Garda National Cyber Crime Bureau

Paul Johnstone

Ransomware Attack – Healthcare Systems

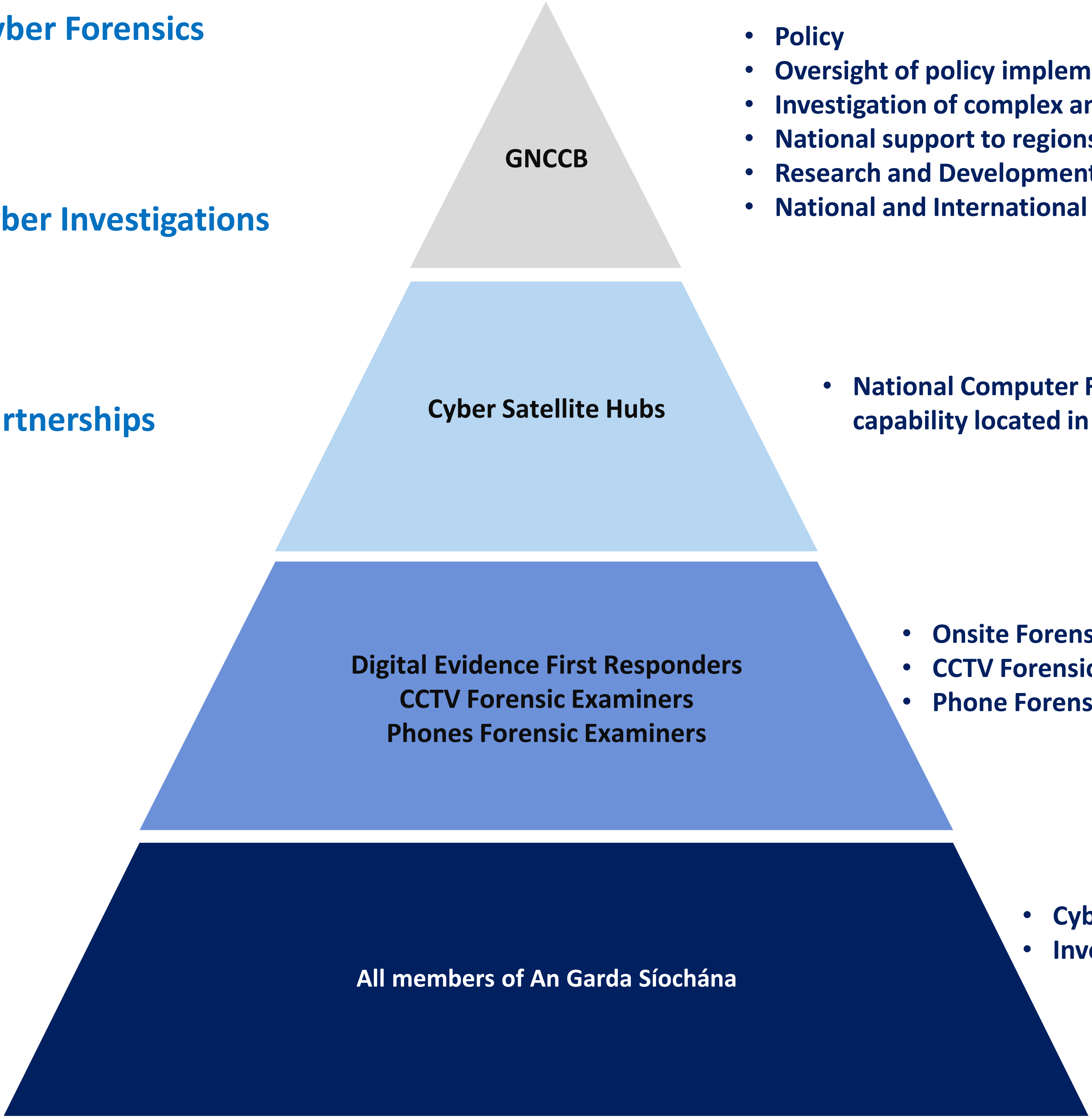
Garda National Cyber Crime Bureau

Cyber Operating Model

Cyber Forensics

Cyber Investigations

Partnerships



GNCCB

- Policy
- Oversight of policy implementation & cyber crime trends
- Investigation of complex and serious cyber crime
- National support to regions & divisions
- Research and Development
- National and International liaison

Cyber Satellite Hubs

- National Computer Forensic and Cybercrime capability located in regions

Digital Evidence First Responders
CCTV Forensic Examiners
Phones Forensic Examiners

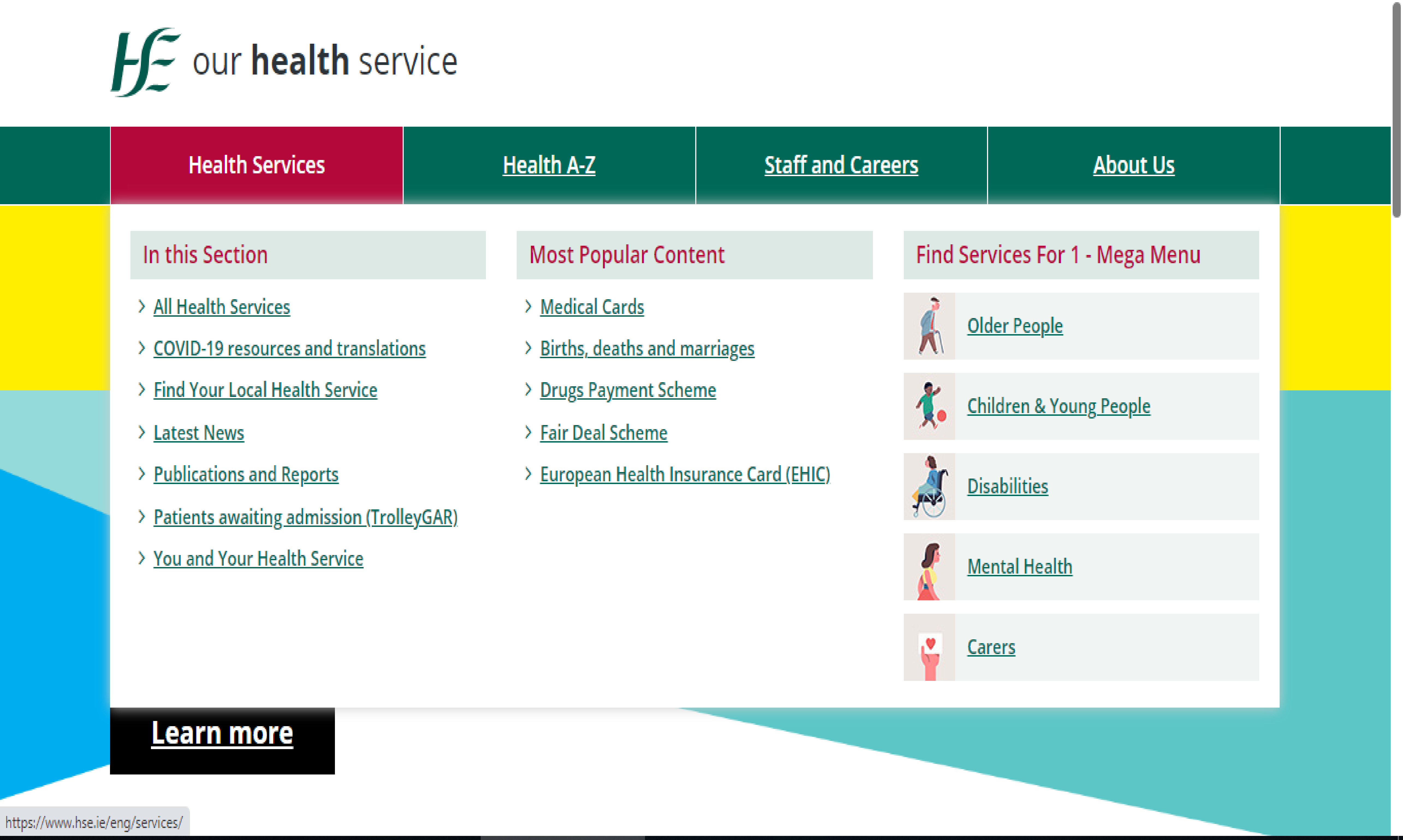
- Onsite Forensics and at scene triage
- CCTV Forensic examinations
- Phone Forensic examinations

All members of An Garda Síochána

- Cybercrime awareness
- Investigate less serious cybercrime matters

Garda National Cyber Crime Bureau

Health Service Executive attack



our **health** service

Health Services | Health A-Z | Staff and Careers | About Us

In this Section

- All Health Services
- COVID-19 resources and translations
- Find Your Local Health Service
- Latest News
- Publications and Reports
- Patients awaiting admission (TrolleyGAR)
- You and Your Health Service

Most Popular Content

- Medical Cards
- Births, deaths and marriages
- Drugs Payment Scheme
- Fair Deal Scheme
- European Health Insurance Card (EHIC)

Find Services For 1 - Mega Menu

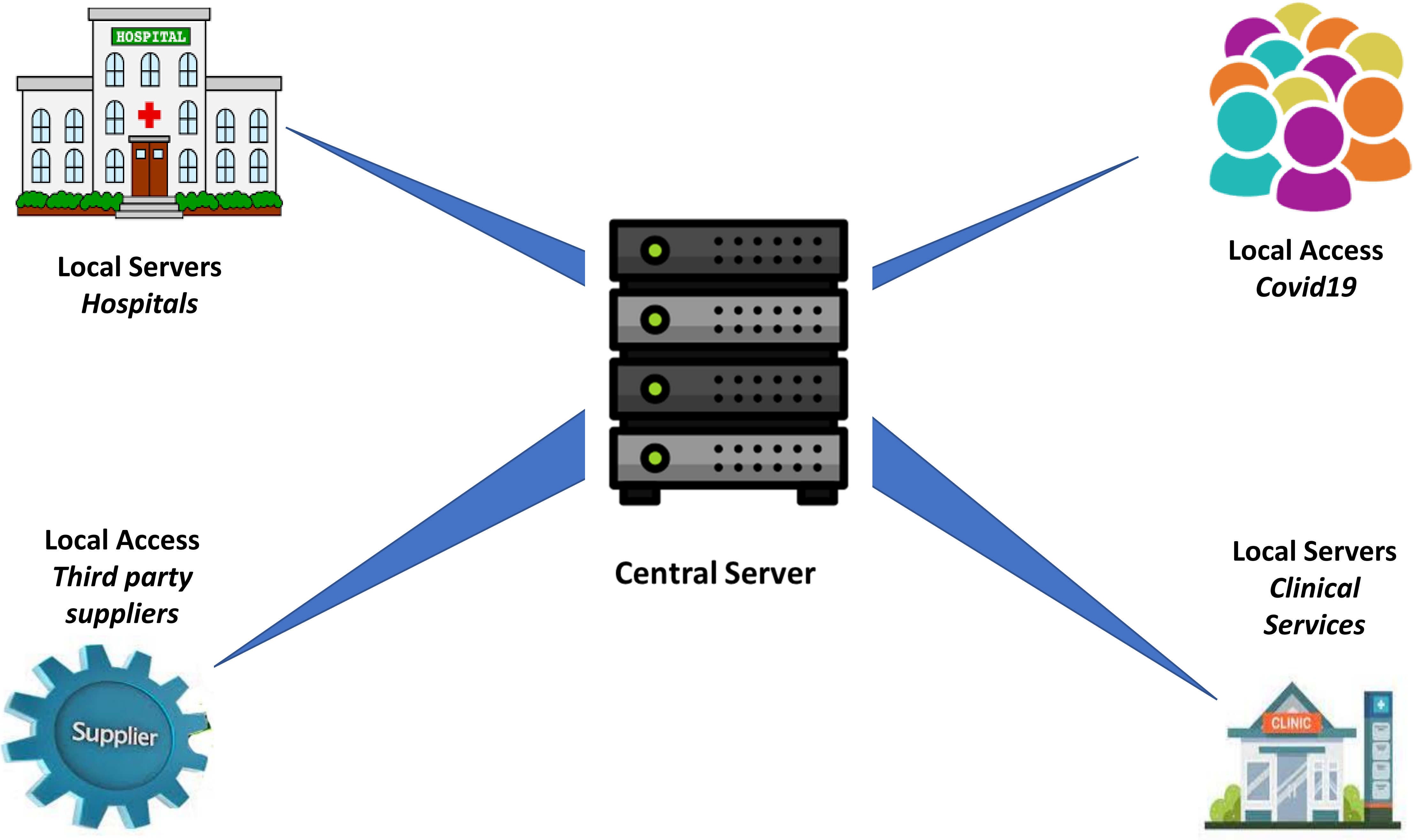
- Older People
- Children & Young People
- Disabilities
- Mental Health
- Carers

Learn more

https://www.hse.ie/eng/services/

Garda National Cyber Crime Bureau

Structure of HSE Network



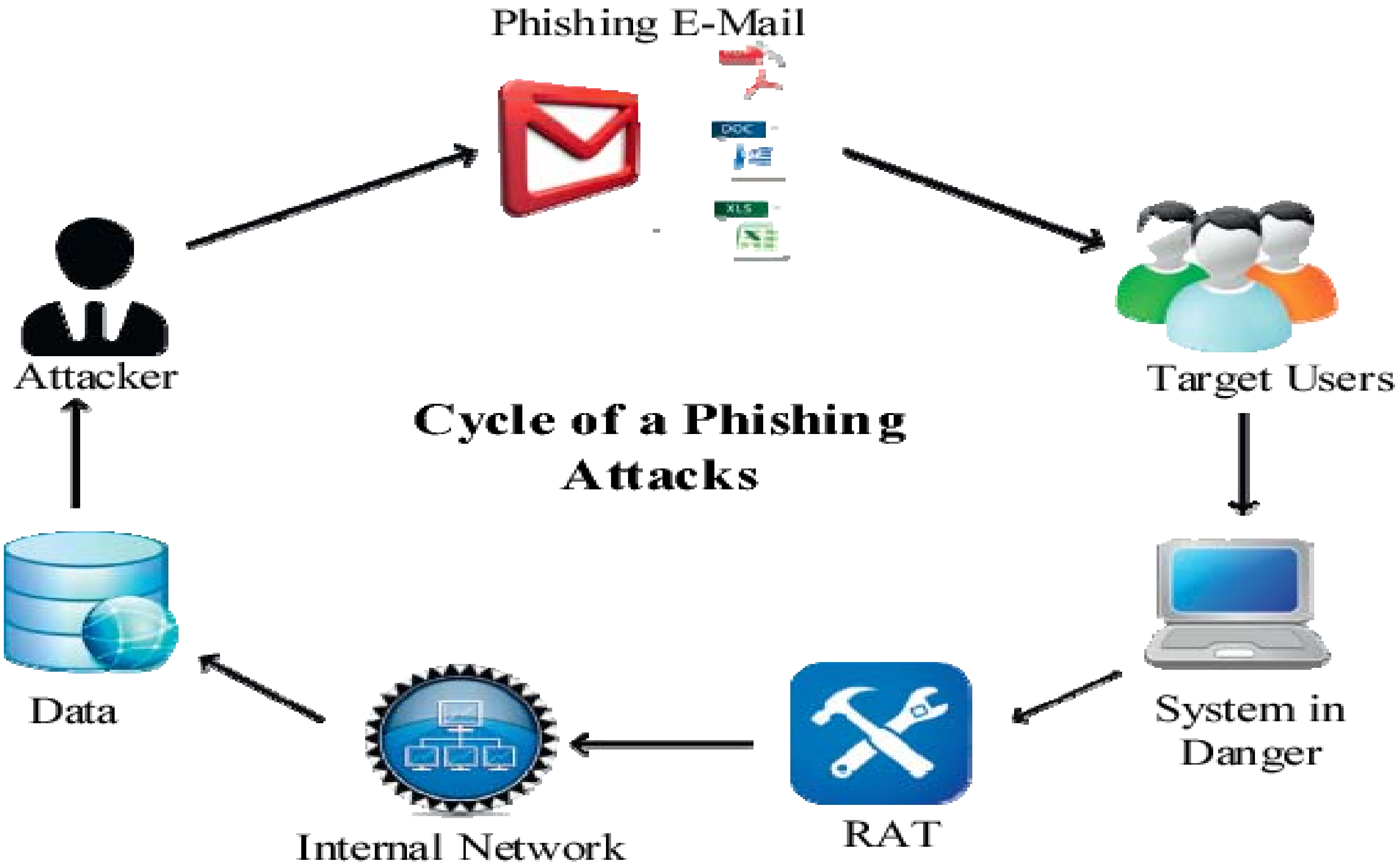
Local Servers
Hospitals

Local Access
Covid19

Central Server

Local Access
Third party suppliers

Local Servers
Clinical Services


Phishing E-Mail
DOC
XLS
Attacker
Target Users
Cycle of a Phishing Attacks
Data
System in Danger
Internal Network
RAT

Investigation

- Local examinations of servers
- Work closely with victim company
- Work with cyber security company
- Work with partners – LEA & Academia

- ONGOING

Cost

- Loss of confidence
- Customer data posted online
- Recovery cost
- Fines
- And……

- ONGOING

Lessons Learned

- Backup
- Have policies re BYOD, VPN, Emails
- Test the Policies
- Train Staff about risks and policies
- Involve LEA early
- Don’t pay

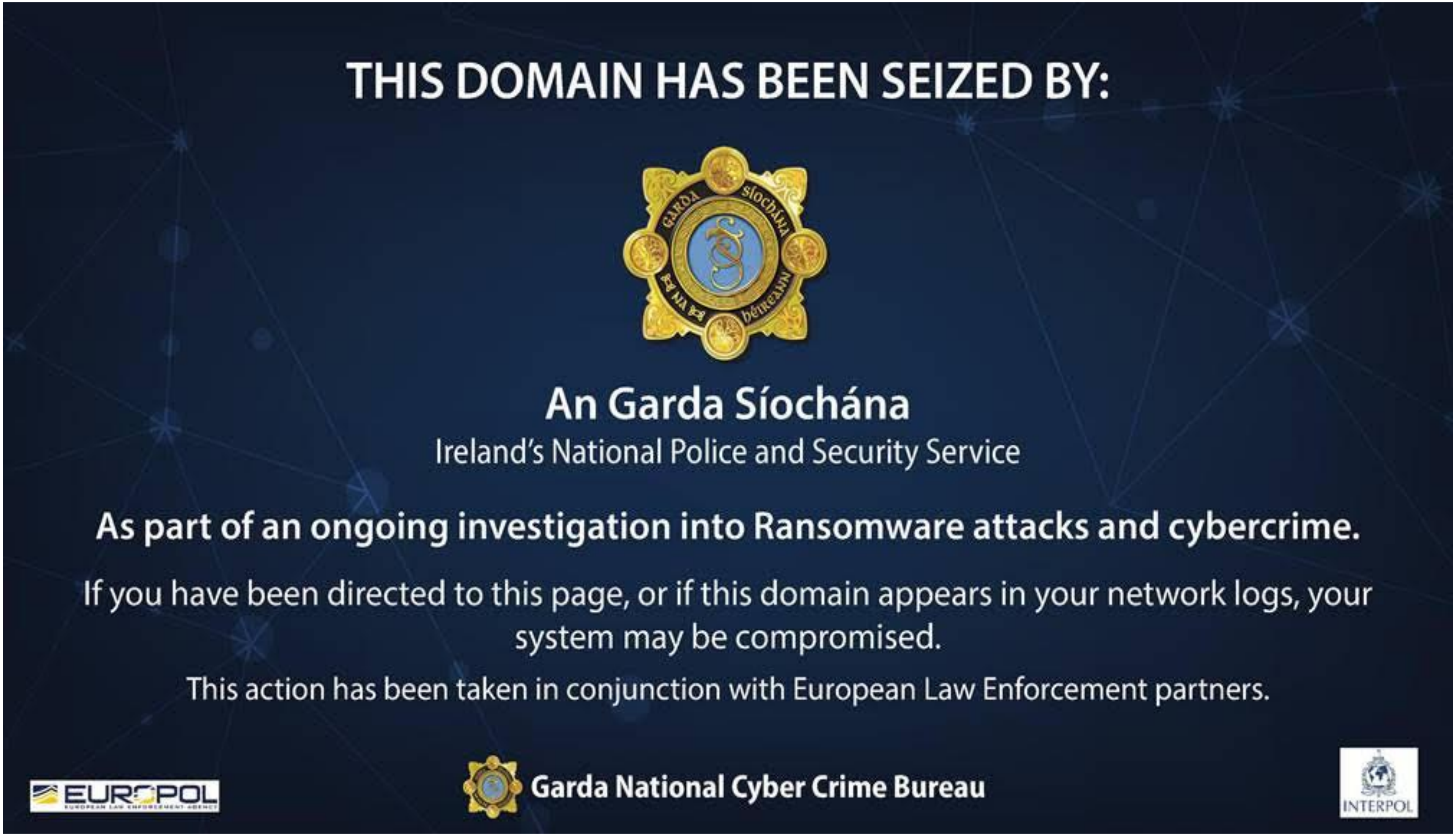
Garda National Cyber Crime Bureau

Why Report?

- Allows for Criminal Investigation & Victim Support
- **EXPERIENCED** EXAMINERS & INVESTIGATORS
- Identify Current and Emerging Trends & Methods of Attack
- Informs Advice to the Public & Corporate Sectors
- Reinforce customer confidence in your responses
- Support Victims of crime & recovery
- Statutory Obligations – Data Protection & s19 Criminal Justice Act 2011

Garda National Cyber Crime Bureau

Disruption



THIS DOMAIN HAS BEEN SEIZED BY:

An Garda Síochána

Ireland's National Police and Security Service

As part of an ongoing investigation into Ransomware attacks and cybercrime.

If you have been directed to this page, or if this domain appears in your network logs, your system may be compromised.

This action has been taken in conjunction with European Law Enforcement partners.

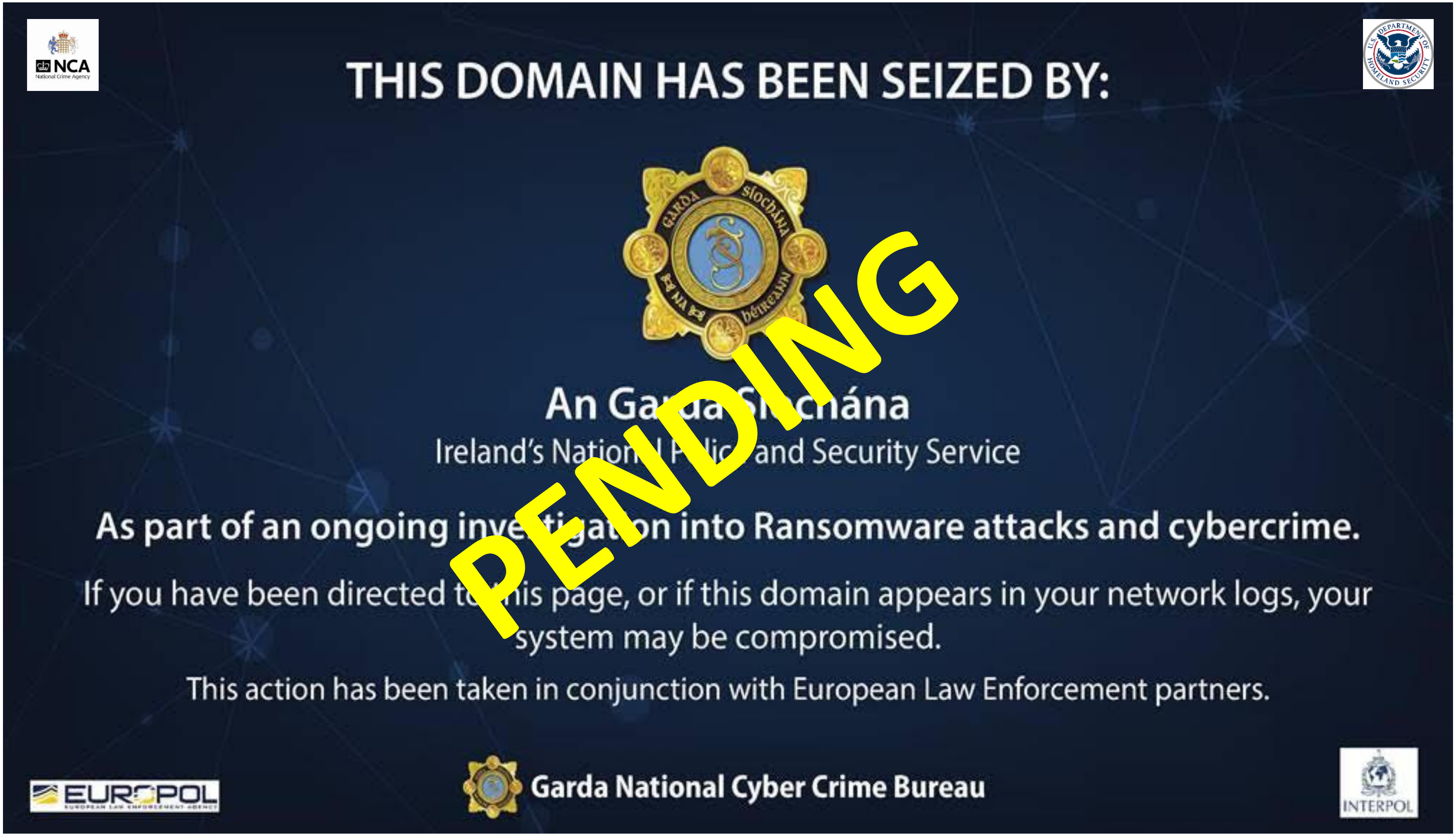
Garda National Cyber Crime Bureau

Server Disruption

- Malicious IP and Domain Names identified
- Non registered Domains identified – hard coded into malware
- Used to keep malware alive when other domains are taken down
- Unregistered domains purchased by AGS & monitored
- Incoming traffic to domains was from infected systems
- Infection process ended by seizure
- Over 1000 attempts to connect from global systems

Garda National Cyber Crime Bureau

Disruption – To Be Announced



THIS DOMAIN HAS BEEN SEIZED BY:

An Garda Síochána

Ireland's National Police and Security Service

As part of an ongoing investigation into Ransomware attacks and cybercrime.

If you have been directed to this page, or if this domain appears in your network logs, your system may be compromised.

This action has been taken in conjunction with European Law Enforcement partners.

Garda National Cyber Crime Bureau

PENDING

NCA
National Crime Agency
U.S. DEPARTMENT OF HOMELAND SECURITY
GARDA SÍOCHÁNA NA hÉIREANN
EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY
INTERPOL

Server Disruption

- Malware server identified in joint operation - ongoing
- Malware infections hosted and deployed
- Thousands of connections to server from global systems
- Information relayed to LEA partners
- Companies informed and enabled to deploy safeguards and updates etc
- Maintaining until ……

Contacts

Detective Sergeant Paul Johnstone
Garda National Cyber Crime Bureau
Harcourt Square
Harcourt Street
Dublin 2
D02 DH42
IRELAND

Email: GNCCB@garda.ie

Telephone: +353 1 6663708