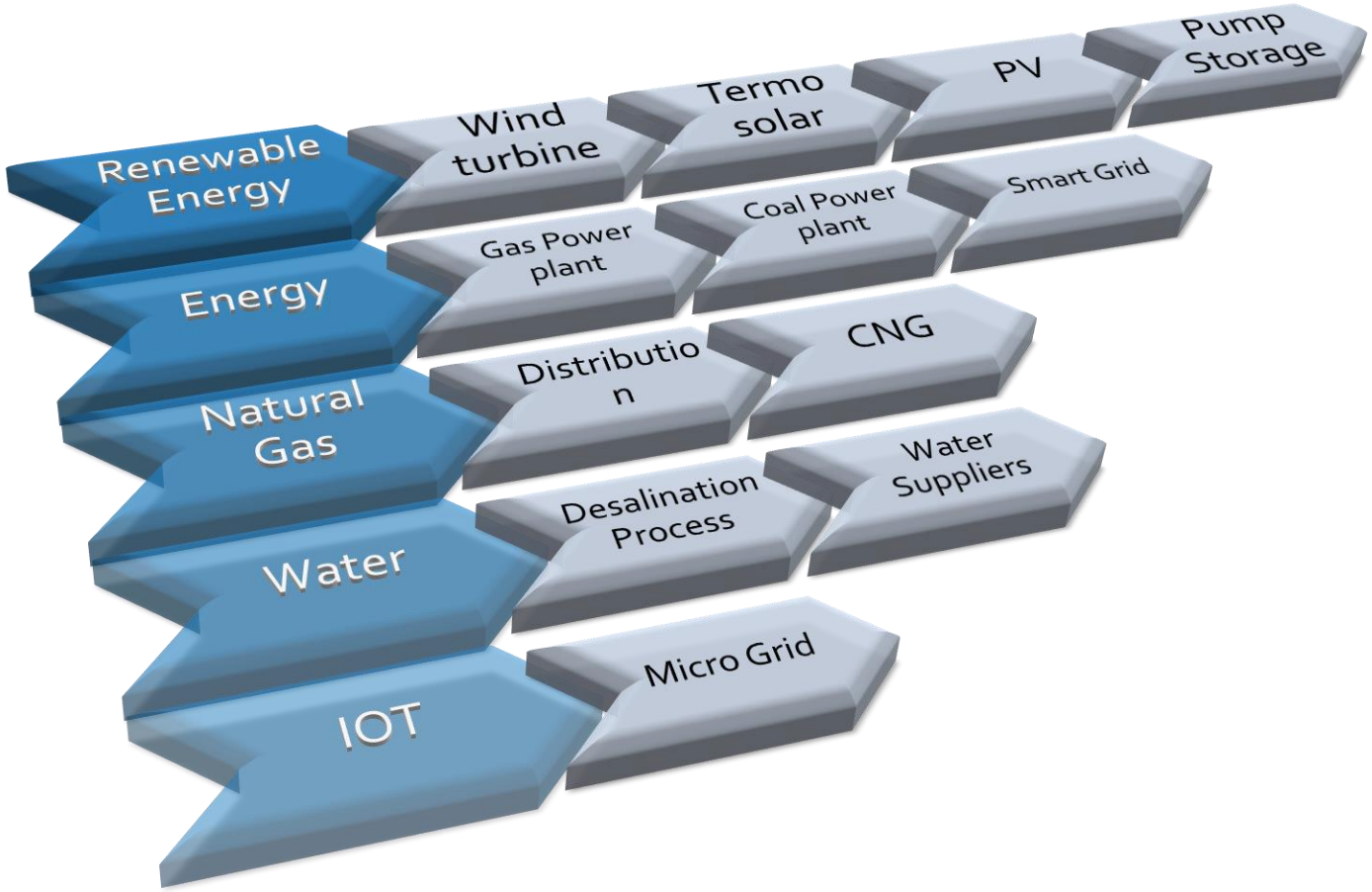
Lack of knowledge

Major Risk

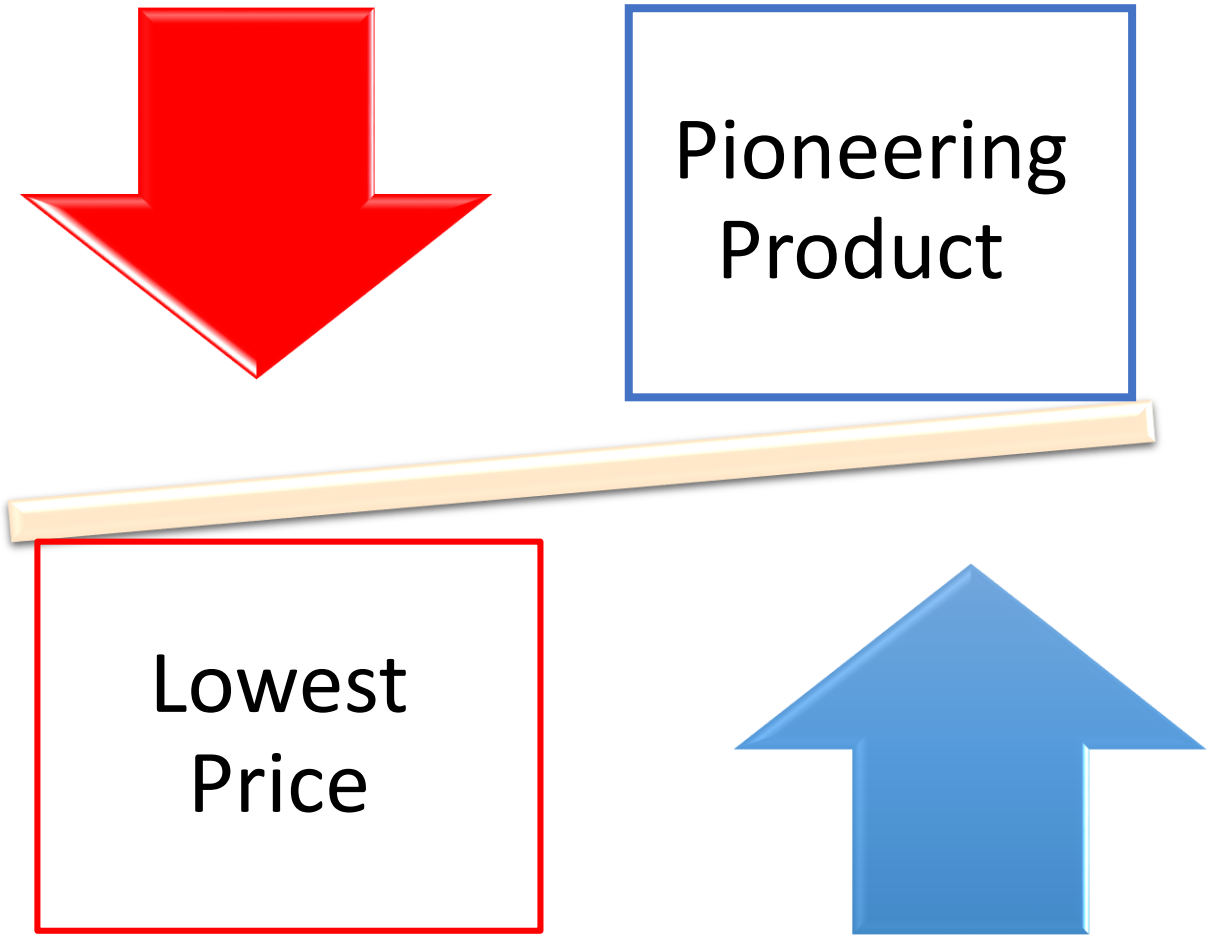
Market Failure

Cyber Israel
National Cyber Directorate

National SCADA lab



Government Innovation Cyber Tenders



Cyber Israel
National Cyber Directorate

Heat Map – Risk & Damage Indicators

Cyber Infrastructure Assets	Information Asset	Top in Sector	Critical to Emergency	Damage to Public Trust	Governance	A necessity for the public without an alternative	Economic Damage	Human life	Score
	Small to medium database	Rated at 30% less important than the sector	Not significant in an emergency	Partial & temporary damage to public trust		Inconvenience to hundreds of people	Millions of $ Indirect damage to the state	None	1
provides the infrastructure for a number of individual systems	Large private database with the potential to harm civilians	Is rated between 30% -70% of the sector	Emergency products are required	Damage to public confidence that is restored by itself			Millions of dollars in direct damage to the state	None	2
The service provides infrastructure for dozens of systems	Very complex	Ranked among the % of the	essential in an emergency	Damage to public confidence in its rehabilitation took weeks		tional difficulty for sands of people	Tens of millions of $ in indirect damage millions of dollars in direct damage to the state	Several	3
The service provides the infrastructure for hundreds of systems	An information asset of national importance	Ranked among the top 10% in the sector	Participate in national service objectives	Significant damage to the public's confidence in its rehabilitation took months		An existential difficulty for scores or functional difficulties for thousands	To d damage to the state	Dozens	4
The service serves as the infrastructure for a critical system in hundreds of organizati	A governmental information asset or a basis for other repositories	Rated part of the 5 most important in sector	Critical emergency service	Serious damage to public confidence in its rehabilitation takes	Undermining the government's ability to govern	An existential difficulty for hundreds of people without alternatives	Financial damage of millions of dollars or more	Larger than many dozens	5

Law Firm

Hosting

Large Food Manufacture

Insurance Company

First Responders

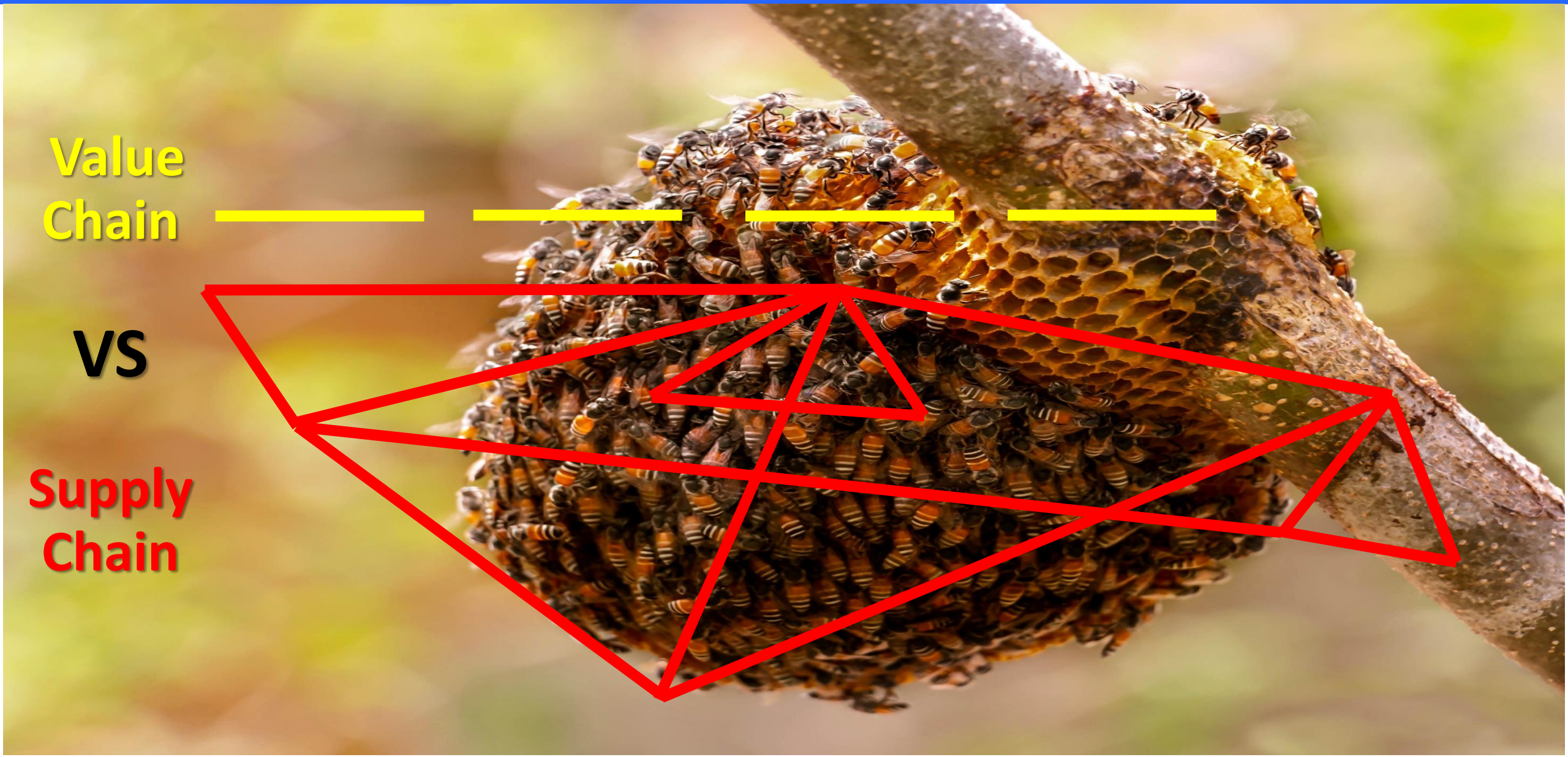
Large IT Integrator

Elections Committee

Bank

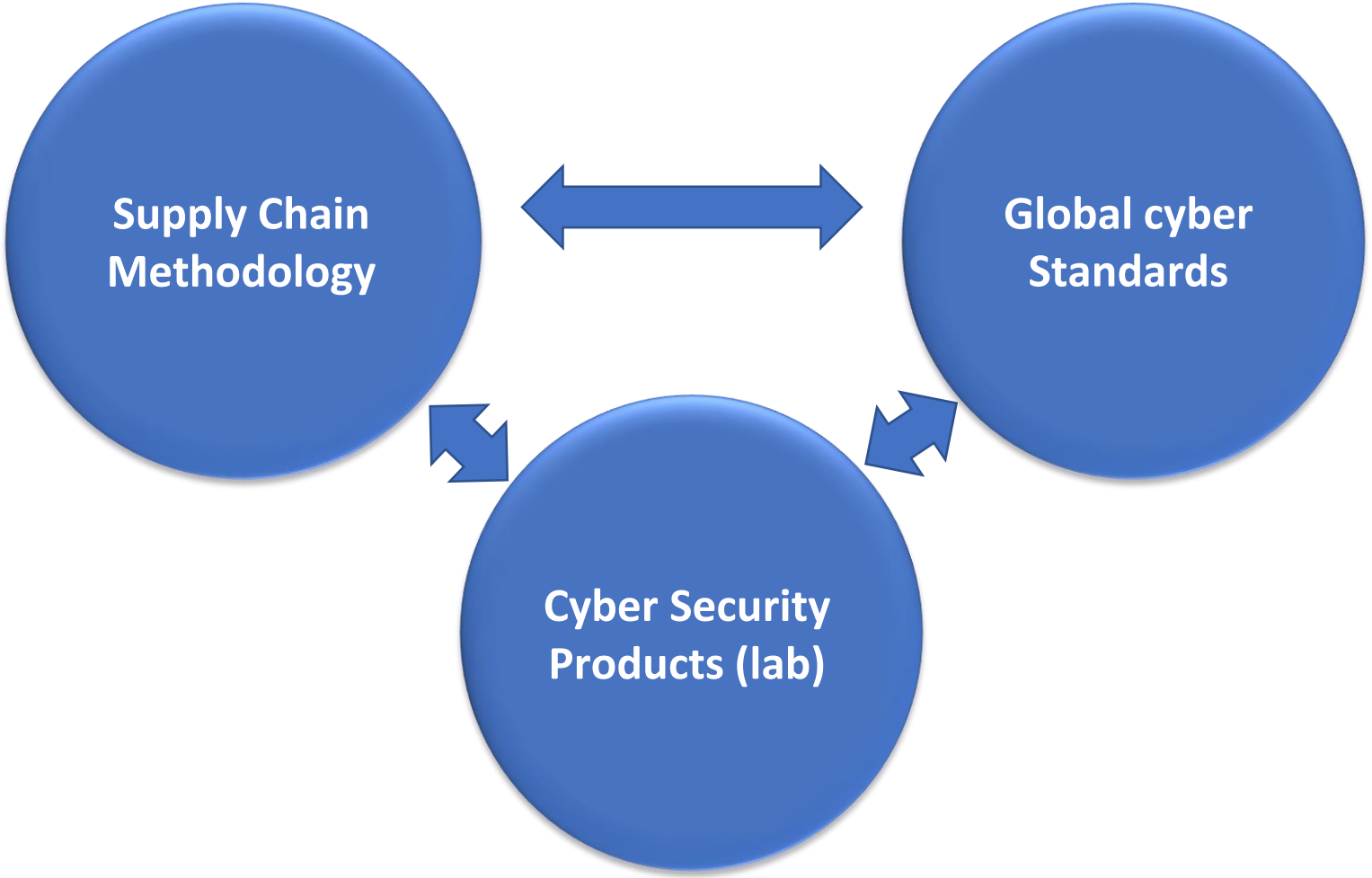
Hospitals

IEC – Economy & life Damage (CNI)

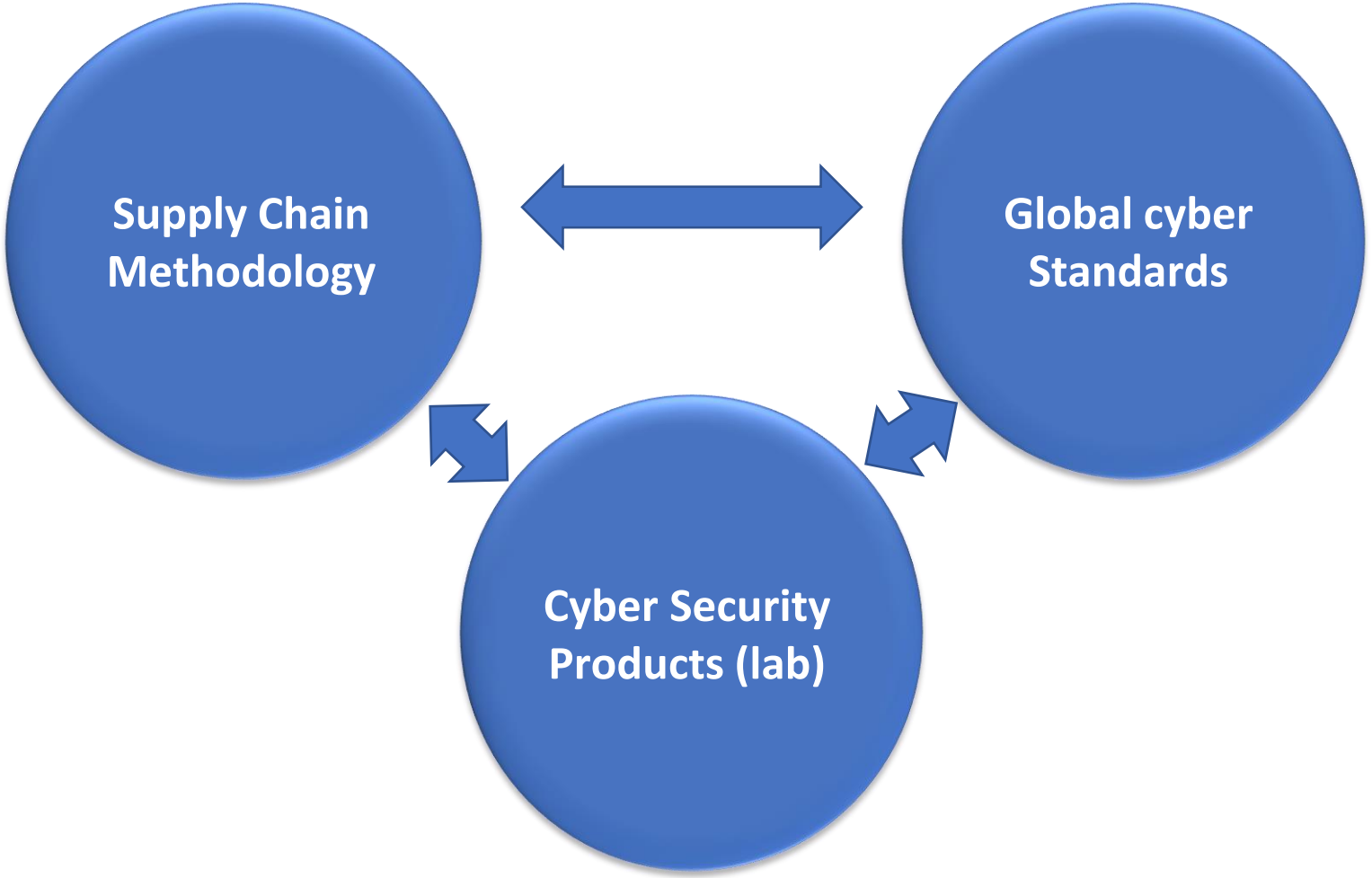


Cyber Israel
National Cyber Directorate

Supply Chain Eco System



Supply Chain Eco System



Our Global Reach

85 INTERNATIONAL PARTNERS (States & Organizations)

80 INTERNATIONAL DELEGATIONS

22 INTERNATIONAL AGREEMENTS

200 INTERNATIONAL TRAINEES

3 INTERNATIONAL CONFRENCES

2500 VISITORS TO CERT IL

8 HEAD OF STATES

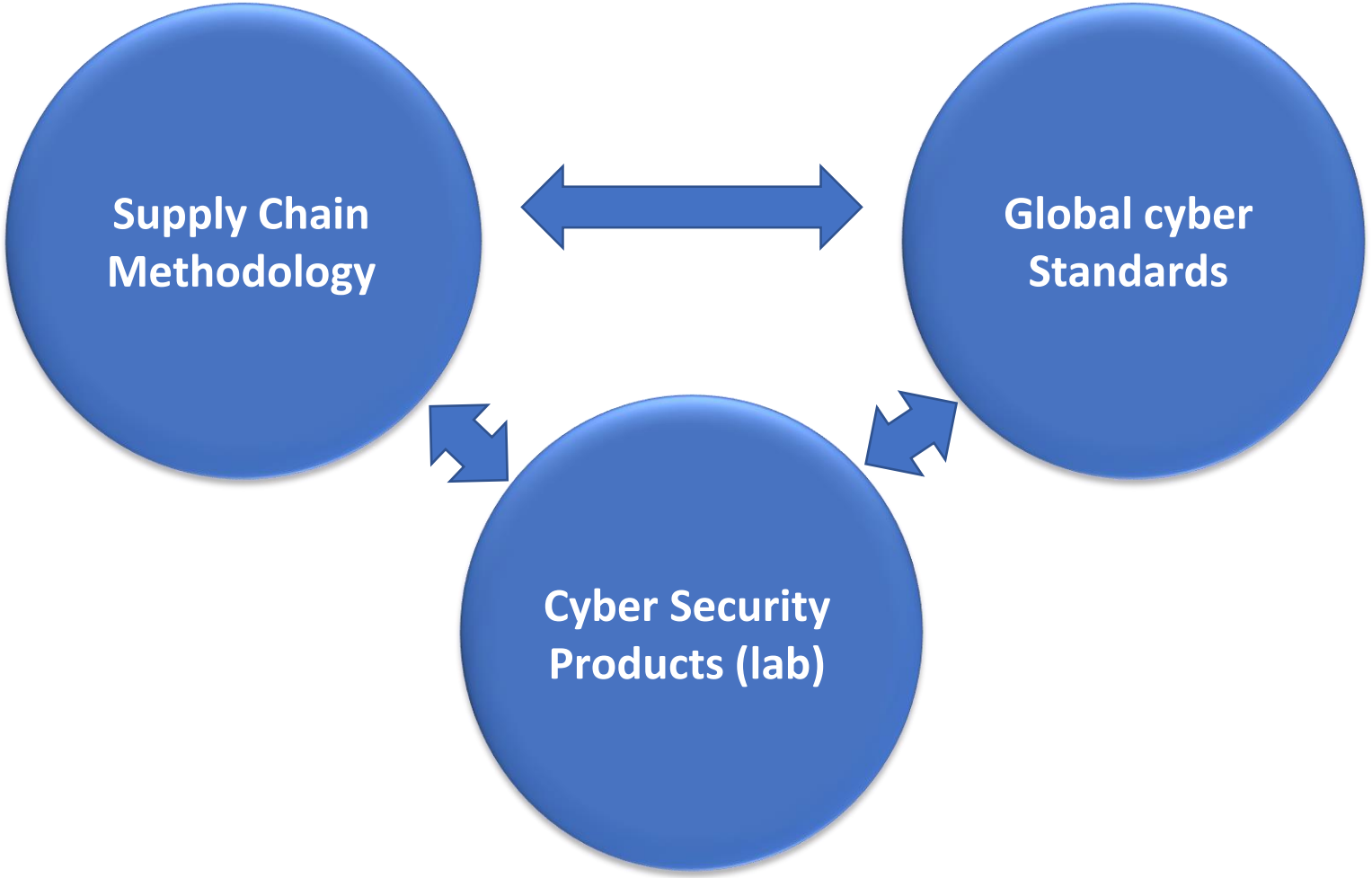
4 INTERNATIONAL CYBER EXCERSICES

SHARING INFORMATION PLATFORMS

CAPACITY BUILDING ADVISORY MISSION

B2B EVENTS

Supply Chain Eco System



Innovation Labs

FC3 – Finance

SCADA & OT

Biometric & ID

Meteor

Transportation & Aviation

Cloud & 5G

Cyber Israel
National Cyber Directorate

THANK YOU

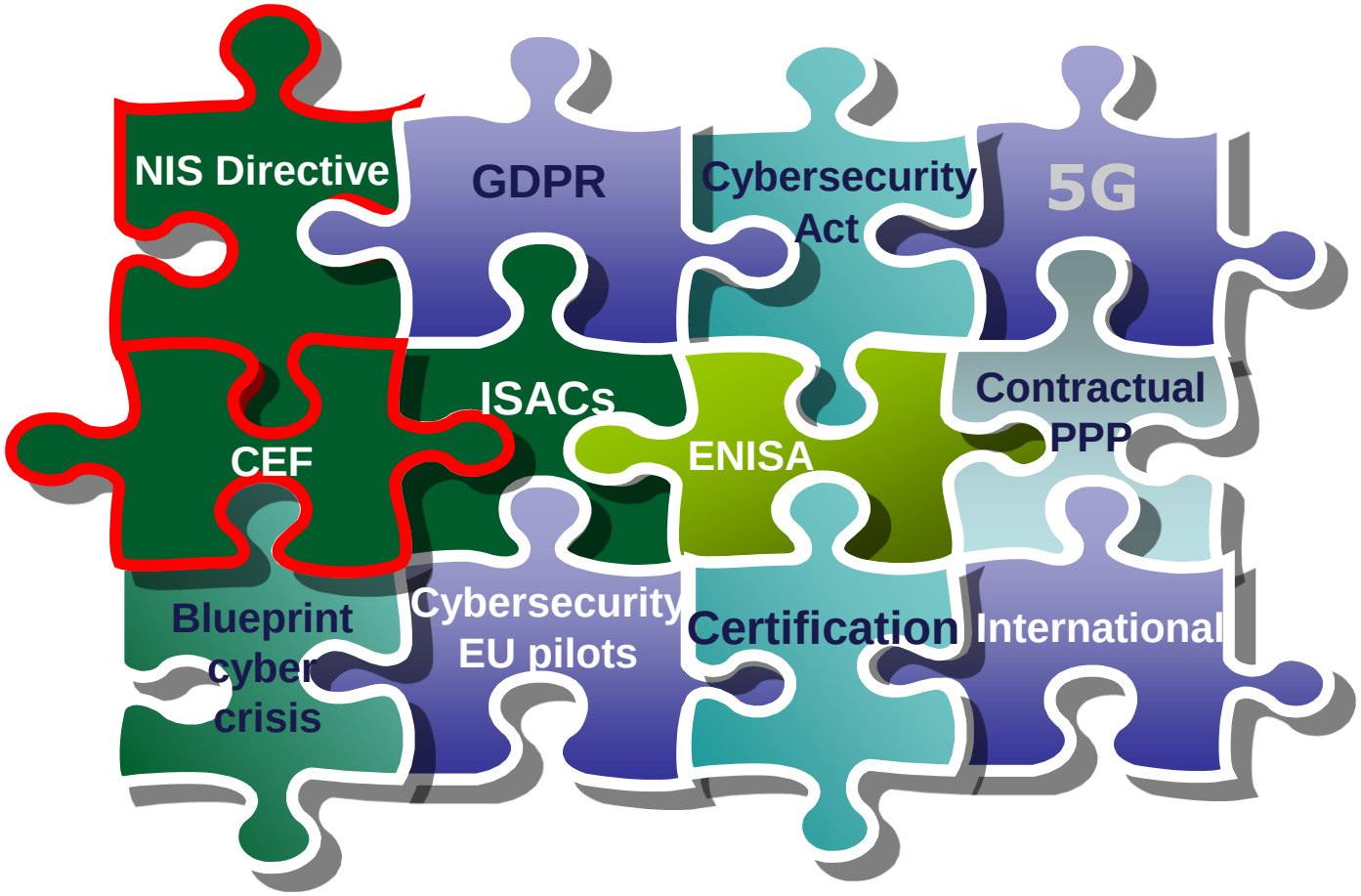
OECD Global Forum on Digital Security for Prosperity

Session 1 - Strategic Initiatives for Digital Security Innovation

14 November 2019
London

Ioannis Askoxylakis
Cybersecurity Technology & Capacity Building
Digital Society, Trust and Cybersecurity
DG Communications Networks, Content and Technology
European Commission

EU action in cybersecurity



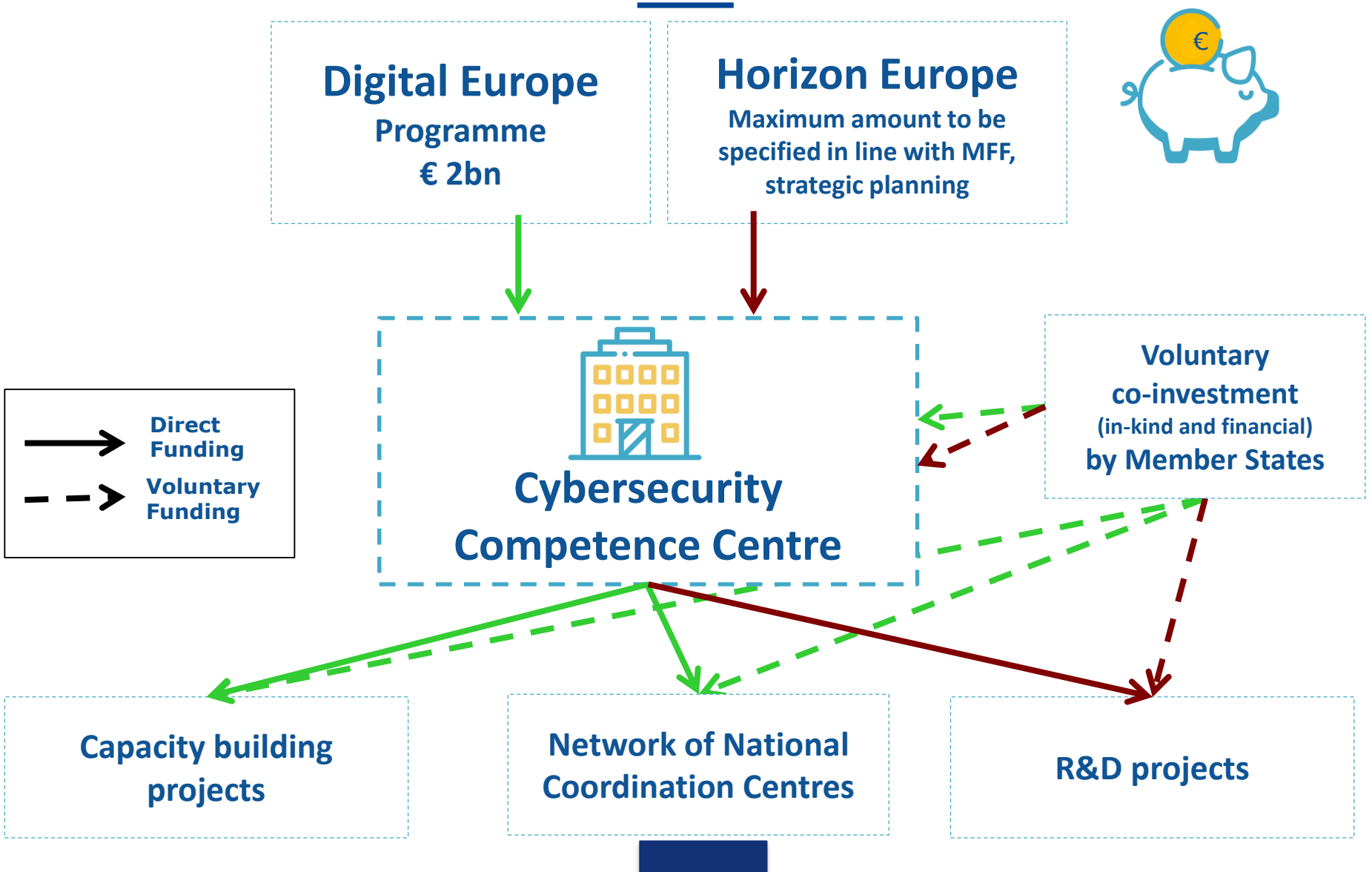
The Proposal for a European Cybersecurity Industrial, Technology & Research Competence Centre & Network of National Coordination Centres

European Cybersecurity Industrial Technology and Research Competence Centre

Centre's Role:

- Network coordination and support
- Research programming and implementation
- Procurement
- Ensuring synergies between civilian and defence spheres

2021-2027 proposed EU cybersecurity funding sources



DIGITAL EUROPE - initial funding priorities 1/2

- **Support to the network of National Coordination Centres;**

- **Key capacity building: the cybersecurity shield**

  Deploying a quantum-secured public communication infrastructure (terrestrial segment) with the aim at deploying Quantum Key Distribution (QKD) in various large-scale networks;

  Deploying through cyber ranges, with Member States and industry, a European cyber threat information network;

DIGITAL EUROPE - initial funding priorities 2/2

- **Certification scheme(s)**

  Support certification capacities

  Support SMEs to certify their products

  Provide certification testbed;

- **Widening the deployment of cybersecurity tools**

  Support for faster validation and market take-up of innovative cyber security solutions by businesses and public buyers;

- **Supporting the NIS Directive implementation**

  Strengthening the activities started under the current CEF Telecom programme (national authorities, CSIRTs, OES, DSP, …)

HORIZON EUROPE - initial funding priorities 1/2

- **Automated security quantification and certification**

  Verifiable security, privacy, and ethics

- **Resilient infrastructures and interconnected systems**

  Advanced cryptography; quantum

  Automated threat prediction, detection and response

  Human factors – risk and crisis management

  Authentication of IoT objects

HORIZON EUROPE - initial funding priorities 2/2

- **Securing disruptive technologies**

  Security ing AI - 5G - IoT – blockchain – distributed computing

  Big Data privacy

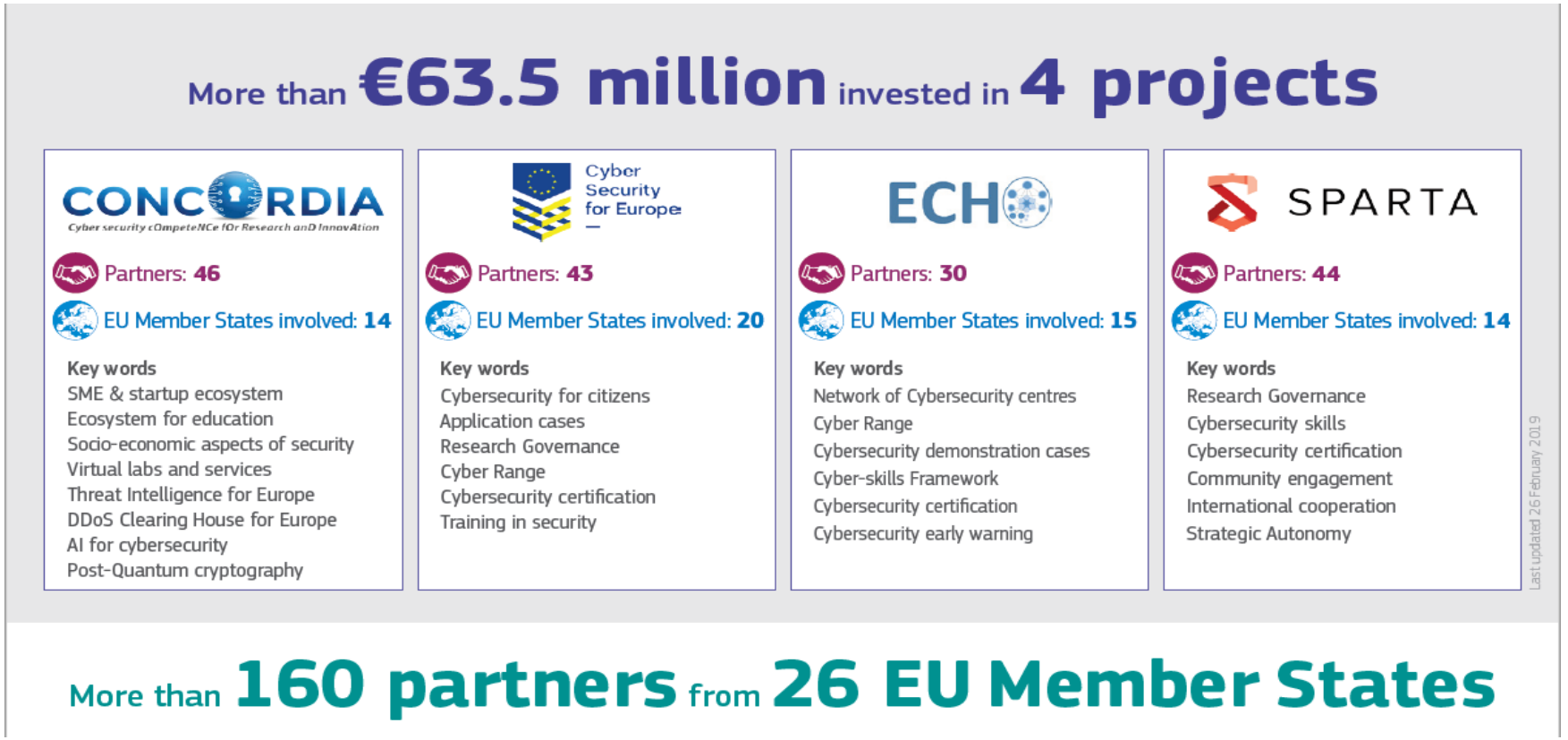
- **Hardware and supply chain security**

  Cryptography and its implementation

  Secure systems, despite vulnerable components

  Virtualisation

EU pilots to prepare the European Cybersecurity Competence Network



More info at:
https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

Current EU funding opportunities

Forthcoming topics in H2020 1/2

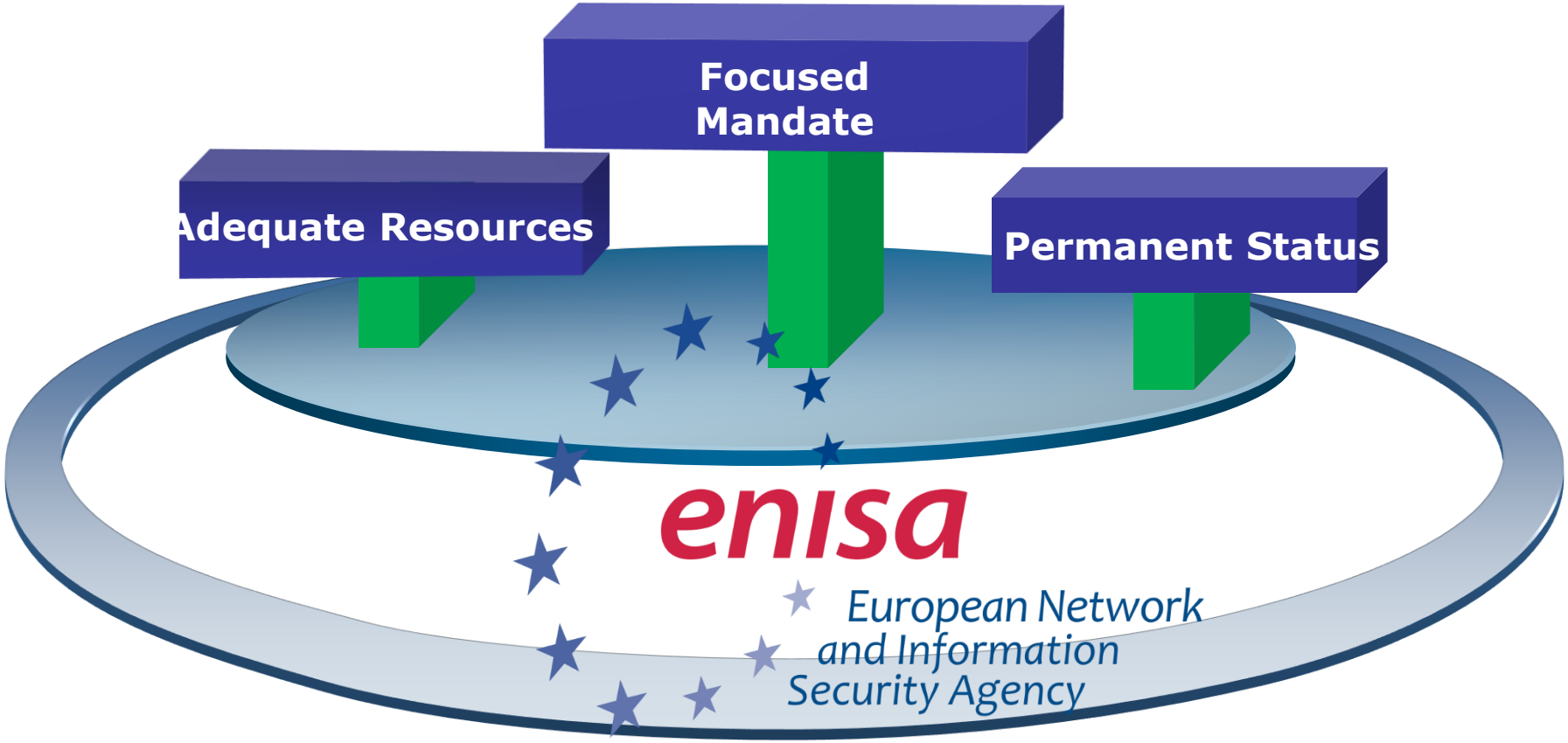
- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems. (RIA, 47.00 MEUR 19/11/2019)
- SU-DS02-2020: Intelligent security and privacy management. (RIA/IA, 38.00 MEUR 27/08/2020)
- SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. (IA, 10.80 MEUR 27/08/2020)

Forthcoming topics in H2020 2/2

- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. (IA, 20.00 MEUR 27/08/2020)
- SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. (IA, 20.70 MEUR 27/08/2020)
- SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe (IA, CSA 20.00 MEUR 27/08/2020)

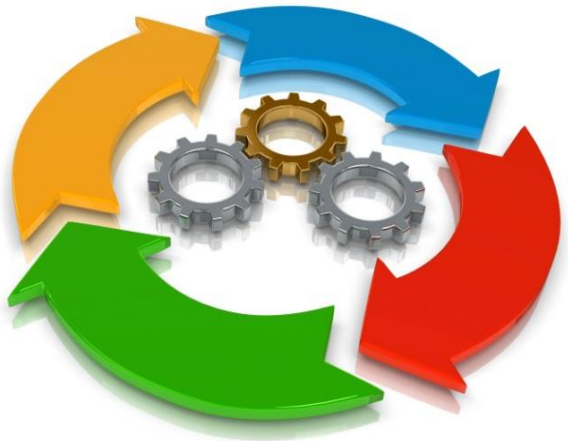
The EU Cybersecurity Act

What's new with the new proposal?



Cybersecurity Certification

*A **voluntary European** cybersecurity certification **framework….***



…to enable the creation of tailored EU cybersecurity certification schemes for ICT products and services…

…that are valid across the EU

European Commission

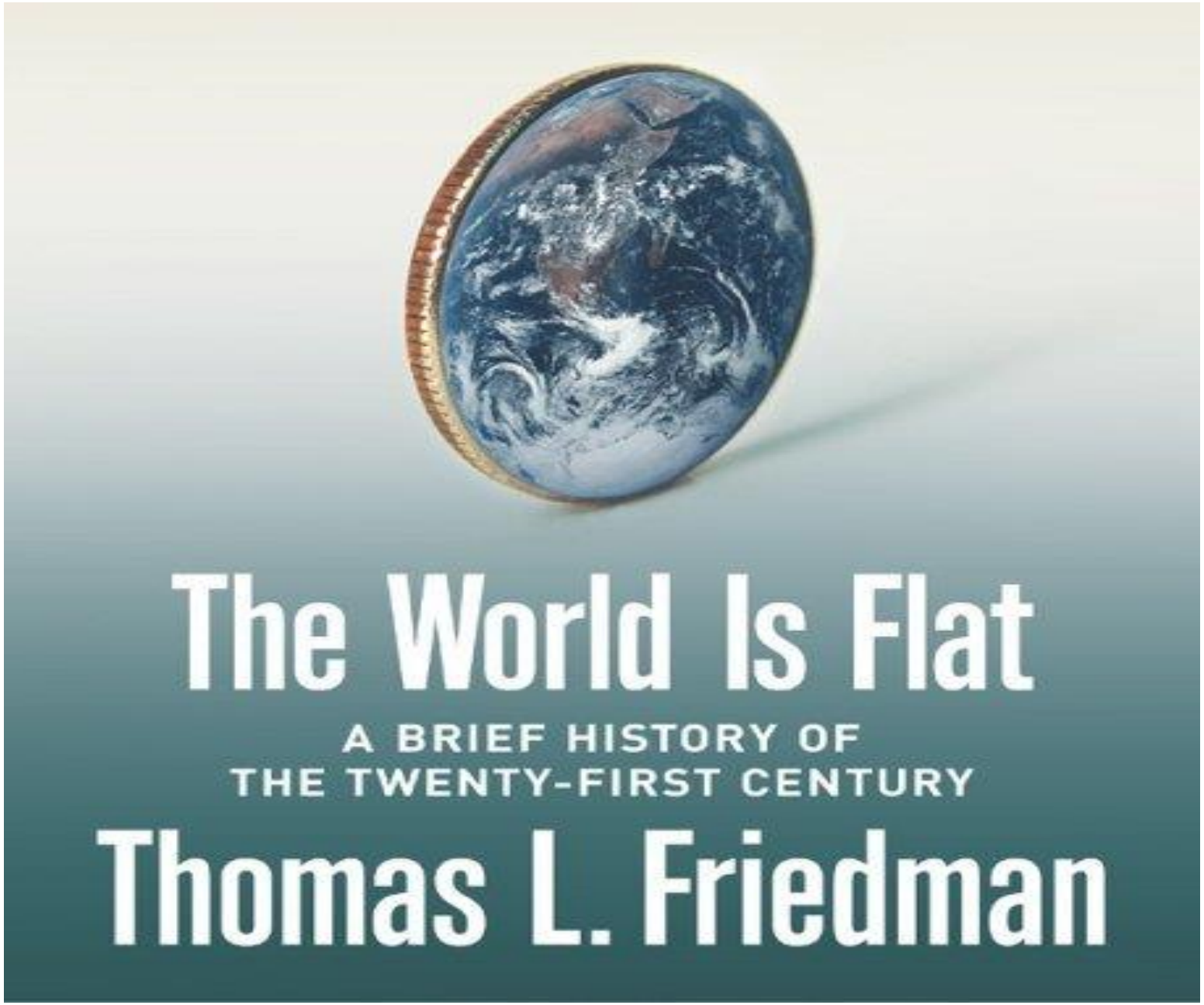
Thank you for your attention!

Opportunities and Challenges to Enable Digital Security Innovation: MIT's systematic approach to innovation through ecosystems and stakeholders

Dr Phil Budden

MIT School of Management

Here East, London: 14 November 2019

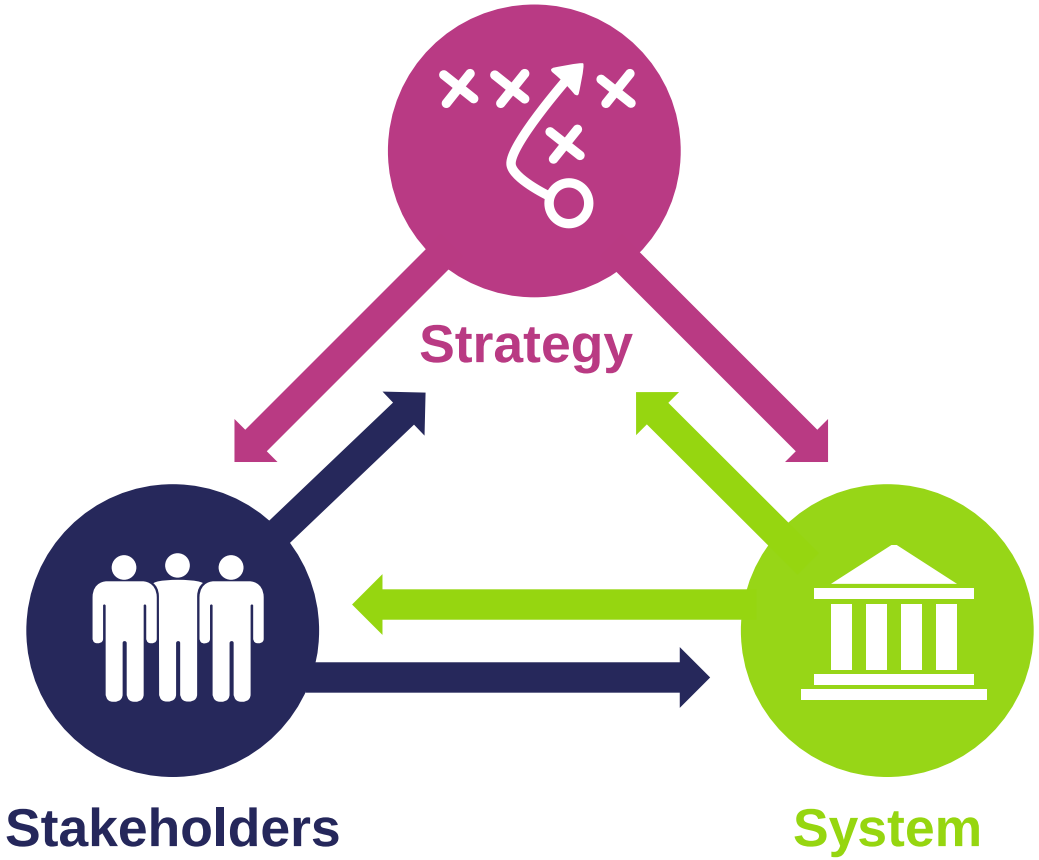

The World Is Flat
A BRIEF HISTORY OF
THE TWENTY-FIRST CENTURY
Thomas L. Friedman

In the new global innovation economy, the world is NOT flat…..

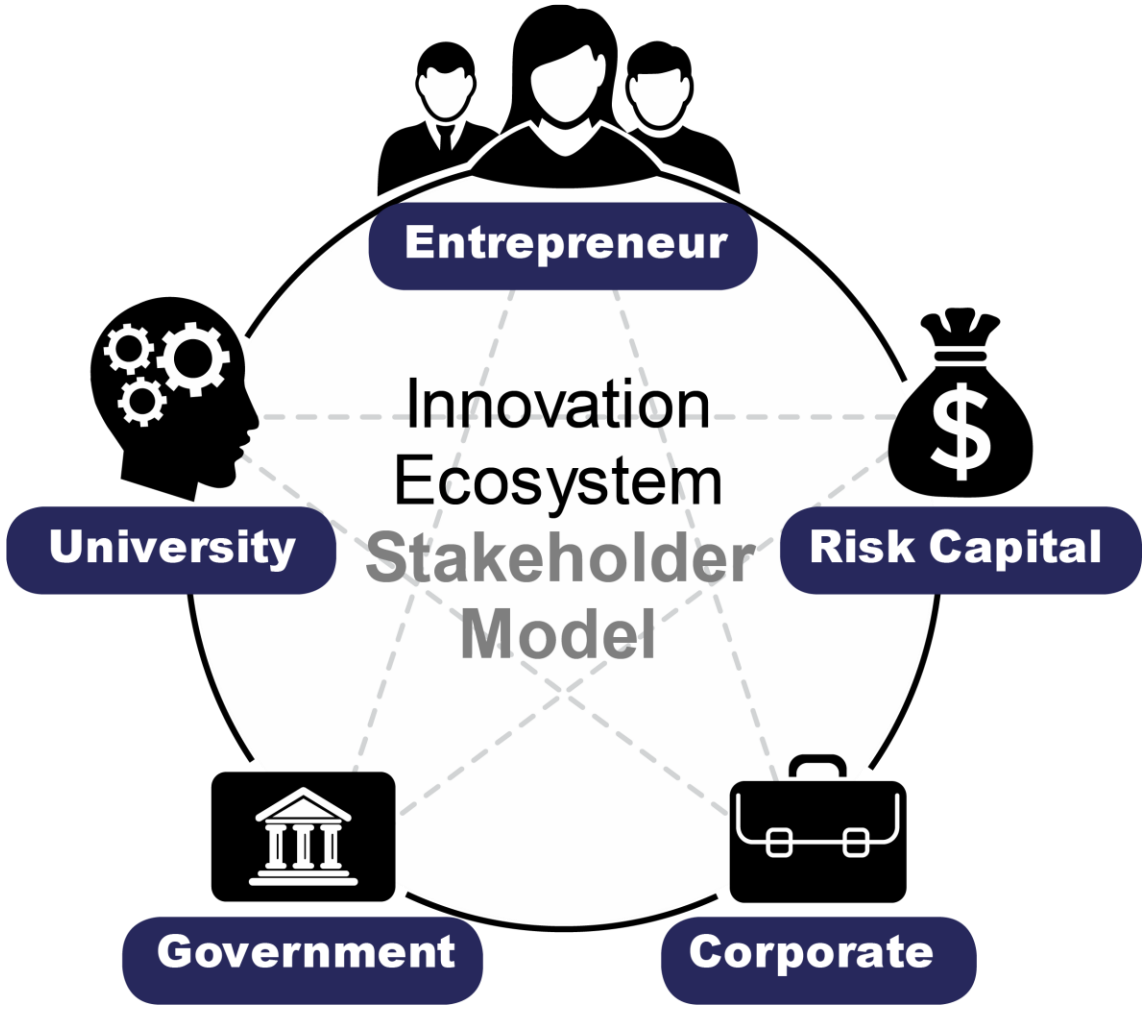
…a growing number of innovation ecosystems with unique comparative advantage that can support such entrepreneurship across sectors…

…and this seems true of cyber/digital security too.

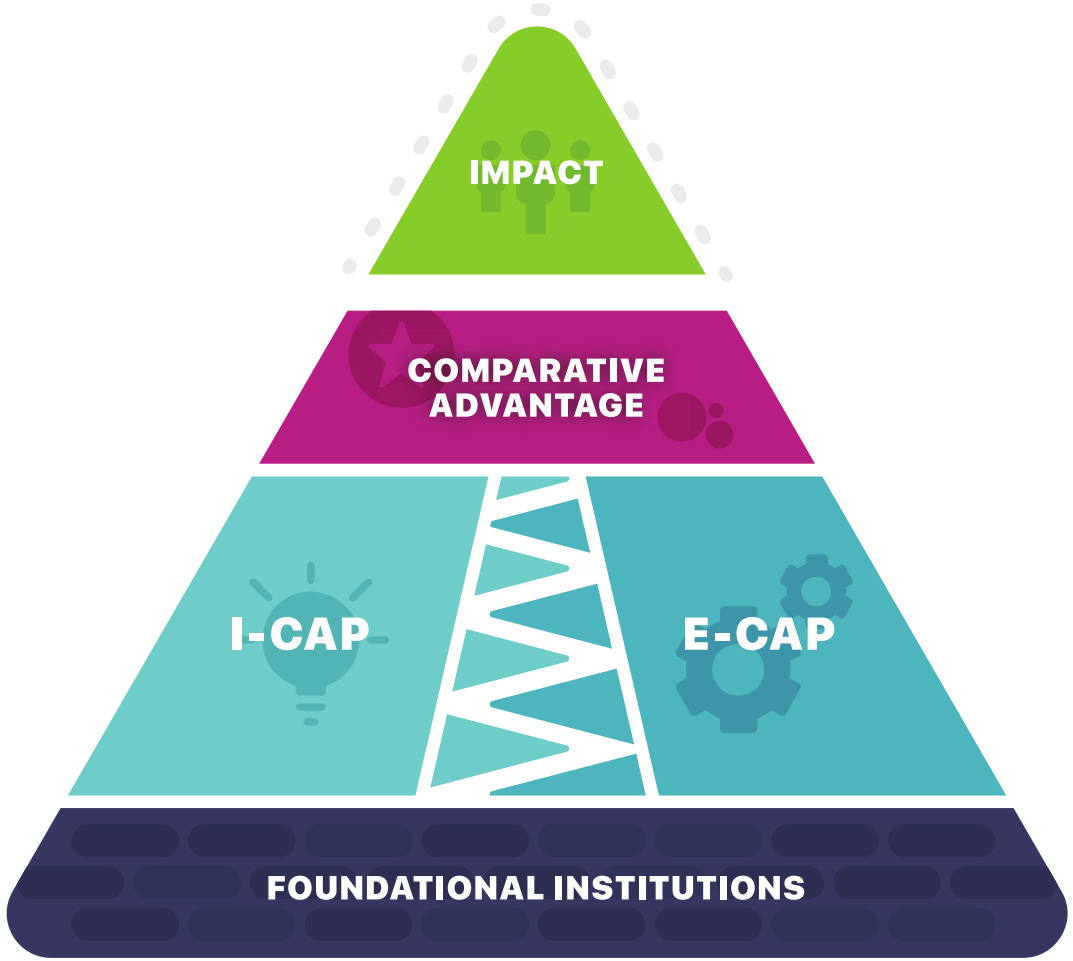
MIT's approach to Innovation Ecosystems



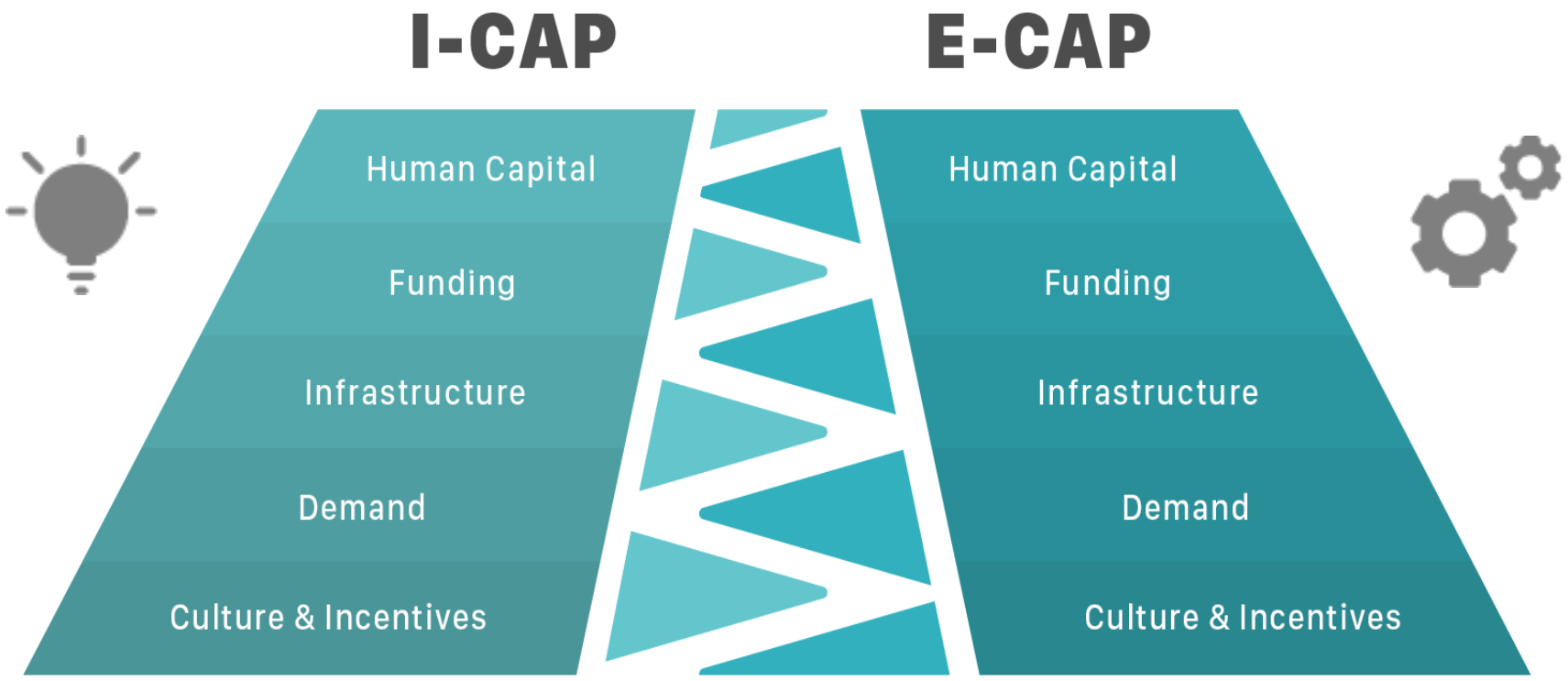
MIT's iEcosystem approach recognizes engagement with multiple Stakeholders (not just those in the 'triple helix')



In MIT's Innovation Ecosystem model, we outline this 'System'



Each Capacity has 5 input categories, combining for ‘innovation-driven entrepreneurship’

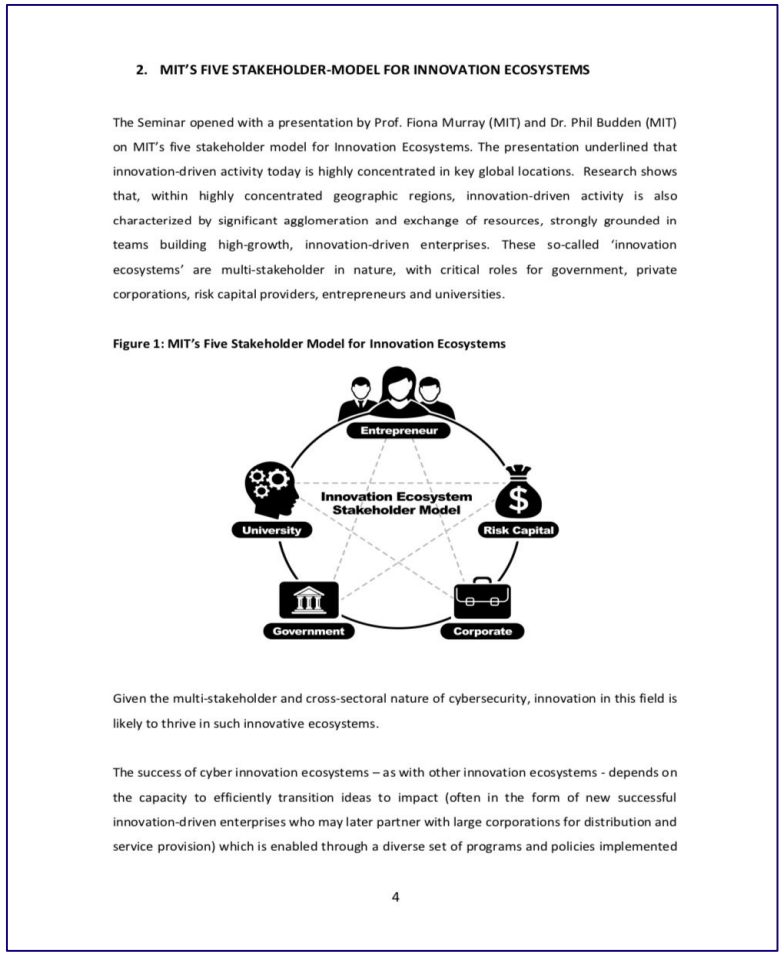


https://innovation.mit.edu/assets/Assessing-iEcosystems-V2-Final.pdf

Leaders only then choose a Strategy for change (eg to enhance digital security innovation)

Designing programmatic/policy interventions (PPIs) based on a region's comparative advantage(s)

MIT hosted Workshop: 'Enhancing Cybersecurity: the Role of Innovation Ecosystems' in April 2019



2. MIT'S FIVE STAKEHOLDER-MODEL FOR INNOVATION ECOSYSTEMS

The Seminar opened with a presentation by Prof. Fiona Murray (MIT) and Dr. Phil Budden (MIT) on MIT's five stakeholder model for Innovation Ecosystems. The presentation underlined that innovation-driven activity today is highly concentrated in key global locations. Research shows that, within highly concentrated geographic regions, innovation-driven activity is also characterized by significant agglomeration and exchange of resources, strongly grounded in teams building high-growth, innovation-driven enterprises. These so-called 'innovation ecosystems' are multi-stakeholder in nature, with critical roles for government, private corporations, risk capital providers, entrepreneurs and universities.

Figure 1: MIT's Five Stakeholder Model for Innovation Ecosystems

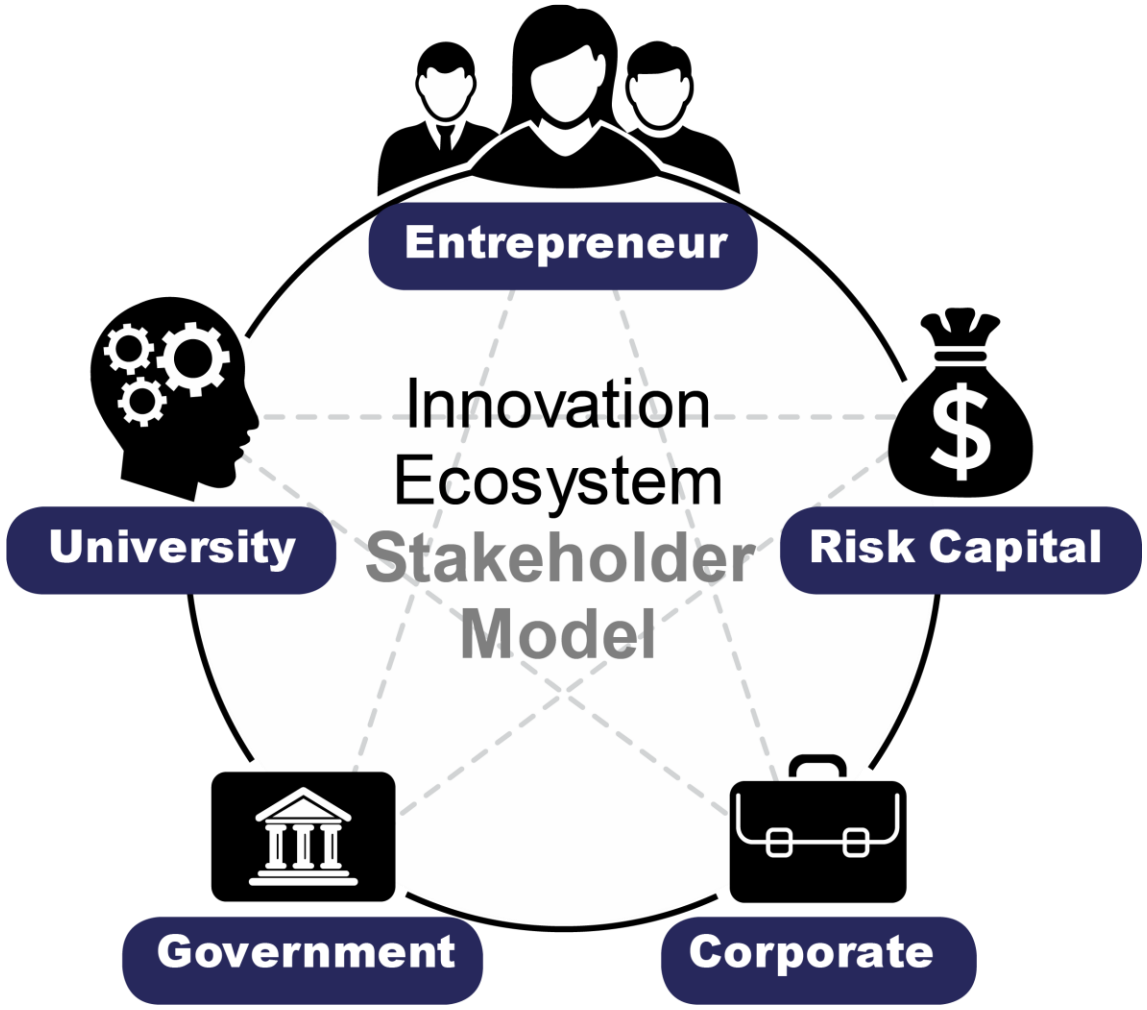
Given the multi-stakeholder and cross-sectoral nature of cybersecurity, innovation in this field is likely to thrive in such innovative ecosystems.

The success of cyber innovation ecosystems – as with other innovation ecosystems - depends on the capacity to efficiently transition ideas to impact (often in the form of new successful innovation-driven enterprises who may later partner with large corporations for distribution and service provision) which is enabled through a diverse set of programs and policies implemented

4

https://innovation.mit.edu/assets/Enhancing-Cybersecurity-The-Role-of-Innovation-Ecosystems.pdf

Given MIT's ecosystem approach to innovation, what is it that the different Stakeholders need for cyber/digital innovation?



On to the first Session of the Panel…

pbudden@mit.edu

GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

Second Annual Event

Encouraging Digital Security Innovation

TÜV SÜD

OECD

BETTER POLICIES FOR BETTER LIVES