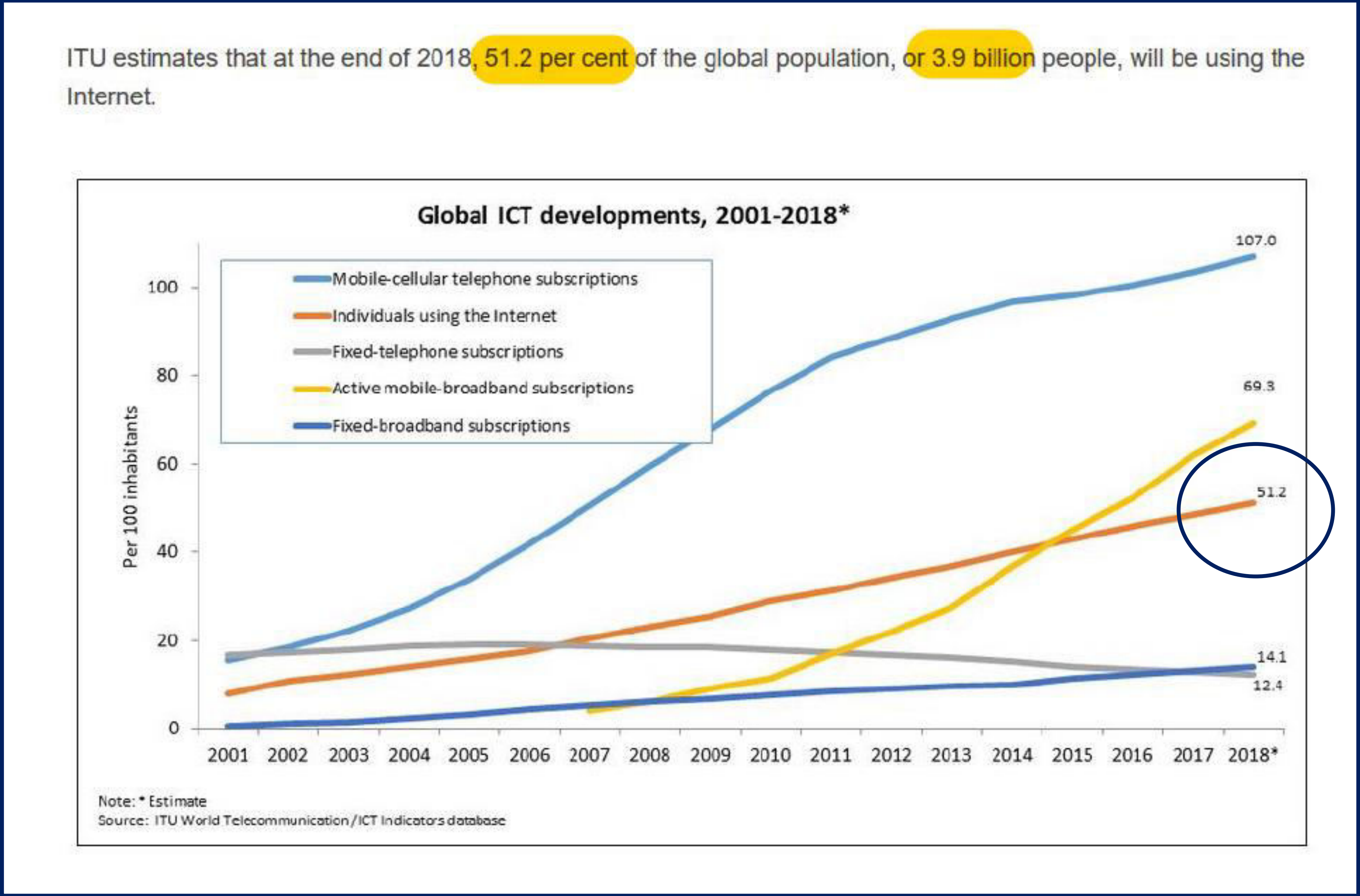
WORLD BANK GROUP

CAPACITY BUILDING FOR CYBERSECURITY

Deborah Housen-Couriel, Adv.

December 13, 2018



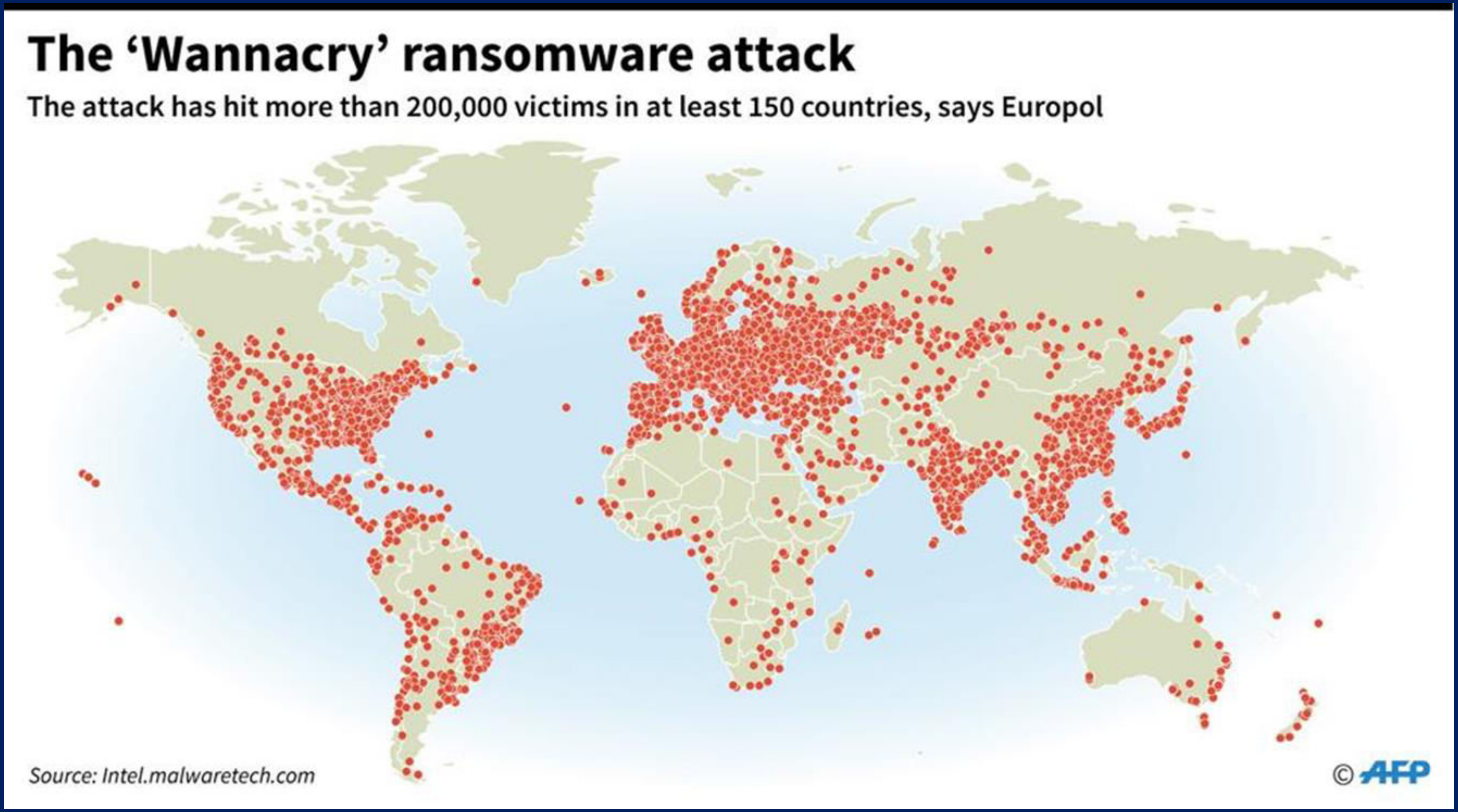
ITU estimates that at the end of 2018, 51.2 per cent of the global population, or 3.9 billion people, will be using the Internet.

Global ICT developments, 2001-2018*

Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

ADVANTAGES + VULNERABILITIES > REQUIRE CAPACITY BUILDING

WANNACRY – May 12-13, 2017



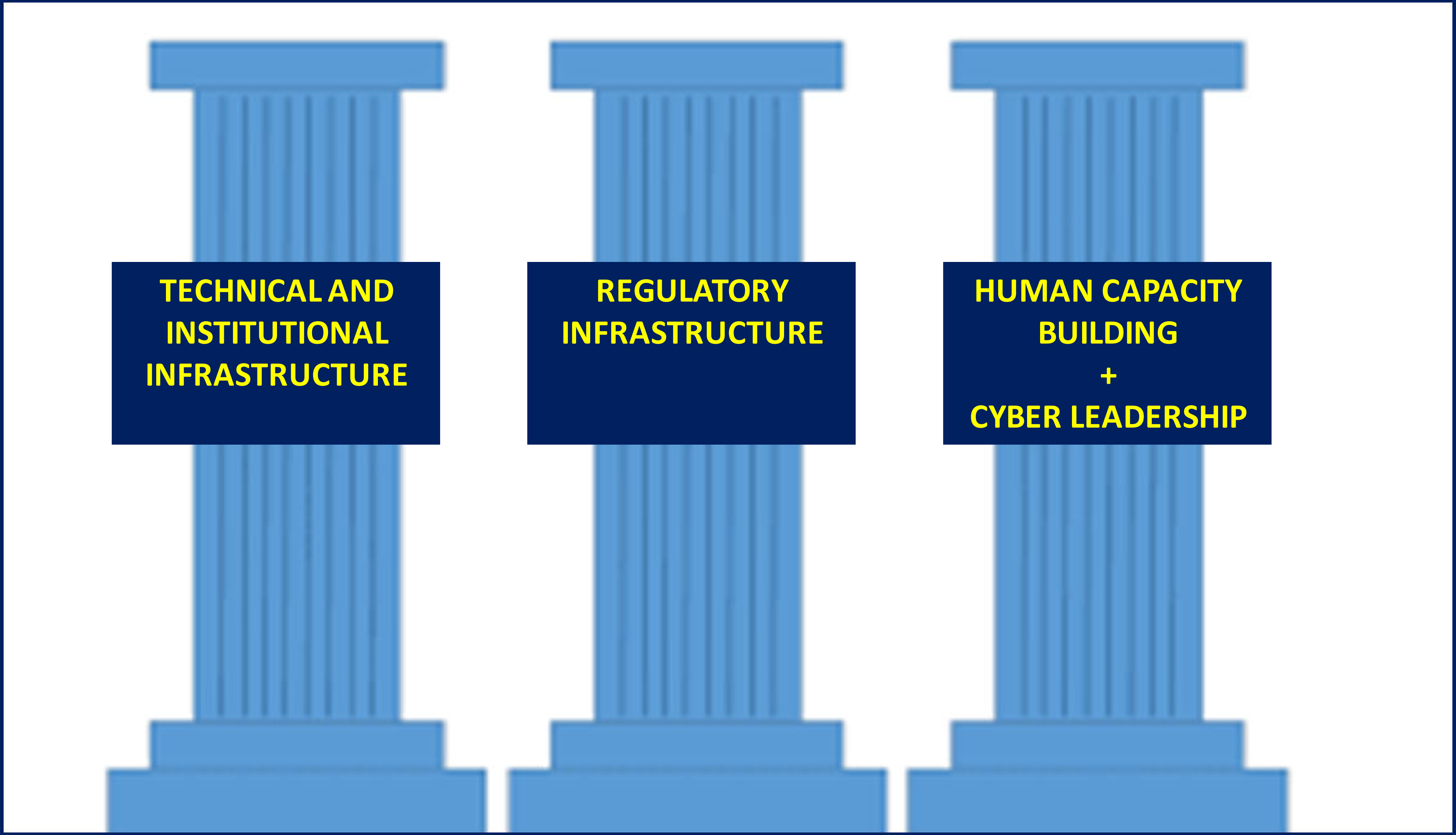
The ‘Wannacry’ ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

Source: Intel.malwaretech.com

© AFP

CAPACITY BUILDING



TECHNICAL AND INSTITUTIONAL INFRASTRUCTURE

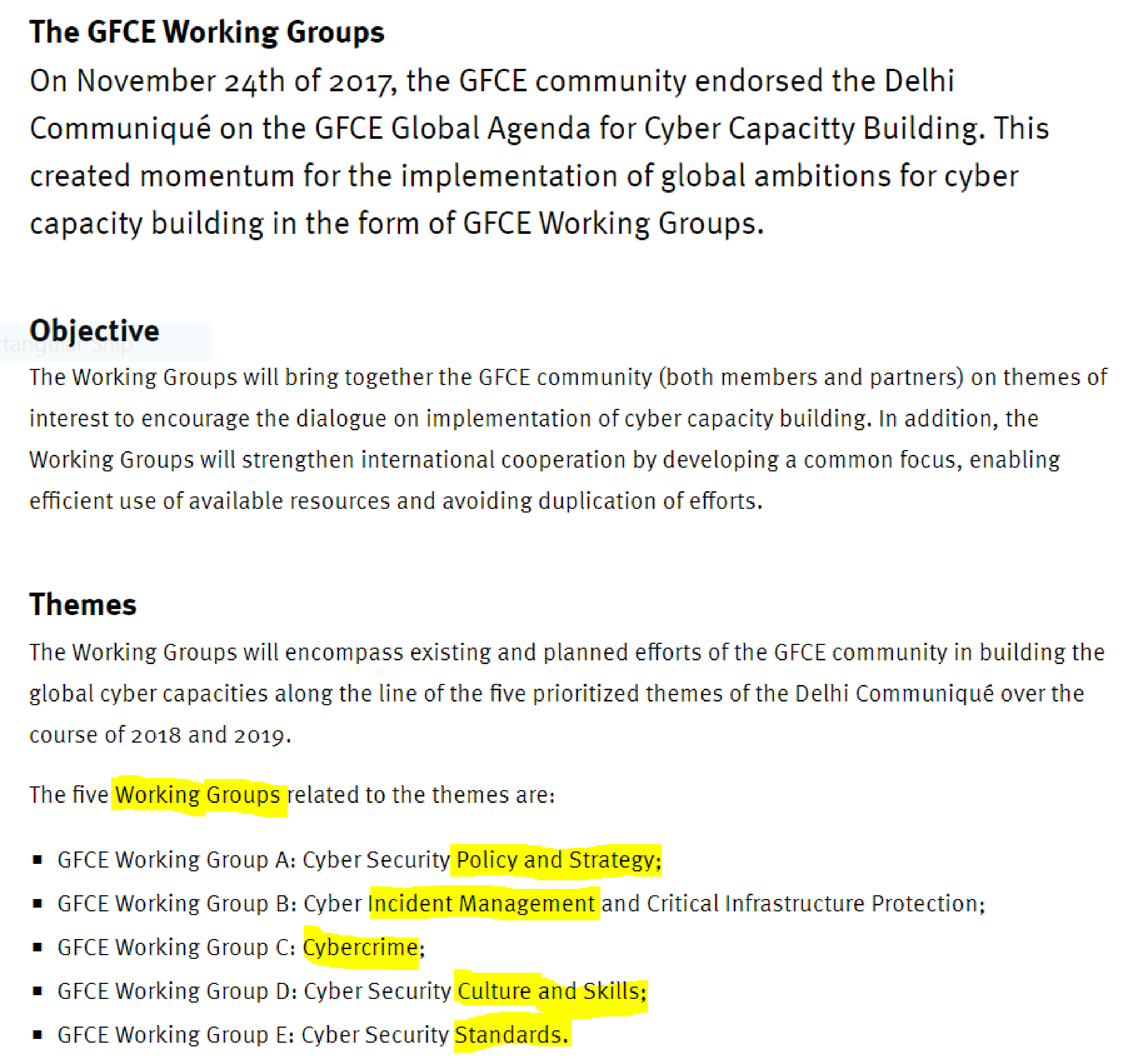
REGULATORY INFRASTRUCTURE

HUMAN CAPACITY BUILDING
+
CYBER LEADERSHIP

TECHNICAL AND INSTITUTIONAL INFRASTRUCTURE

GFCE

Global Forum on Cyber Expertise



The GFCE Working Groups

On November 24th of 2017, the GFCE community endorsed the Delhi Communiqué on the GFCE Global Agenda for Cyber Capacitty Building. This created momentum for the implementation of global ambitions for cyber capacity building in the form of GFCE Working Groups.

Objective

The Working Groups will bring together the GFCE community (both members and partners) on themes of interest to encourage the dialogue on implementation of cyber capacity building. In addition, the Working Groups will strengthen international cooperation by developing a common focus, enabling efficient use of available resources and avoiding duplication of efforts.

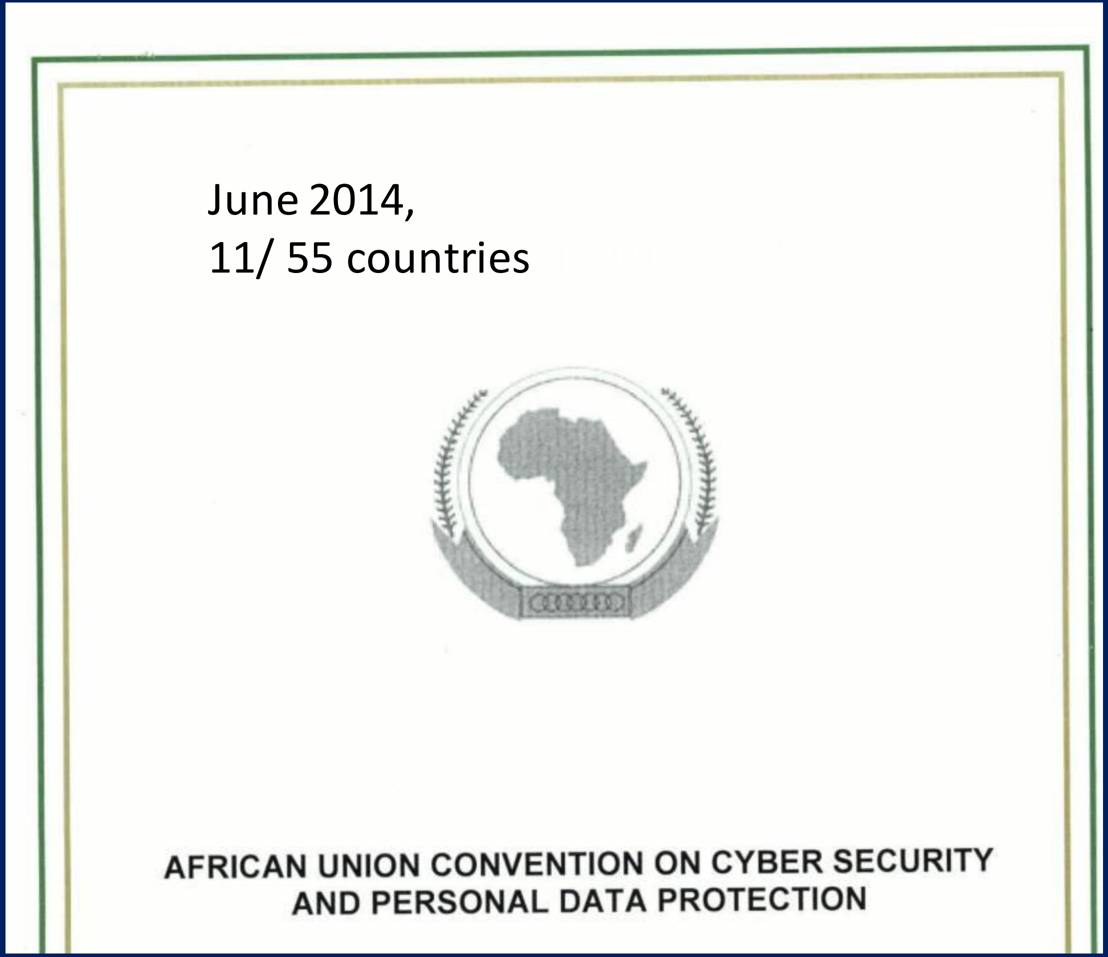
Themes

The Working Groups will encompass existing and planned efforts of the GFCE community in building the global cyber capacities along the line of the five prioritized themes of the Delhi Communiqué over the course of 2018 and 2019.

The five Working Groups related to the themes are:

- GFCE Working Group A: Cyber Security Policy and Strategy;
- GFCE Working Group B: Cyber Incident Management and Critical Infrastructure Protection;
- GFCE Working Group C: Cybercrime;
- GFCE Working Group D: Cyber Security Culture and Skills;
- GFCE Working Group E: Cyber Security Standards.

REGULATORY INFRASTRUCTURE



June 2014,
11/ 55 countries

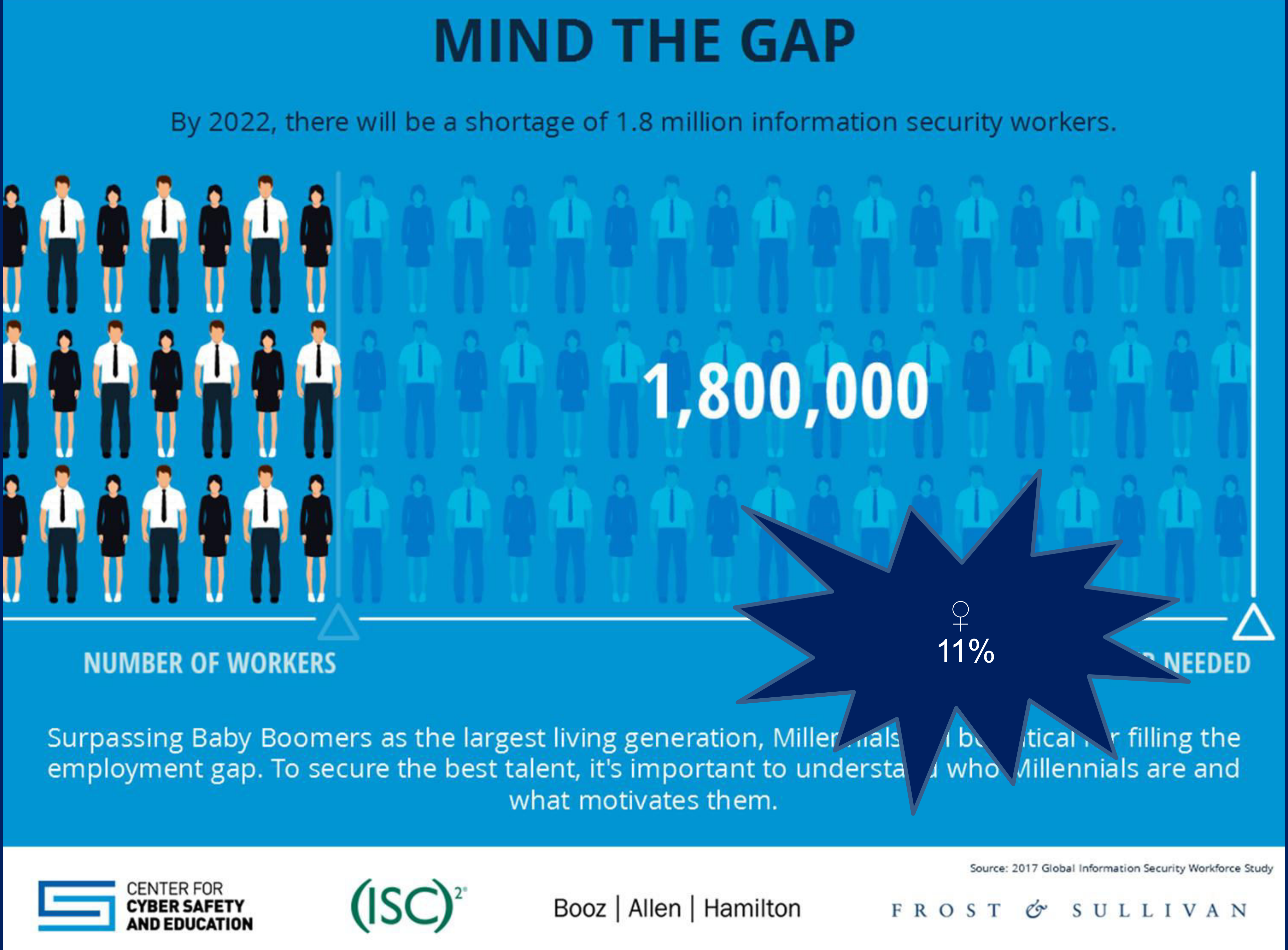
AFRICAN UNION CONVENTION ON CYBER SECURITY
AND PERSONAL DATA PROTECTION

- **National strategies – critical**

- **Adapting laws to new cyber realities**
  - **Contract law**
  - **Criminal law**
  - **Damages**

- **Engaging the private sector**
  - **Licensing**
  - **Critical infrastructure protections**

PEOPLE AND CYBER LEADERSHIP



MIND THE GAP

By 2022, there will be a shortage of 1.8 million information security workers.

1,800,000

NUMBER OF WORKERS

NEEDED

♀
11%

Surpassing Baby Boomers as the largest living generation, Miller ials l b tical r filling the employment gap. To secure the best talent, it's important to understa d who Millennials are and what motivates them.

Source: 2017 Global Information Security Workforce Study

CENTER FOR CYBER SAFETY AND EDUCATION

(ISC)²

Booz | Allen | Hamilton

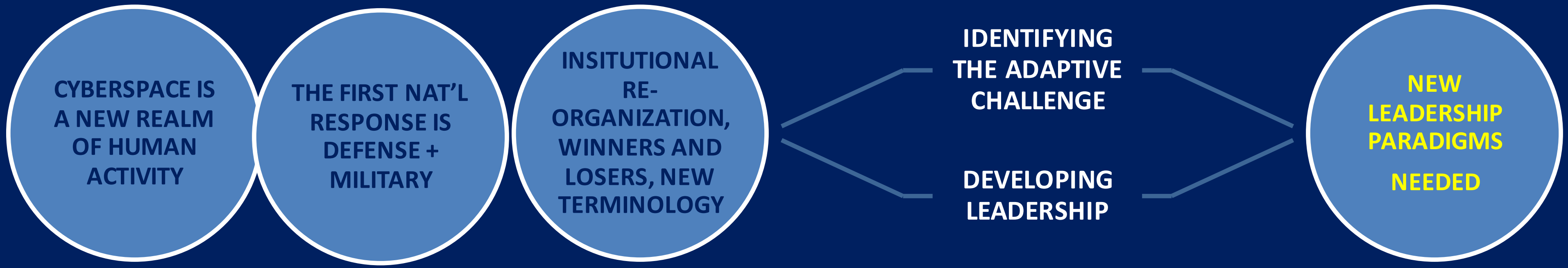
FROST & SULLIVAN

We’ve entered a new era, and we lack the shared vocabulary and political doctrines to make sense of it.

Perhaps more importantly, the generation of leaders who can seamlessly integrate policies in the physical and digital worlds is still emerging.

- William Burns, President of the Carnegie Foundation, February 2017

AN ADAPTIVE CHALLENGE



CYBERSPACE IS A NEW REALM OF HUMAN ACTIVITY

THE FIRST NAT'L RESPONSE IS DEFENSE + MILITARY

INSITUTIONAL RE-ORGANIZATION, WINNERS AND LOSERS, NEW TERMINOLOGY

IDENTIFYING THE ADAPTIVE CHALLENGE

DEVELOPING LEADERSHIP

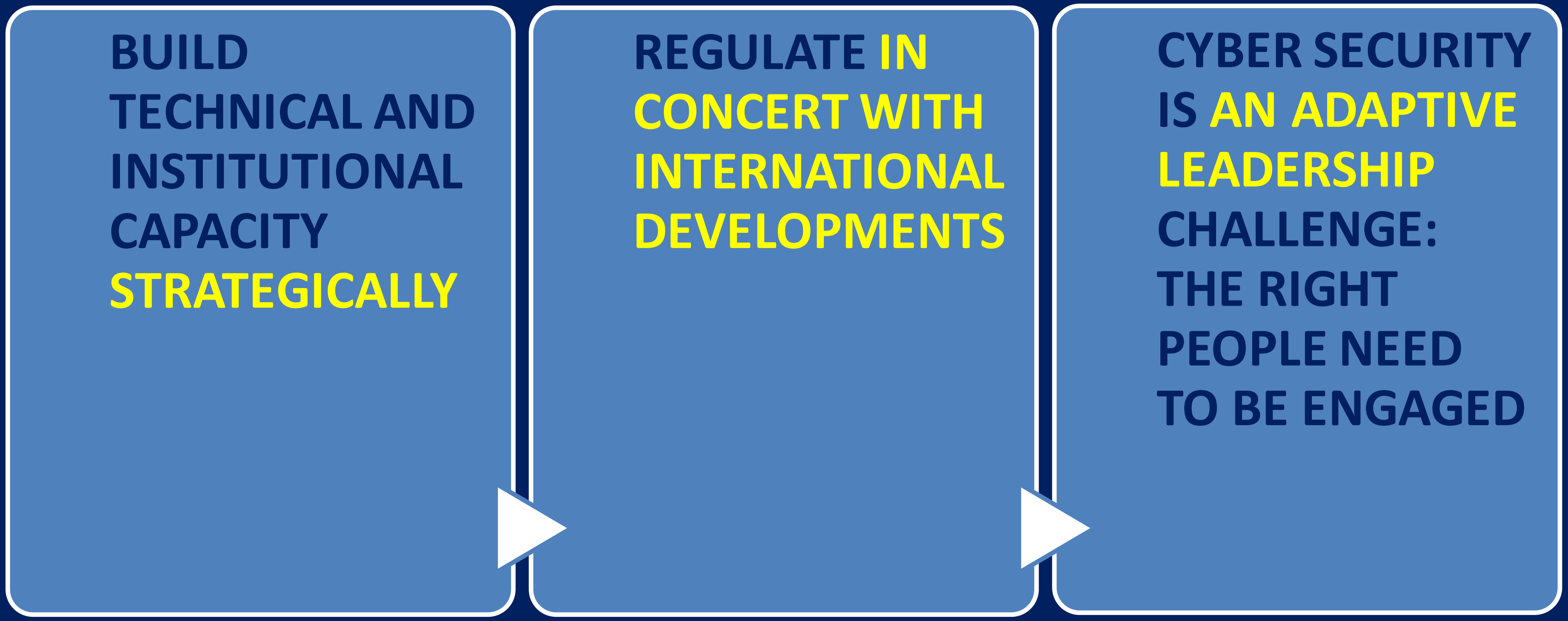
NEW LEADERSHIP PARADIGMS

NEEDED

THE ADAPTIVE CHALLENGE BECOMES CLEAR AS TACTICAL RESPONSES FAIL

- Cybercrime costs rise globally
- Extent of hostile cyber activity broadens and quickens
- Internet governance remains an unruly issue
- New targets: electoral systems, critical infrastructure
- Collective security?

WRAPPING UP: SOME INSIGHTS



BUILD TECHNICAL AND INSTITUTIONAL CAPACITY **STRATEGICALLY**

REGULATE **IN CONCERT WITH INTERNATIONAL DEVELOPMENTS**

CYBER SECURITY IS **AN ADAPTIVE LEADERSHIP** CHALLENGE: THE RIGHT PEOPLE NEED TO BE ENGAGED

THANK YOU.

Deb Housen-Couriel, Adv.