

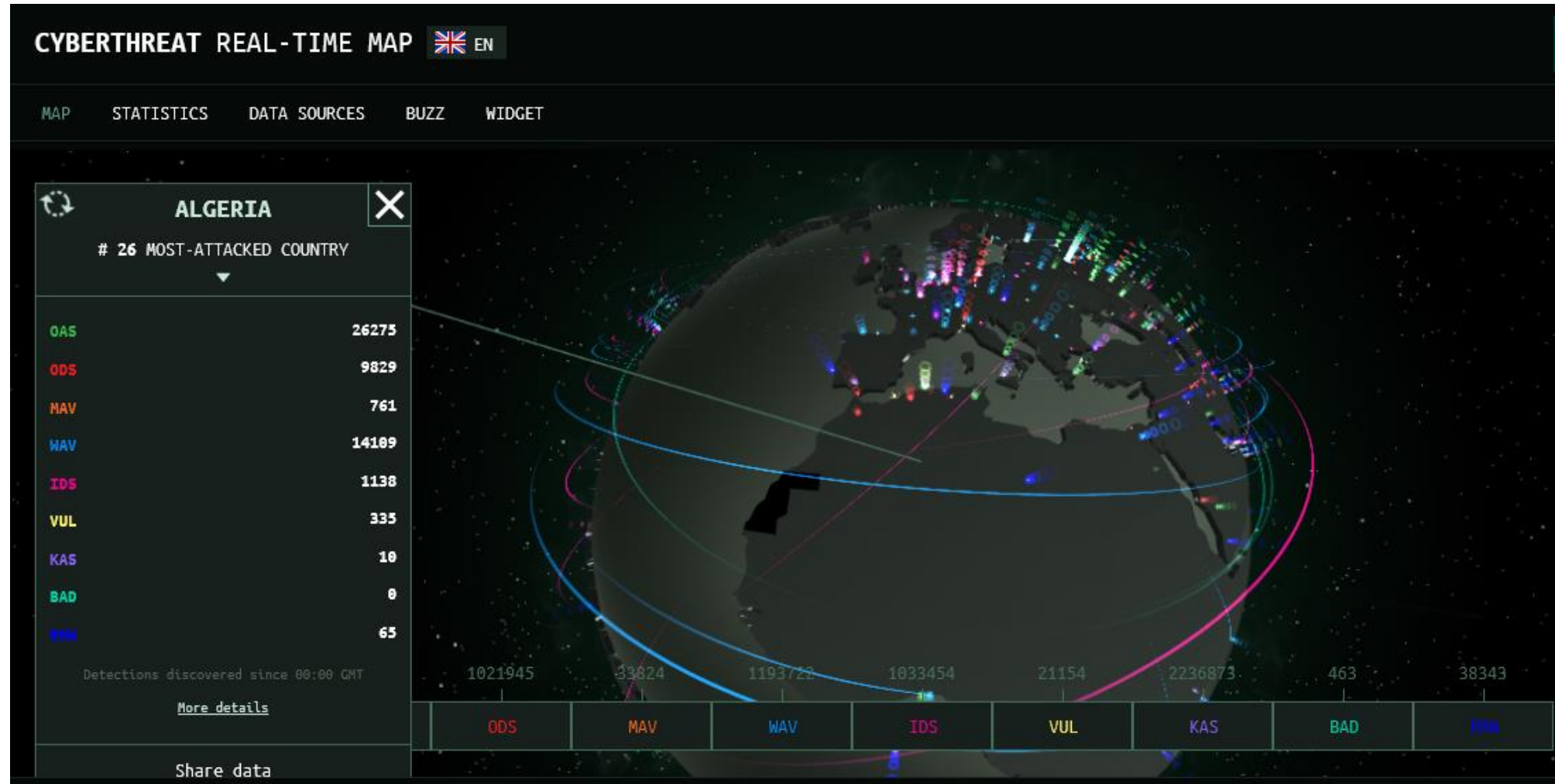
Building Cybersecurity Controls

Abdel Basset Zerrouki
Cybersecurity Consultant

(Board Member of OWASP Algiers Chapter)
PECB (ISO 27001 LI, 22301 LI), ISACA (CISM, CISA)

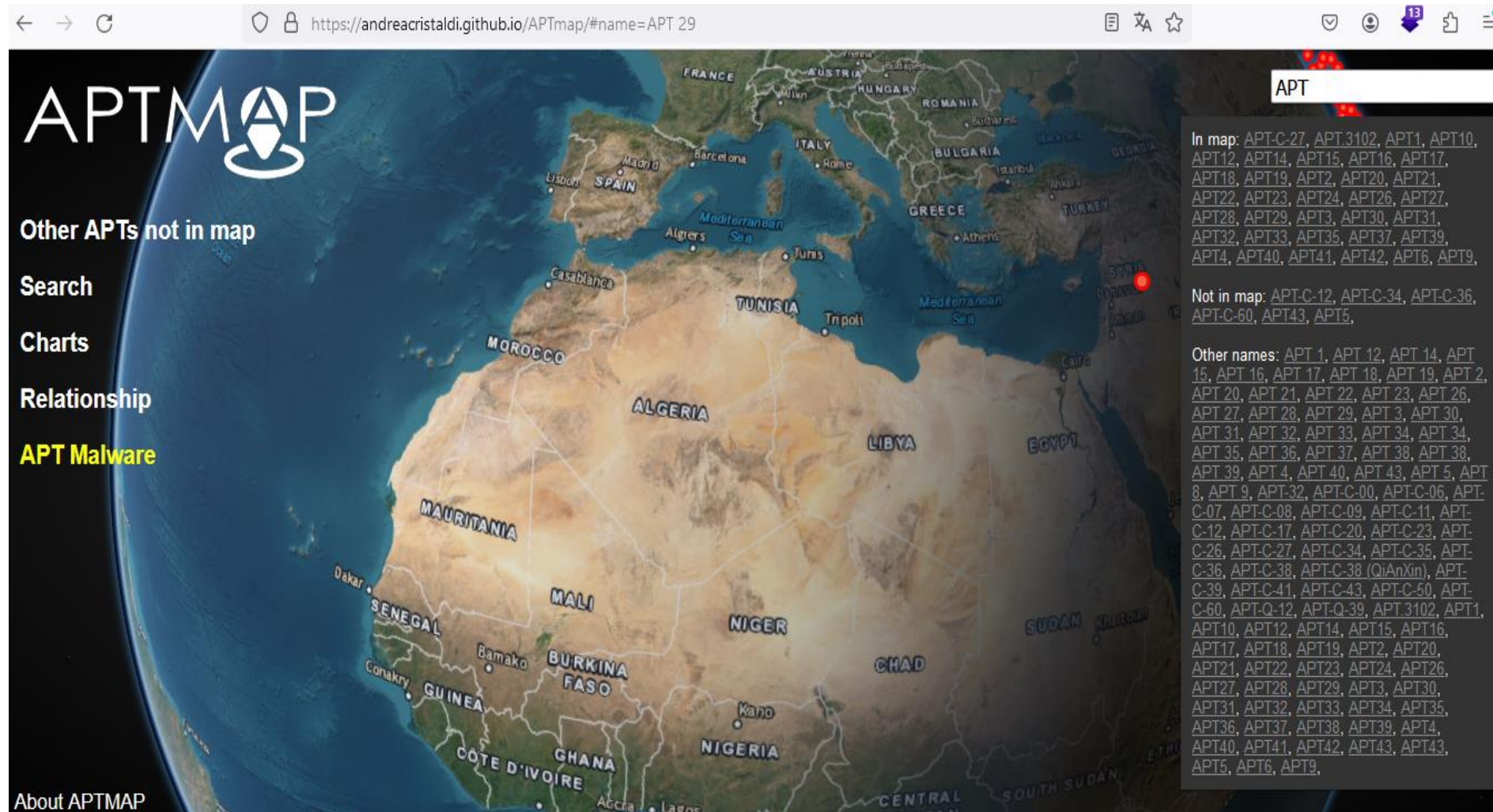


Cyber Attacks Map

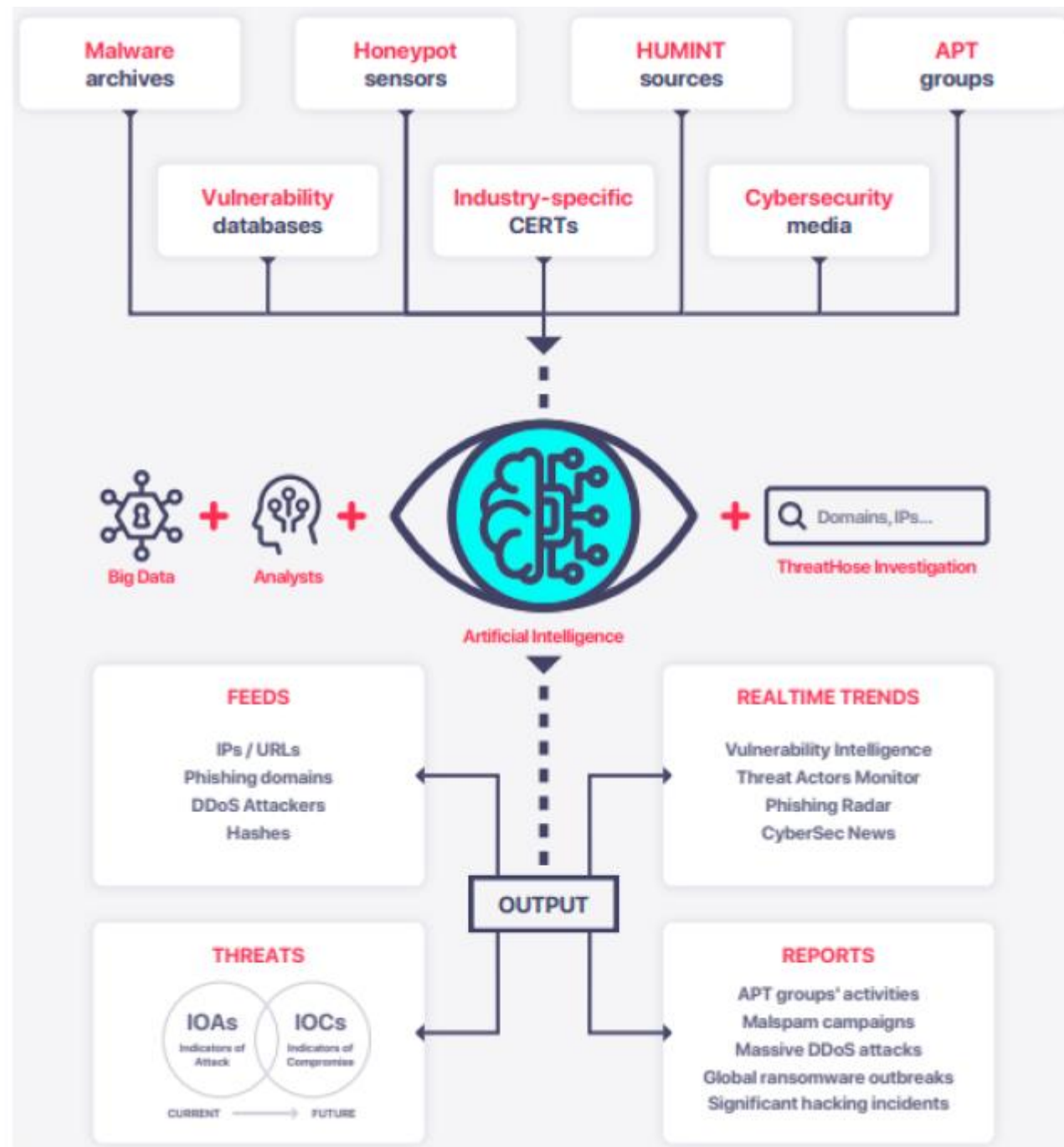


<https://cybermap.kaspersky.com/>

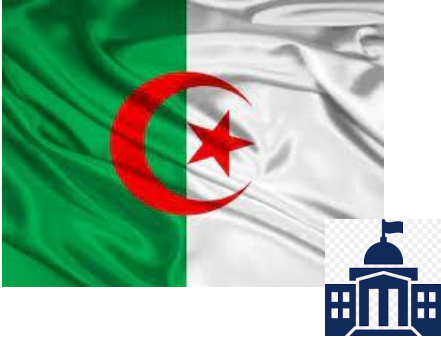
APT Map (Advanced Persistent Threats)



<https://andreacristaldi.github.io/APTmap/#name=APT%2029>



National Cybersecurity Context



- Understand and Assess internal and external cyber threat actors
(APT Groups – <https://attack.mitre.org/>).
- Secure Digital Gov Service (تقديم خدمات حكومية آمنة)
- Global Cybersecurity Index (تحسين الترتيب العالمي في الأمن السيبراني)
- Establishment of regulatory bodies (Cybersecurity , data protection) –
إنشاء الهيئات التنظيمية (الأمن السيبراني، حماية البيانات)

Administrations - Institutions - Organizations
(Public and Private)

مؤسسات – شركات عمومية وخاصة – بنوك،
... مستشفيات، تعليم

- Provide secure and Resilient digital services
- Comply with Regulatory Organizations

أفراد
Citizen

- Consume digital services
- Social media
- Mail, ...
- Personal data
- Cyber Awareness

إنشاء نظام وطني لأمن نظم المعلومات - (20-05) مرسوم رئاسي - Presidential decree



Strategic Level

- Conseil National de la Sécurité des Systèmes d'Information
المجلس الوطني لأمن نظم المعلومات

Tactical & Operational Level

- Agence de la Sécurité des Systèmes d'Information
الوكالة الوطنية لأمن نظم المعلومات



قانون 07-18
حماية البيانات الشخصية

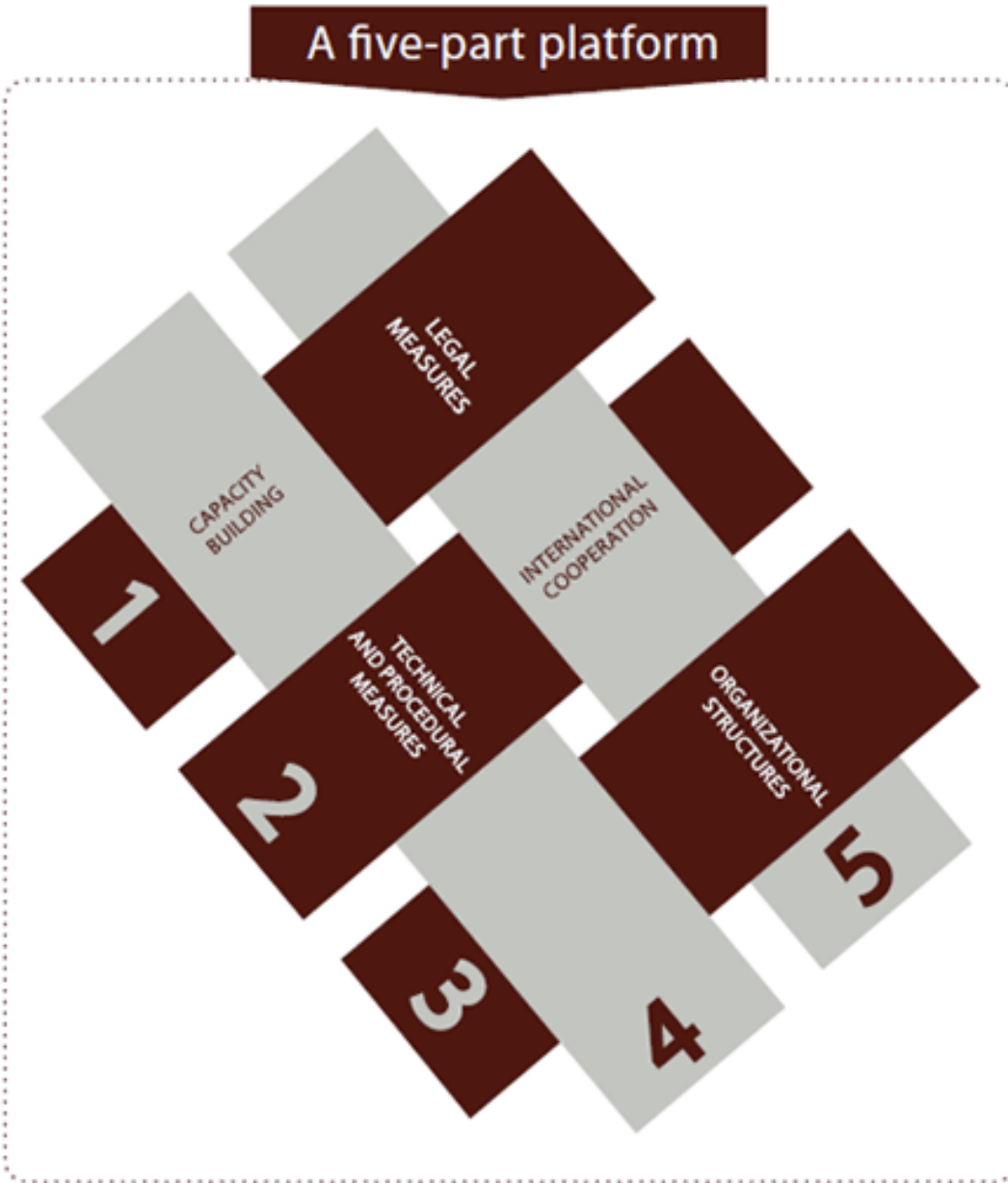
Global Cybersecurity Index



مؤشر الأمن السيبراني العالمي – Global Cybersecurity Index

هو مرجع موثوق به يقيس التزام الدول بالأمن السيبراني على المستوى العالمي لزيادة الوعي بأهمية وأبعاد الأمن السيبراني.

نظرًا لأن الأمن السيبراني له مجال واسع للتطبيق ، يشمل العديد من الصناعات والقطاعات المختلفة ، يتم تقييم مستوى التنمية أو المشاركة لكل بلد على أساس خمس ركائز :



- (1) التدابير القانونية Legal Measures
- (2) التدابير التقنية Technical & Procedural Measures
- (3) التدابير التنظيمية Organizational Structures
- (4) تنمية القدرات Capacity Building
- (5) التعاون International Cooperation

Global Position

Malaysia is highly ranked in cybersecurity because it has policies focused on developing a solid national strategy



Source: International Telecoms Union

BloombergOpinion

3. GCI results: Score and rankings

3.1 Global scores and ranking of countries

The following table sets out the score and rank for each country that took part in the questionnaire.

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10



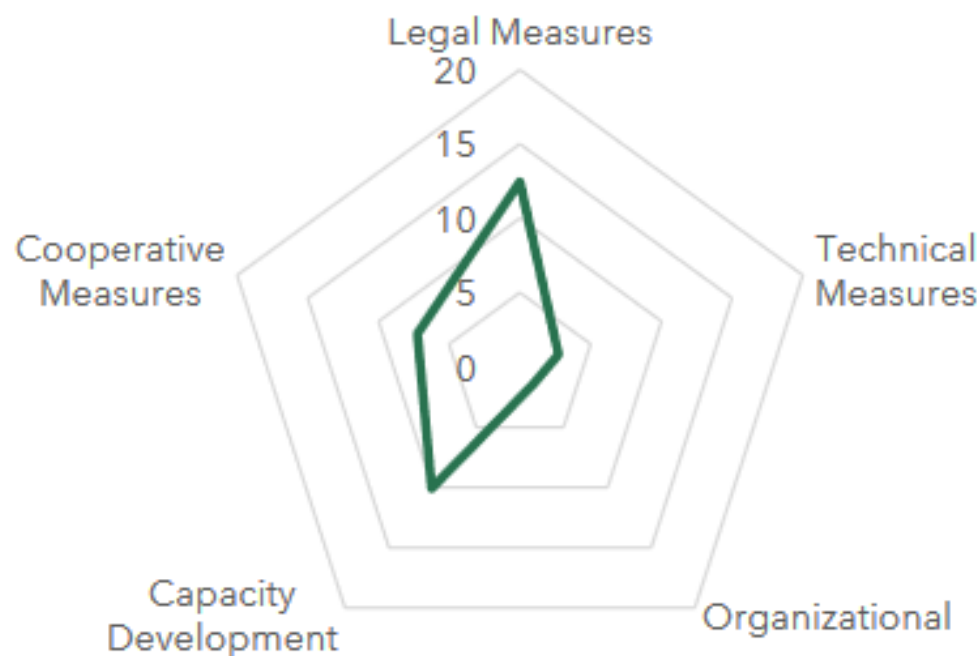
Senegal	35.85	100
Liechtenstein**	35.15	101
Sudan	35.03	102
Panama	34.11	103
Algeria	33.95	104
Togo	33.19	105
Jamaica**	32.53	106
Gambia	32.12	107



Country Name	Overall Score	Regional Rank
Saudi Arabia	99.54	1
United Arab Emirates	98.06	2
Oman	96.04	3
Egypt	95.48	4
Qatar	94.5	5
Tunisia	86.23	6
Morocco	82.41	7
Bahrain	77.86	8
Kuwait	75.05	9
Jordan	70.96	10
Sudan	35.03	11
Algeria	33.95	12
Lebanon**	30.44	13
Libya	28.78	14
State of Palestine	25.18	15
Syrian Arab Republic**	22.14	16
Iraq**	20.71	17
Mauritania	18.94	18
Somalia	17.25	19
Comoros**	3.72	20
Djibouti	1.73	21
Yemen*	0	22

Arab States region

Algeria (People's Democratic Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures

Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
33.95	12.46	2.73	1.44	10.07	7.25

Source: ITU Global Cybersecurity Index v4, 2020

International Cybersecurity Regulatory Organizations



هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority



NDMO
مكتب إدارة البيانات الوطنية
National Data
Management Office

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER



National Cyber
Security Centre

ACSC

Australian
Cyber Security
Centre



NCC 
CYBERSECURITY NATIONAL
COORDINATION CENTRE
GERMANY



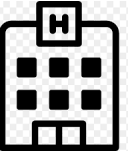
International cybersecurity Standards and Guidelines



The NIST
Cybersecurity
Framework

المرجع الوطني لأمن المعلومات
Référentiel National de la sécurité de
l'information (RNSI 2020)

المنصة الرقمية لمستشفى – Hospital Digital Platform – Study case :



HR System

Financial System

...

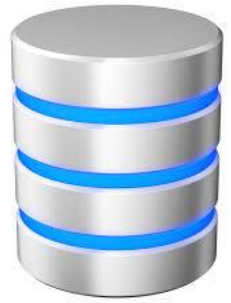


مركز بيانات – Data Center

منصة رقمية لمستشفى



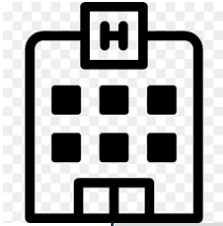
قاعدة بيانات للمعلومات شخصية للمرضى
Personal Information



بيانات شخصية للفريق الطبي
Personal Information

بيانات مالية (الفواتير، بنك، ...)
Financial Information

متطلبات الامتثال – Compliance Requirements



مركز بيانات – Data Center

منصة رقمية لمستشفى



الامتثال لمتطلبات المرجع الوطني لأمن المعلومات
Référentiel National de la sécurité de
l'information

الامتثال لمتطلبات قانون حماية البيانات
ذات الطابع الشخصي

18-07

الامتثال لمتطلبات المعايير الدولية وتطبيق
أفضل الممارسات المتعلقة بالأمن السيبراني

بناء ضوابط الأمن السيبراني – Building Cybersecurity Controls

Control Categories (ISO 27002)

- People Controls
- Technical Controls
- Physical Controls
- Organizational Controls

Security Objectives

- Confidentiality
- Integrity
- Availability

مركز بيانات – Data Center

منصة رقمية لمستشفى

Control Types

- Detective Controls
- Preventive Controls
- Corrective Controls
- Recovery Controls

Controls' Components

- People
- Technology
- Process

Control Cycle

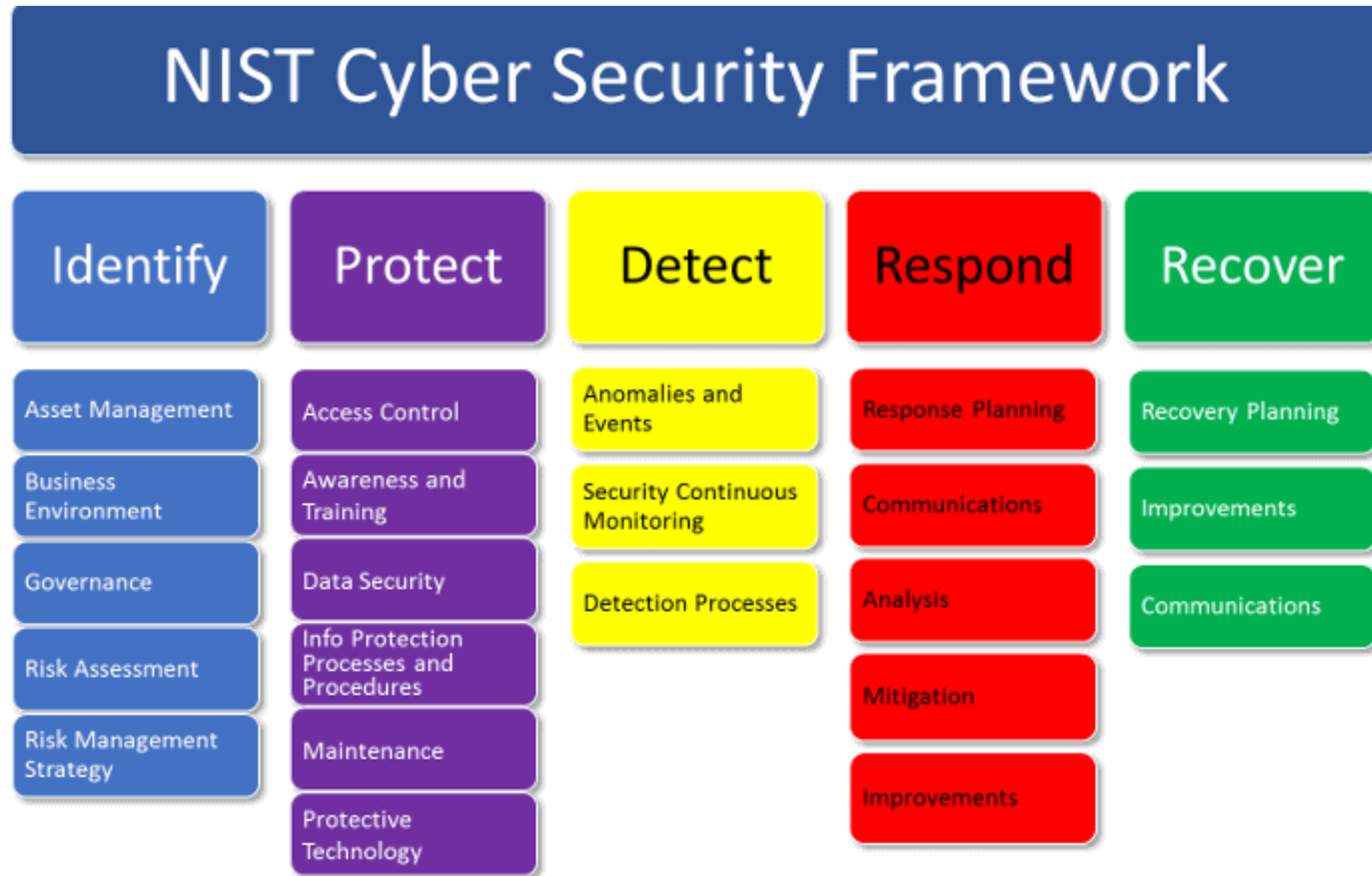
التخطيط - Plan

التنفيذ - Do

التحقق و المراقبة – Check

التحسين المستمر – Act

NIST Cybersecurity Framework



Organizational controls

- Policies for information security
- Information security roles and responsibilities
- Classification of information
- Access control & Identity management
- Threat intelligence
- Information security in project management
- Information transfer
- Privacy and protection of PII
- Information security in supplier relationships
- Information security for use of cloud services
- Response to information security incidents
- Independent review of information security (Security Testing)

سياسات الأمن السيبراني
تحديد الأدوار والمسؤوليات
تصنيف البيانات
إدارة الهويات، الدخول والصلاحيات
استخبارات التهديد
الأمن السيبراني في إدارة المشاريع
نقل البيانات
حماية البيانات الشخصية
الأمن السيبراني مع الأطراف الخارجية
الأمن السيبراني في الحوسبة السحابية
الاستجابة للحوادث الأمنية
التدقيق ، الإختبارات الأمنية

- User endpoint devices
- Protection against malware
- Privileged access rights
- Application security requirements
- Secure development life cycle
- Access to source code
- Secure coding
- Security testing in development and acceptance
- Change management
- Data leakage prevention
- Information backup
- Redundancy of information processing facilities
- Logging & Monitoring (SIEM tool)
- Networks security
- Cryptography.

Technological controls



From everywhere



People controls

- Background check – المسح الأمني
- Cybersecurity Awareness – التوعية حول مخاطر الأمن السيبراني
- Confidentiality Agreement – الحفاظ على السرية
- Responsibility After Termination of Employment
- Remote Work – العمل عن بعد
- Cybersecurity Event Reporting – التعامل مع حوادث الأمن السيبراني

The Essential Eight



**APPLICATION
CONTROL**



**PATCH
APPLICATIONS**



**CONFIGURE
MICROSOFT OFFICE
MACROS**



**USER APPLICATION
HARDENING**



**RESTRICT ADMIN
PRIVILEGES**



**PATCH OPERATING
SYSTEM**



**MULTI-FACTOR
AUTHENTICATION**



DAILY BACKUPS



Australian Government
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre

Essential Controls: 10 Priority Areas for Increased Cyber Resilience

Multifactor Authentication (MFA)



Virtual Private Network (VPN)



Remote Desktop Protocol (RDP)



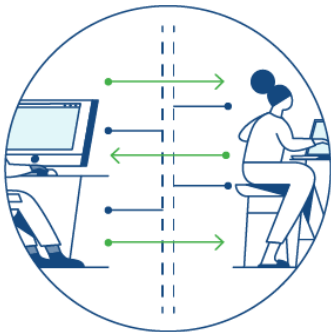
Endpoint Detection and Response (EDR)



Incident Response Planning



Infrastructure and Segmentation



Backups



Access Control



Security Culture Training



Email Hygiene

