DICT

NATIONAL CYBERSECURITY PLAN 2022

#CYBERRESILIENTPH

CONTENTS

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

CONTENTS

4 Key Strategic Imperatives

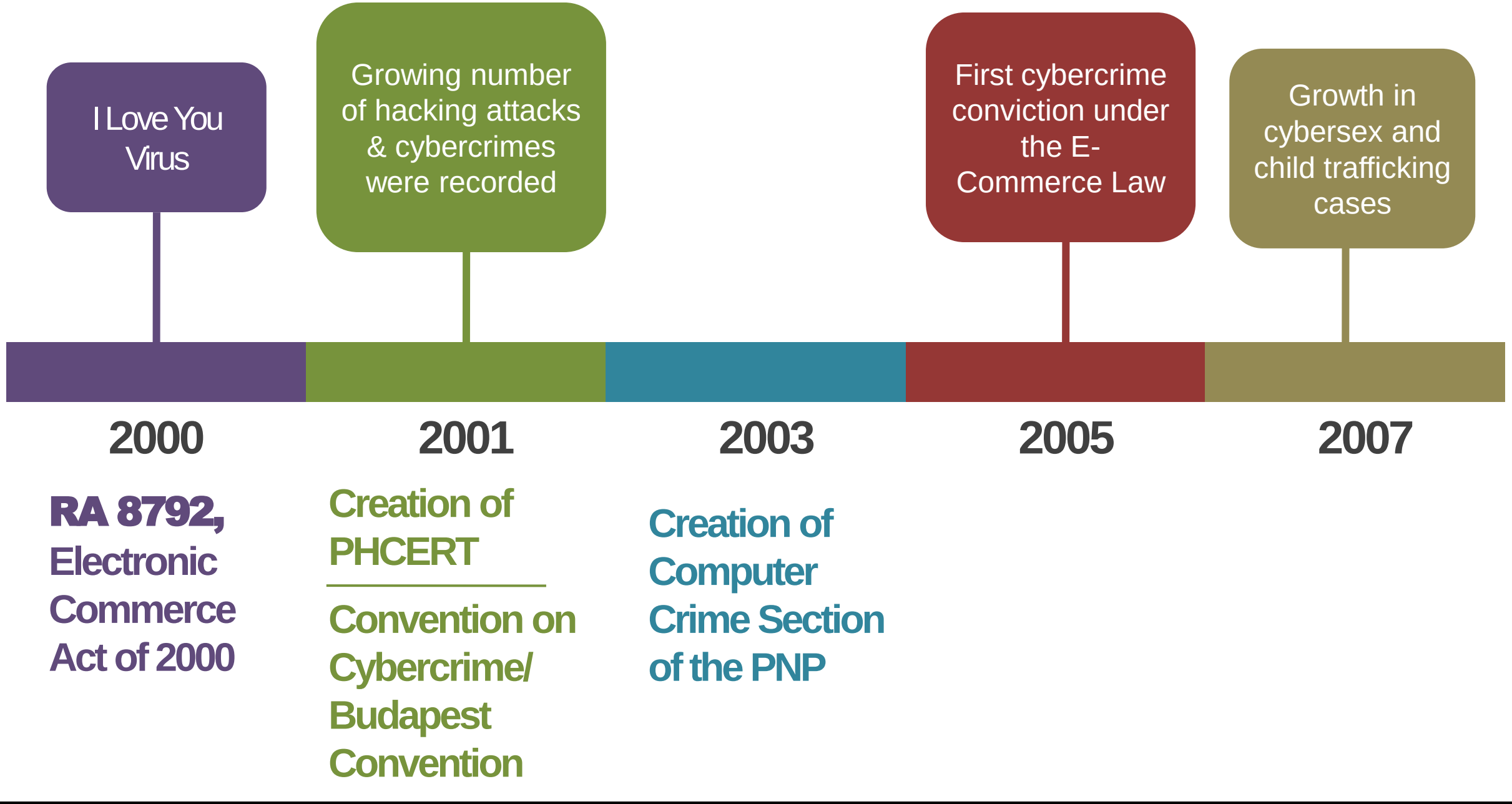
- Enhance Security and Resilience of CII and government public and military networks to deal with sophisticated attacks
- Increase efforts to promote adoption of Cybersecurity measures among individuals and businesses
- Grow Pool of CyberSecurity Experts

5 Strategic Collaboration

- National Level Committee
- Public-Private Partnership
- International Collaborations

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY


History of
CYBERSECURITY
in the Philippines



HISTORY OF CYBERSECURITY IN THE PHILIPPINES

DOJ Reported that 9 out of 10 Filipinos are victims of various forms of cybercrime ranging from hacking attacks to online scams

Election Breach

Bank Heist

2009

RA 9775, Anti-Child Pornography Act of 2009

RA 9995, Anti-Photo and Video Voyeurism Act of 2009

2012

RA 10175, Cybercrime Prevention Act of 2012

RA 10173, Data Privacy Act of 2012

2014

RA 10175 suspension lifted

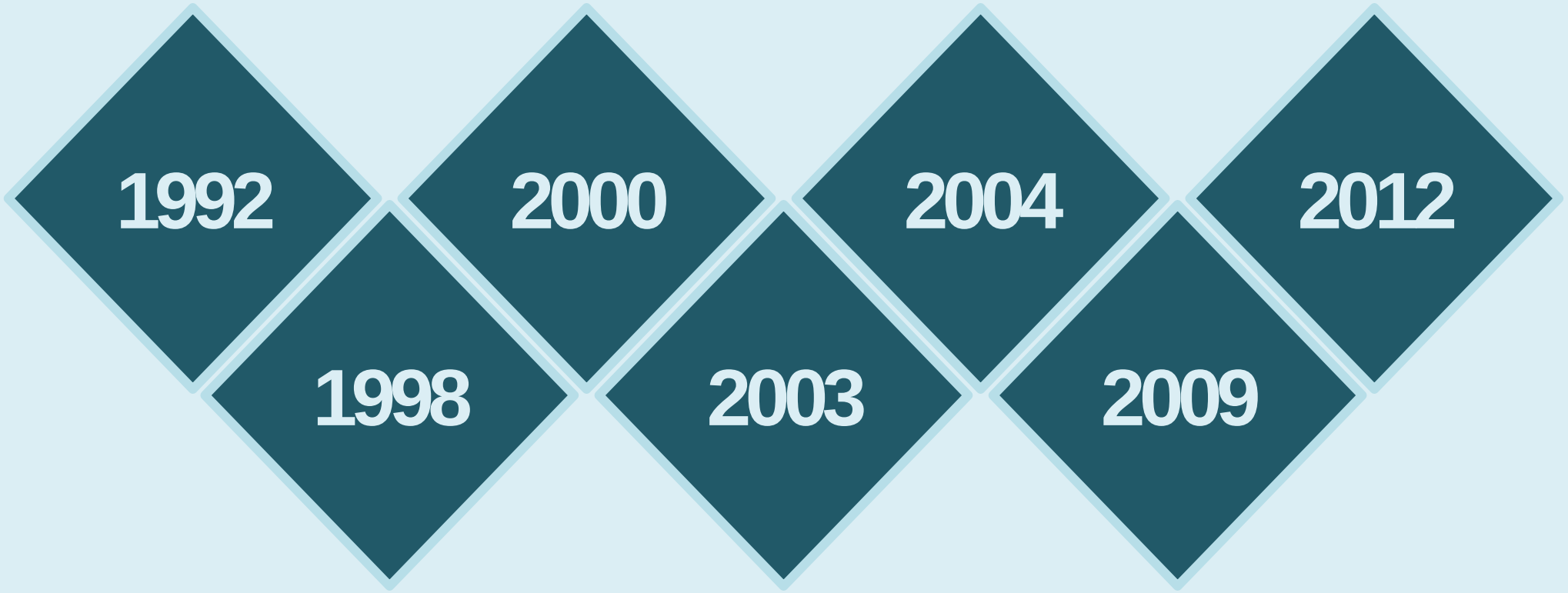
2015

EO 189 s. 2015, Creating the National Cybersecurity Inter-Agency Committee

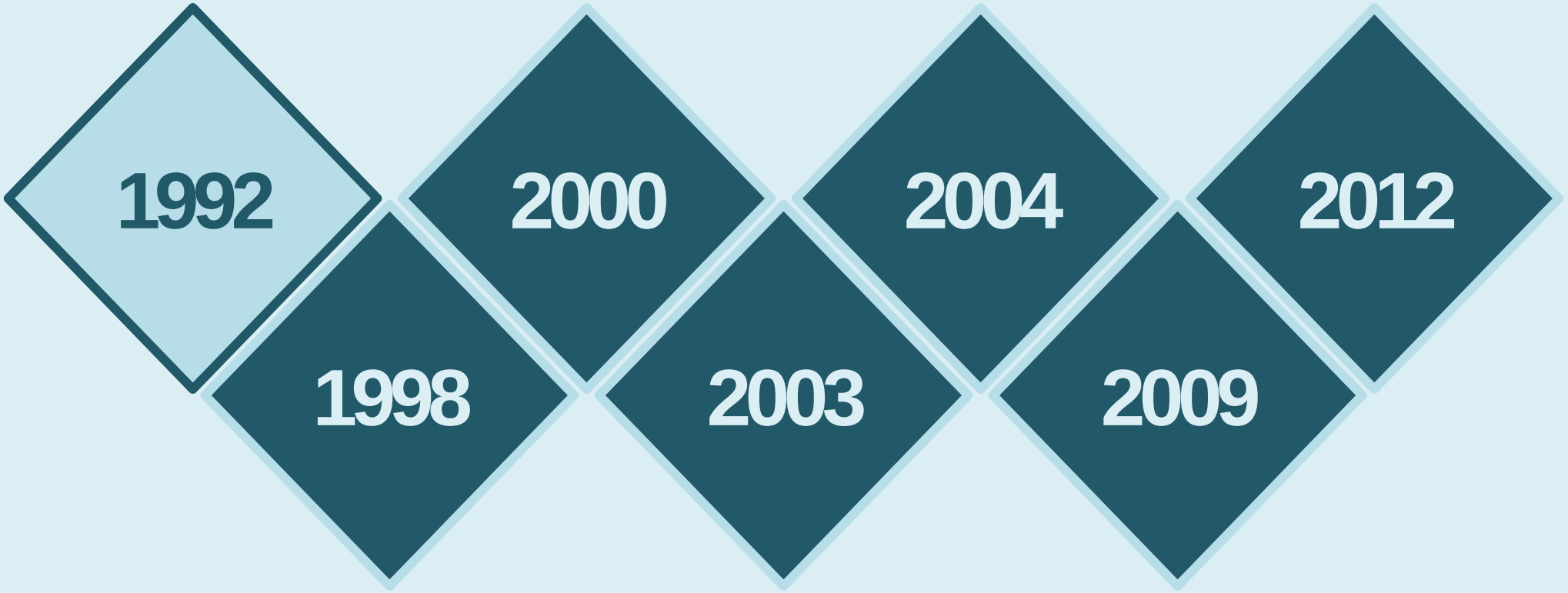
2016

RA 10844, Department of Information and Communications Technology Act

HISTORY OF CYBERSECURITY IN THE PHILIPPINES

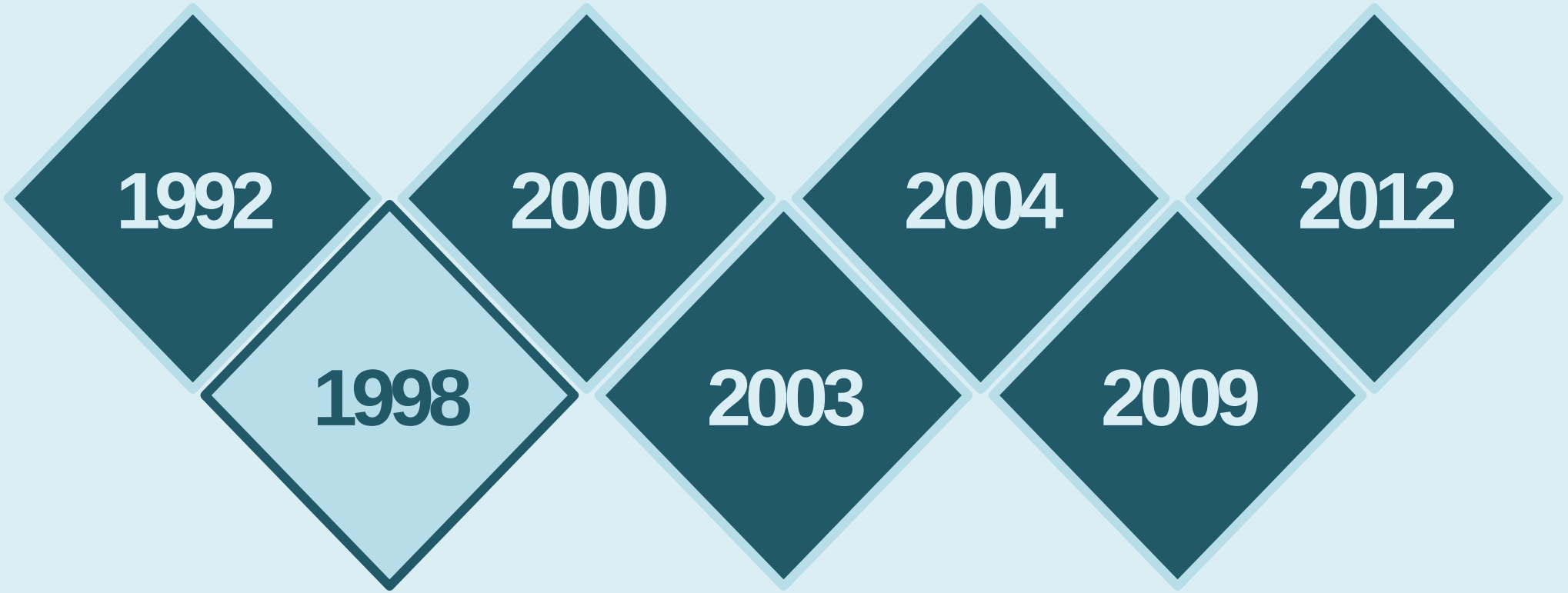


Laws enacted that are technology-related



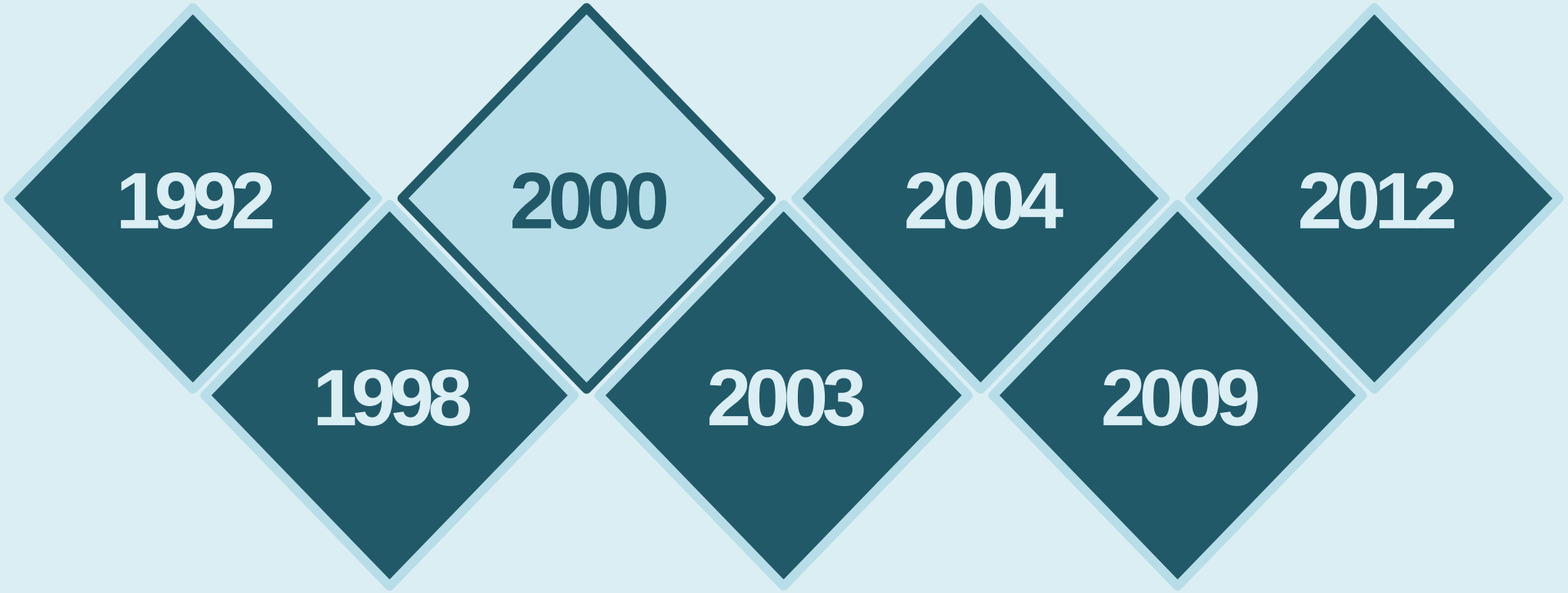
RA 7610

Special Protection of Children against Abuse Act



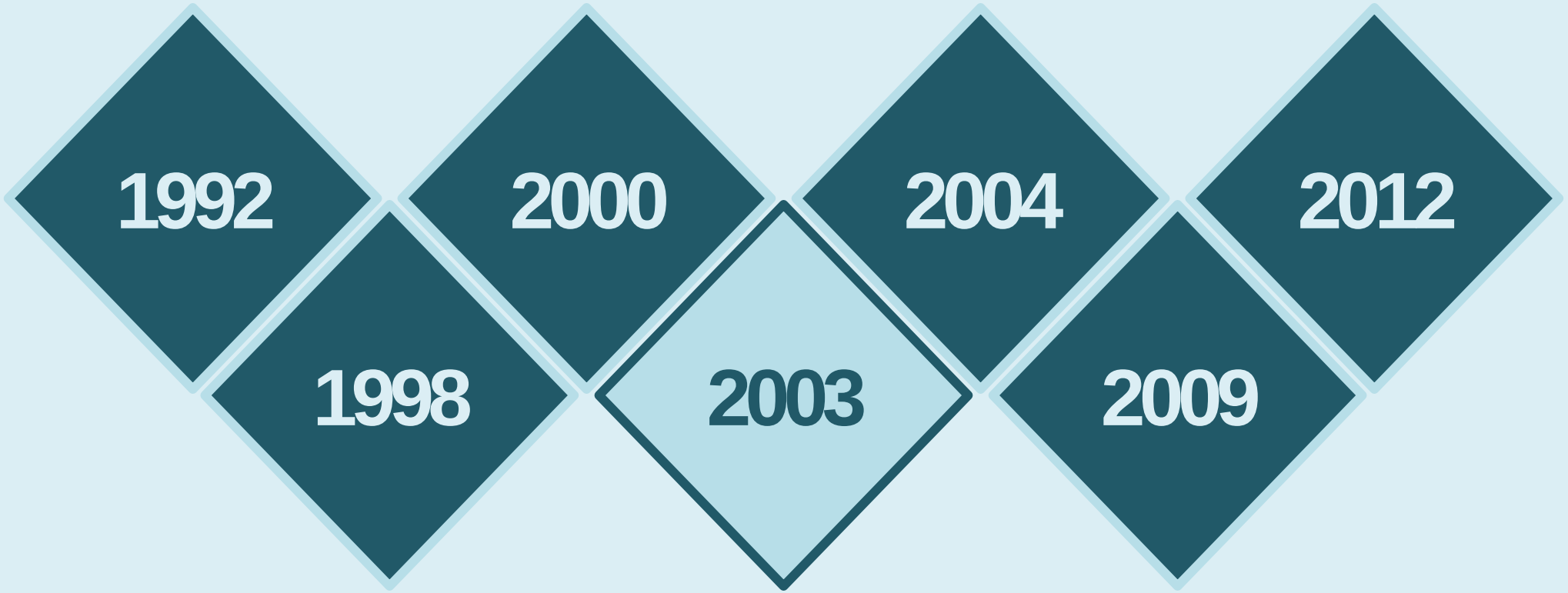
RA 8484

Access Devices Regulation Act



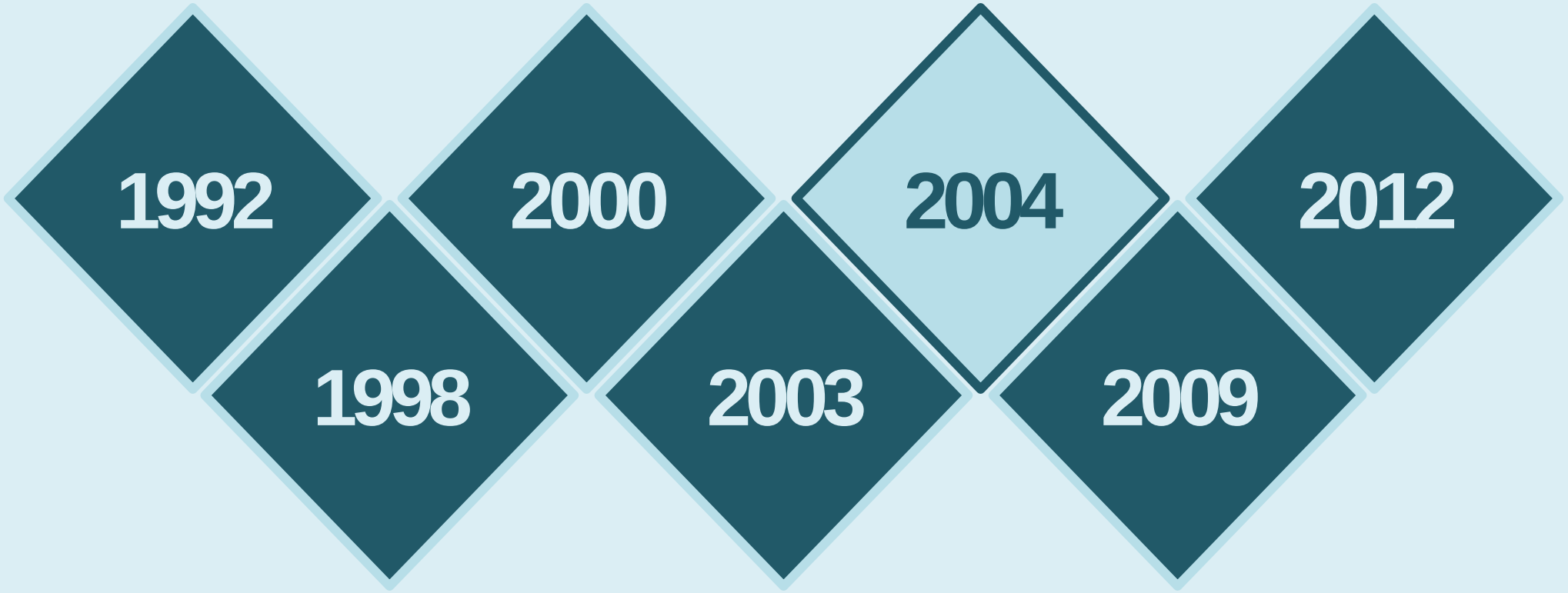
RA 8792

Electronic Commerce Act



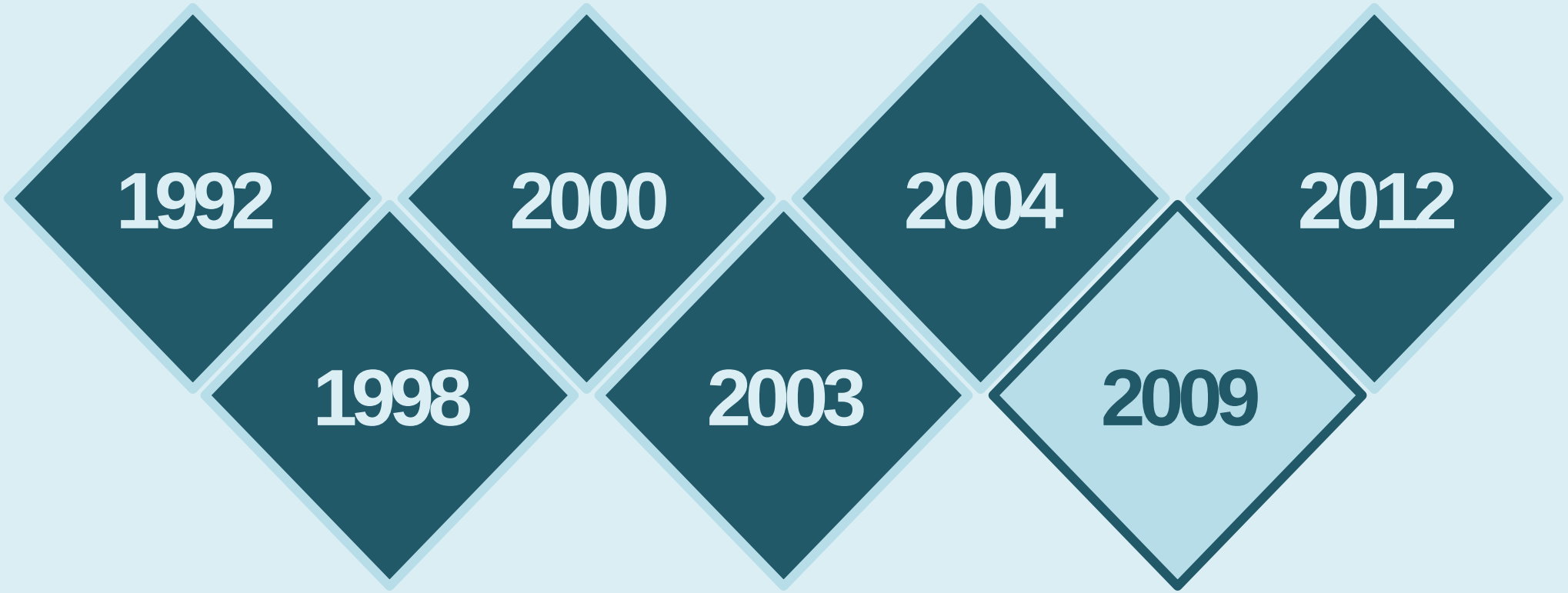
RA 9208

Anti-Trafficking Act



RA 9262

Anti-Violence against Women and Children Act

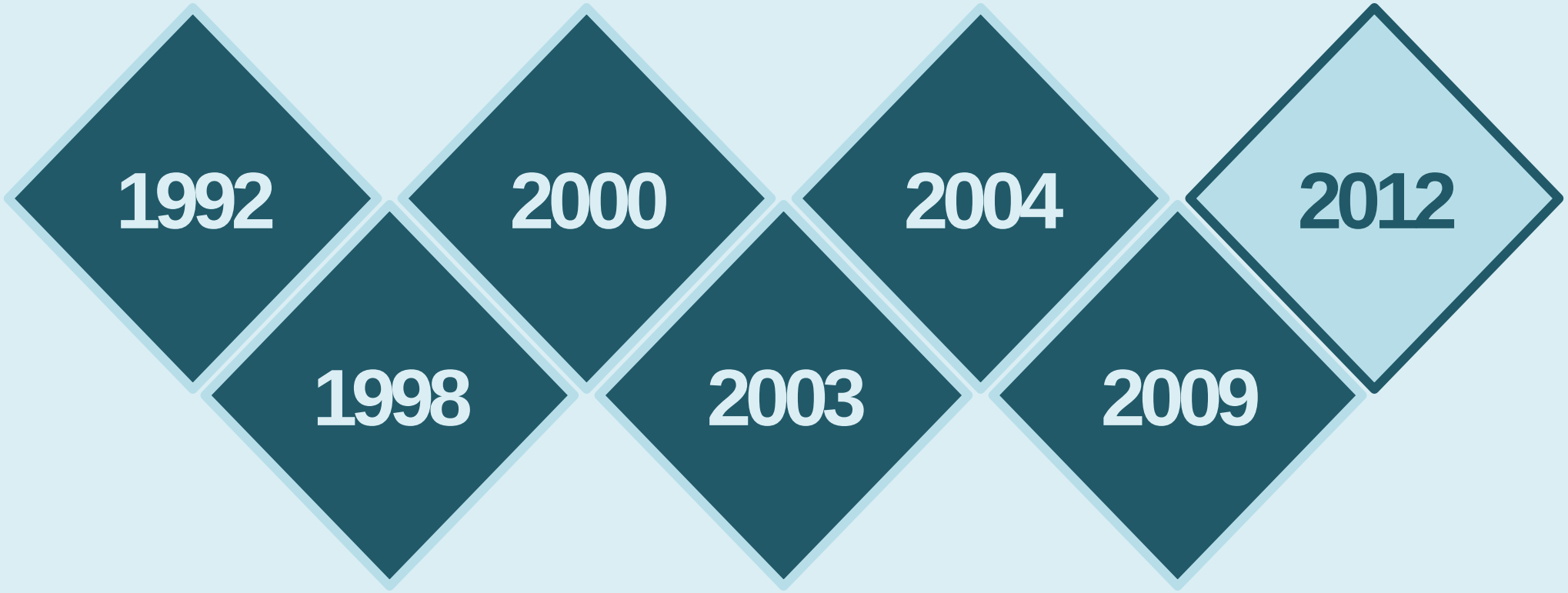


RA 9775

Anti-Child Pornography Act

RA 9995

Anti-Photo and Video Voyeurism



RA 10173

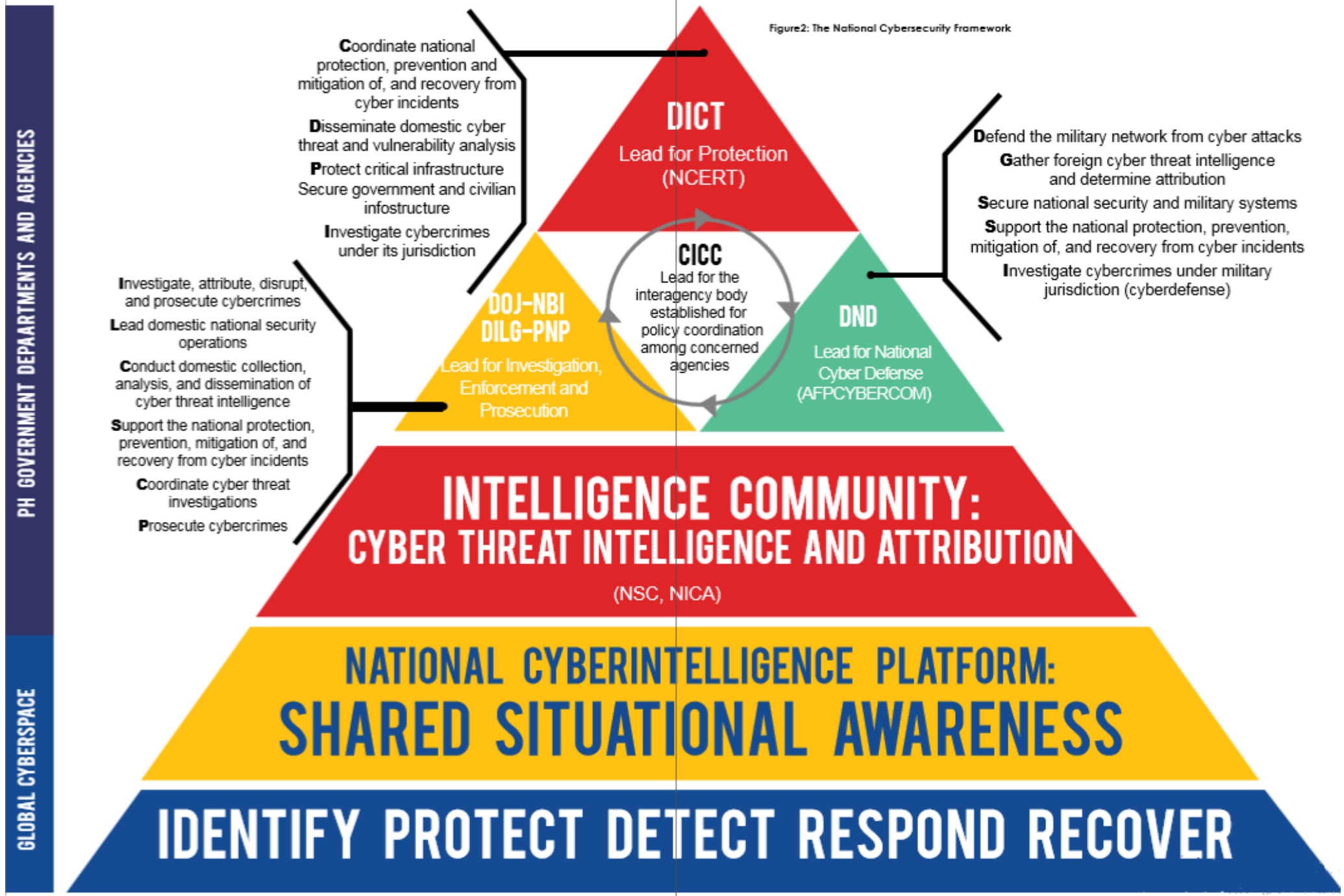
Data Privacy Act

RA 10175

Cybercrime Prevention Act

The National CYBER SECURITY GOVERNANCE FRAMEWORK

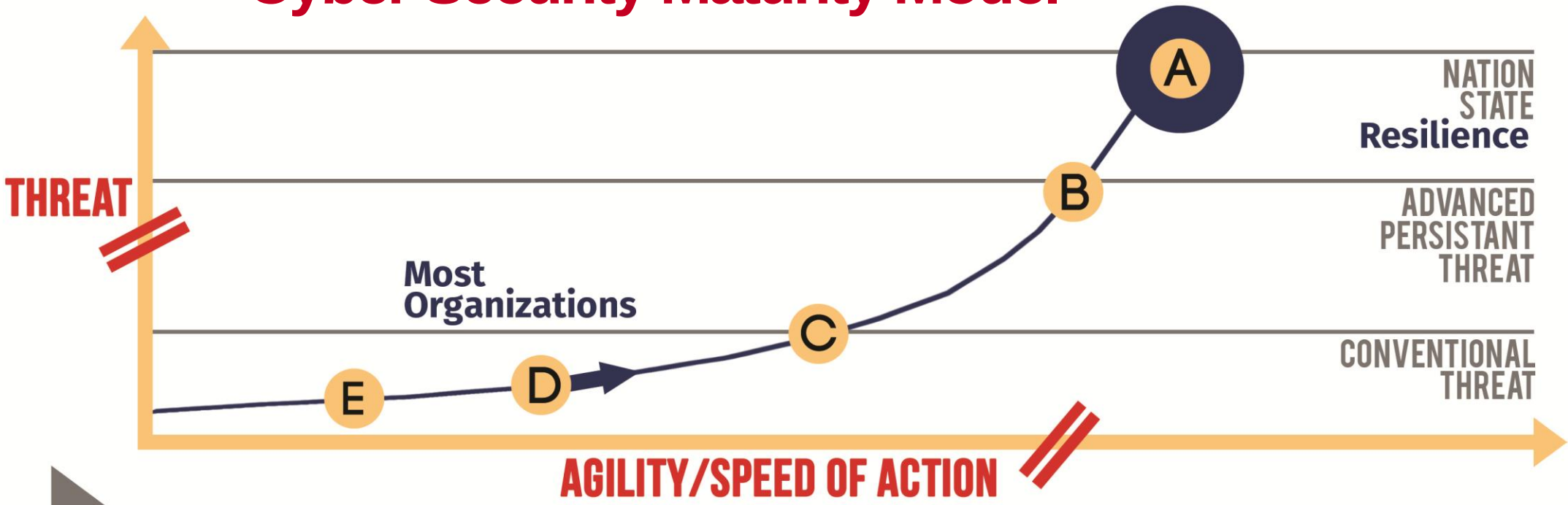
Figure2: The National Cybersecurity Framework



CyberSecurity in the Philippines should be divided according to its major **CyberSecurity Responsibilities:** Law Enforcement, Protection and National Defense

Community	Agency/ Organization	Emphasis
Law Enforcement	**DOJ-NBI** **DILG-PNP**	Identify Criminals Preserve Evidence Prosecute
Network Protection	**DICT** **CICC**	Disseminate Broadly Ensure Timely Release
National Defense	**DND / AFP** **NSC**	Defend the Country Protect Military Networks
Intelligence Community	**NICA**	Attribution Advise and Inform Decision Makers

Cyber Security Maturity Model



E

REACTIVE & MANUAL

People based following doctrine and doing there best to "put out fires"

D

TOOLS-BASED

Applying tools and technologies piecemeal to assist people in reacting faster

C

INTEGRATED PICTURE

Loosely intergrated with focus on interoperability and standards-based data exchange for IA situational awareness

B

DYNAMIC DEFENSE

Predictive and agile, the enterprise instantiates policy, illuminates events, and helps the operators find, fix, and target for response

A

RESILIENT ENTERPRISE

Predictive and mission focused, isolates and contains damage, secure supply chains, and protext key critical infrastructures to operate through cyber attack

*Source: Presentation of **Robert Lentz** Former CISO US Department of Defense*

Cybersecurity STRATEGY

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Where are we now?

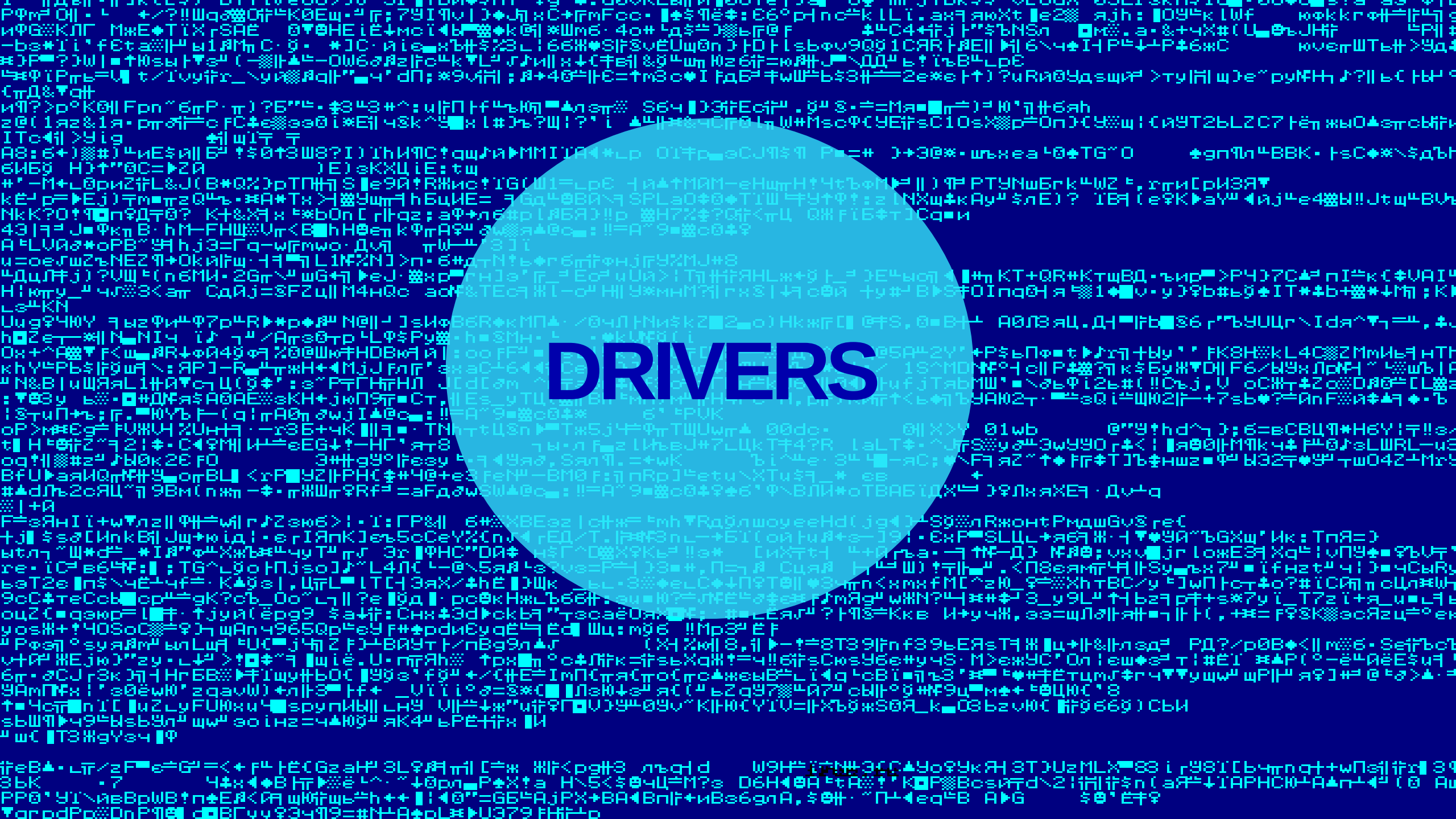
- Tools based
- Reactive / Manual

Cyber Resilient Philippines

What do we want to achieve?

How do we get there?

- Crafting of the National CyberSecurity Strategy, Policies, Plans and Programs
- Establishment of NCERT and Implementation of other Programs defined in the National Cybersecurity Plan


DRIVERS

Attacks to CII

Bank Heist, **N**avigation Systems Manipulation,
Control of Electronic Medical Equipment and Records,
Override of Oil and Gas Systems

Attacks to Government Infostructure

Hacking resulting in Data breach
Defacement of PH Government Agencies Websites

Sophistication of Cyber Attacks

APT, **D**DoS, **S**PAM, **S**pear Phishing,
Social Engineering


DICT
NATIONAL
CYBERSECURITY
PLAN 2022

National Targets:

#CyberToughPH

Making Government Information Environment Secure

#CyberResilientPH

Making Critical Infostructure (CII) Trusted and Secure

#CyberSafePH

Making Individuals Aware and Secure

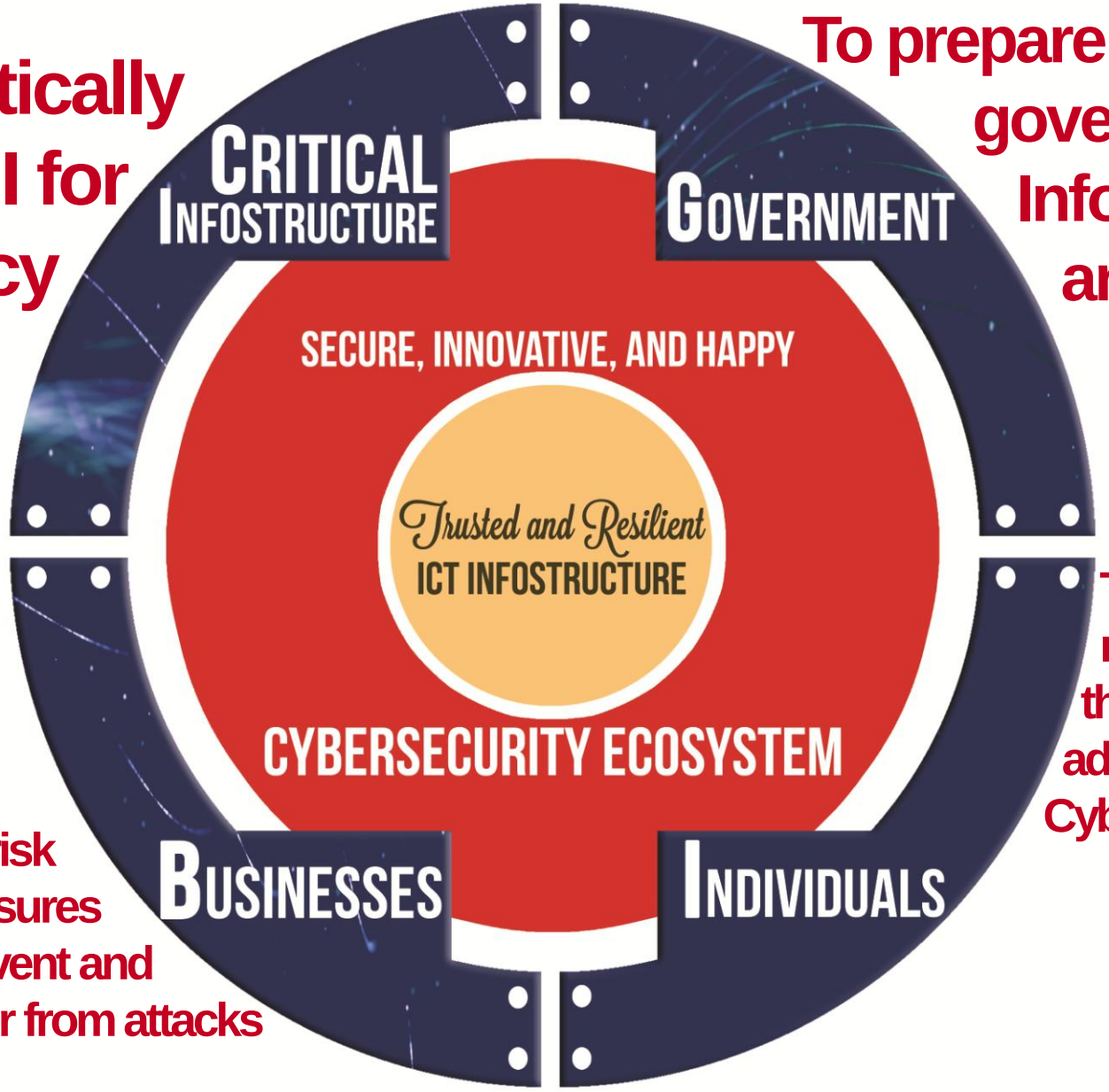
Making Businesses and Supply Chains more Secure

#CyberAssurancePH

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

To systematically harden CII for Resiliency

To prepare and secure government ICT Infostructure (Public and Military)



To raise awareness on cyber risks among users as they are the weakest links, they need to adopt the right norms in CyberSecurity

To raise awareness of cyber risk and use of security measures among businesses to prevent and protect, respond and recover from attacks

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Key
ENABLERS

Develop Cybersecurity Skills and Knowledge (Human Capital)	CYSO sa Departamento	Promote Cybersecurity Development in Industries
Nurture Cybersecurity Research & Development	Strengthen Cybersecurity Domestic and International Collaboration	Public and Private Partnership

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Key Strategic Imperatives

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Key Strategic Imperatives

Protection of Critical Infostructure (CII)

CyberSecurity Assessment and Compliance Programs

Public Networks thru establishment of CERTs

Military Networks thru establishment of Cyber Defense Centers (DND, NSC, AFP)

Protection of Government Networks (Public and Military)

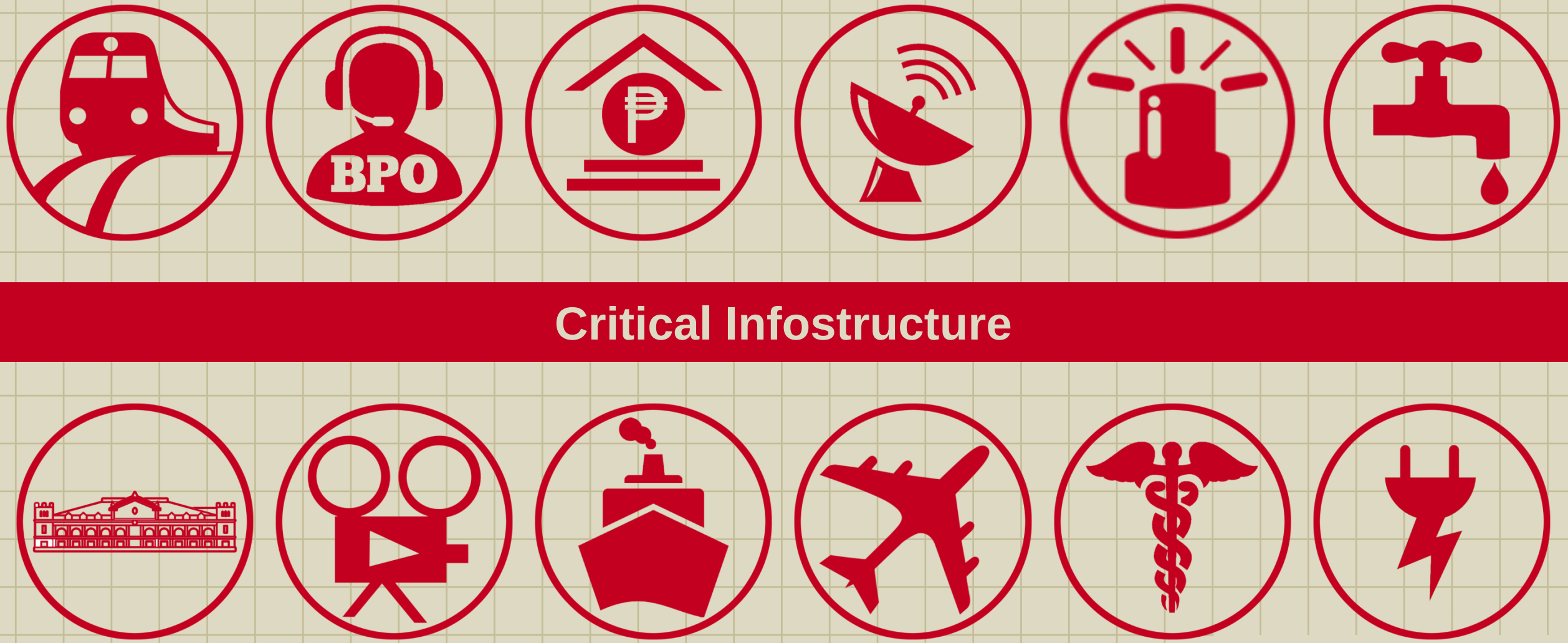
Protection of Businesses and Supply Chains

National Common Criteria Evaluation and Certification Program

Cybersecurity Education Campaign Program

Protection of Individuals

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY



Critical Infostructure

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

CII Protection and Security Assessment Program

- Protection Assessment Project (ICT Systems)
- Security Assessment Project (Readiness)
- Compliance Certification to Cyber Risks of CII

National Cyber Drills and Exercises Program

- Assess the capability and readiness of CII
- Annual Activity

#CyberResilientPH

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Protection for Government Networks

National Computer Emergency Response Program

- NCERT, GCERT, and Sectoral CERTs

Threat Intelligence and Analysis Centers

- DND Cyber Defense Center
- NSC Threat Operations Center
- AFP CYBERCOMMAND
- NICA Cyber Intelligence and Attribution Center

#CyberToughPH

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Protection for Government Networks

#CyberToughPH

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

National Common Criteria Evaluation and Certification Program

- ICT Equipment Security Evaluation and Certification Project
- Creation of Secure Internet of Things (IoT) Systems

#CyberAssurancePH

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

CyberSecurity Education Campaign Program

****Educate, Empower and Encourage (3Es)****

- **T**raining **o**f **T**rainers Project (ToT)
- Cybersecurity Outreach Project (#PRInT)
  - Use of **P**aper, **R**adio, **In**ternet and **T**elevision (PRInT) media to create multiplier effect
- National Cybersecurity Awareness Month
  - Every 3rd week of October
- Integration of Cybersecurity in the education sector

#CyberSafePH | #PRInT

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Increase the Pool of Cybersecurity Experts

Establishment of Cyber Training facilities and Certification Programs

Promote National Cybersecurity R&D Program to attract and cultivate Cyber Experts

Trainings to Develop Cybersecurity Specialist

Promote Communities of Practice (COP)

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Strategic Collaboration

NATIONAL LEVEL COMMITTEE

- National Cybersecurity Inter-Agency Committee
- Cybercrime Investigation and Coordination Center

PUBLIC PRIVATE PARTNERSHIP

- Public Private Partnership Forums

INTERNATIONAL COLLABORATION

- Enhanced international law enforcement and judicial cooperation against cybercrime-information sharing
- Law Enforcement Trainings
- Training for Judges and Prosecutors
- Increased public/private and interagency information sharing in line with cybersecurity standards
- Increased collaboration between and among CERTs

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

International Cooperation

Cyber Security

- JCSWG
- ASEAN TELMIN
- CyberSecurity Malaysia
- APCERT
- FIRST
- JAPAN-ASEAN
- CyberSecurity Working Group of ASEAN Defense Ministers (ADMM)
- Bilateral Security and Defense Partnership (USA)
- CAMP

Cyber Crime

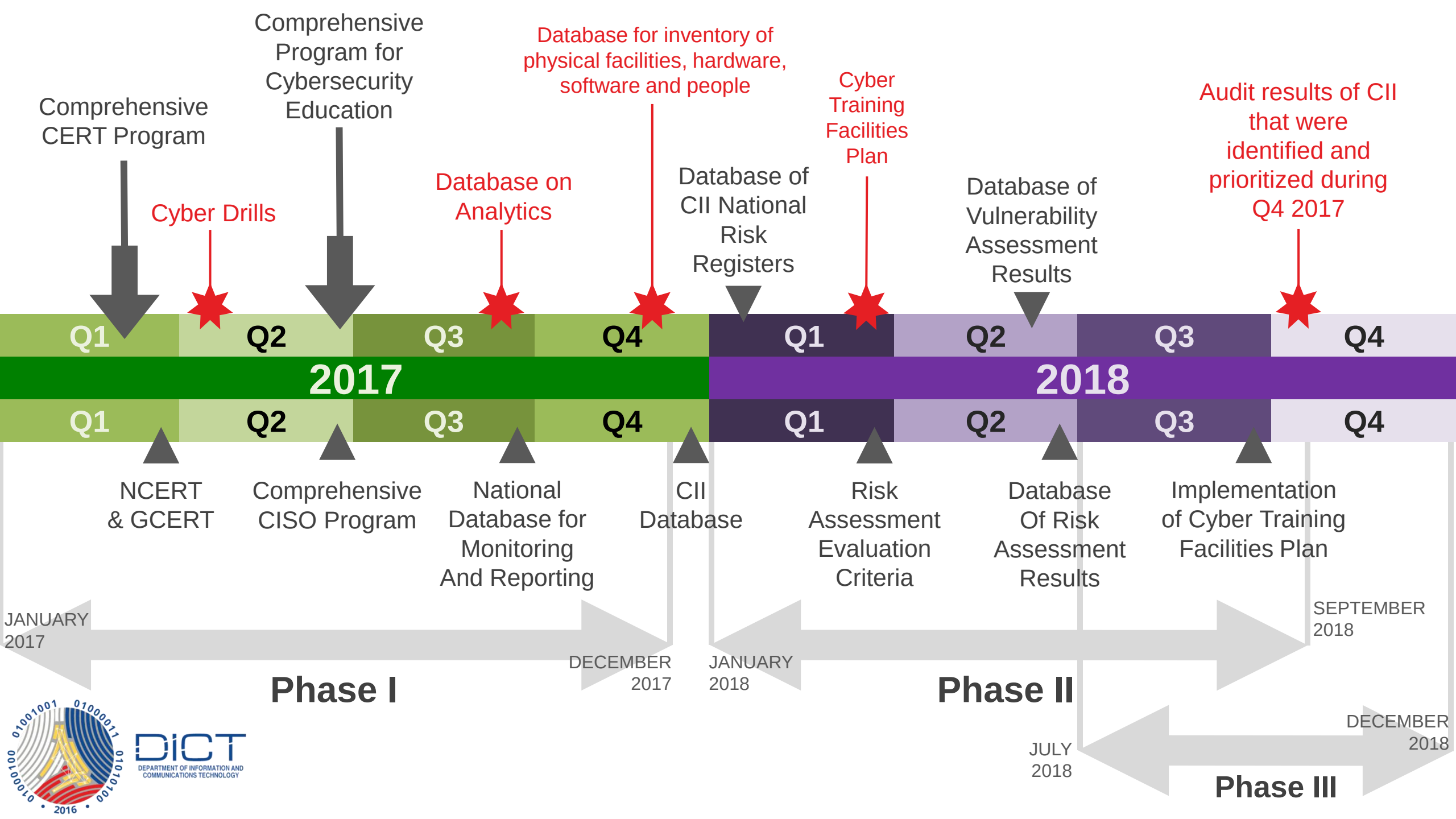
- BUDAPEST Convention
- INTERPOL
- ASEANAPOL
- EUROPOL
- USDOJ

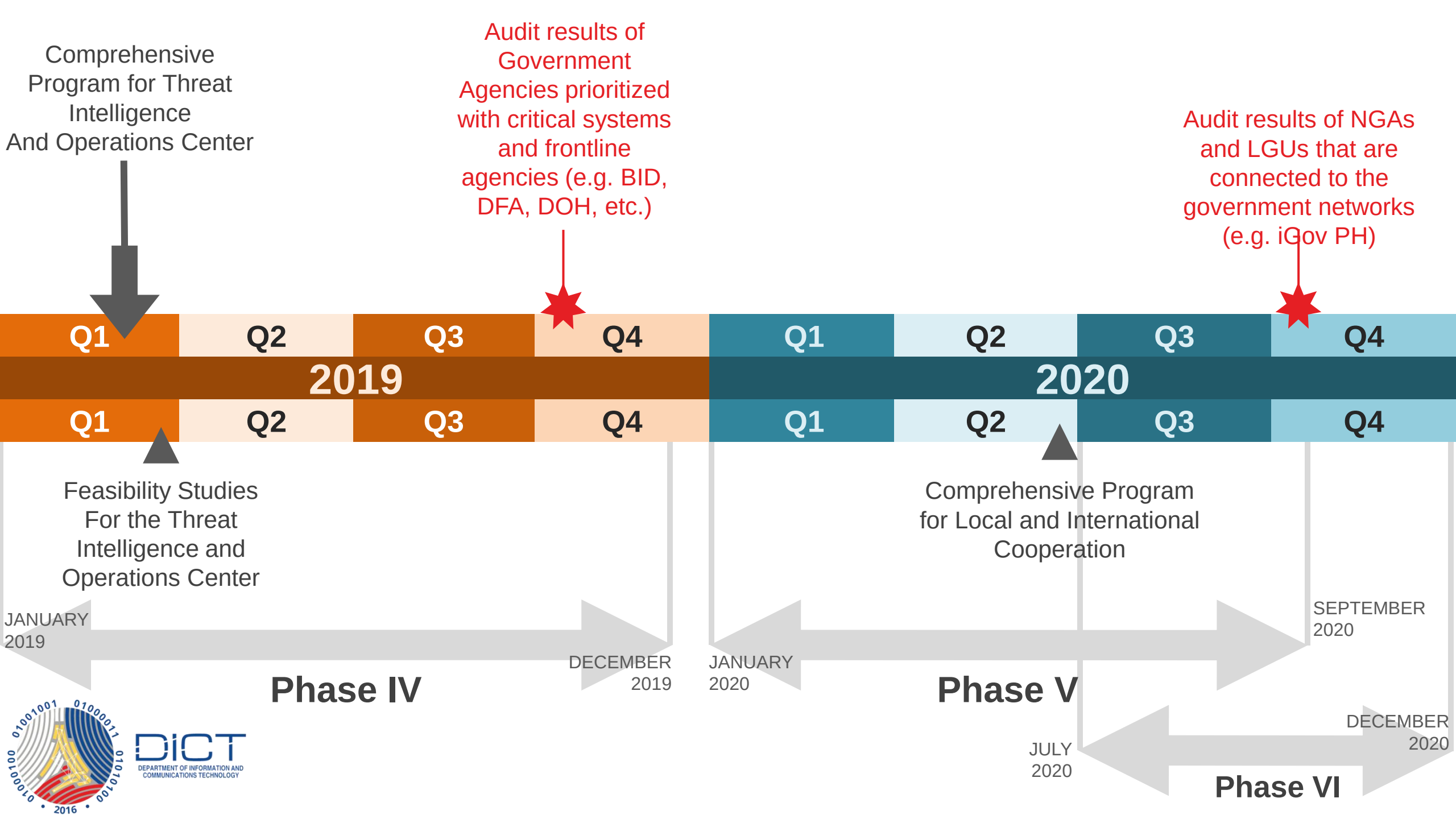
DICT

DICT

NATIONAL CYBERSECURITY PLAN 2022

TIMELINE


Comprehensive CERT Program
Comprehensive Program for Cybersecurity Education
Cyber Drills
Database on Analytics
Database for inventory of physical facilities, hardware, software and people
Database of CII National Risk Registers
Cyber Training Facilities Plan
Database of Vulnerability Assessment Results
Audit results of CII that were identified and prioritized during Q4 2017
Q1 Q2 Q3 Q4 2017 Q1 Q2 Q3 Q4 2018 Q1 Q2 Q3 Q4
NCERT & GCERT
Comprehensive CISO Program
National Database for Monitoring And Reporting
CII Database
Risk Assessment Evaluation Criteria
Database Of Risk Assessment Results
Implementation of Cyber Training Facilities Plan
JANUARY 2017
DECEMBER 2017
JANUARY 2018
SEPTEMBER 2018
JULY 2018
DECEMBER 2018
Phase I
Phase II
Phase III
DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY


Comprehensive Program for Threat Intelligence And Operations Center
Audit results of Government Agencies prioritized with critical systems and frontline agencies (e.g. BID, DFA, DOH, etc.)
Audit results of NGAs and LGUs that are connected to the government networks (e.g. iGov PH)
Q1
Q2
Q3
Q4
2019
Q1
Q2
Q3
Q4
2020
Feasibility Studies For the Threat Intelligence and Operations Center
Comprehensive Program for Local and International Cooperation
JANUARY 2019
DECEMBER 2019
Phase IV
JANUARY 2020
SEPTEMBER 2020
Phase V
JULY 2020
DECEMBER 2020
Phase VI
DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
2016

Tactical Work Plan

NATIONAL CYBERSECURITY PLAN 2022

12.08.2016

Launching of the NCSP 2022

Working Draft NCSP for comments (target date: January 15, 2016)

01.23.2017

Round Table Discussion Memorandum Circular

03.20.2017

National Cybersecurity Inter-Agency Council (NCIAC) Meeting

05.02.2017

Publication of NCSP 2022 Release of Memorandum Circular

Quick Wins

- Release DICT Department Orders for the Implementation of the National Cybersecurity Plan 2022
- Establish and activate the National Cyber Intelligence Platform (NCERT)
- Establish the Cyber Threat Intelligence and Analysis Centers
- Institutionalize the Cyber Safety Advocacy Promotion
- Establish the ICT Equipment Testing Laboratory
- Establishment of Cyber Training Facilities

#CYBERRESILIENTPH

DICT

NATIONAL CYBERSECURITY PLAN 2022

THANK YOU!