JCSC
Jersey Cyber Security Centre

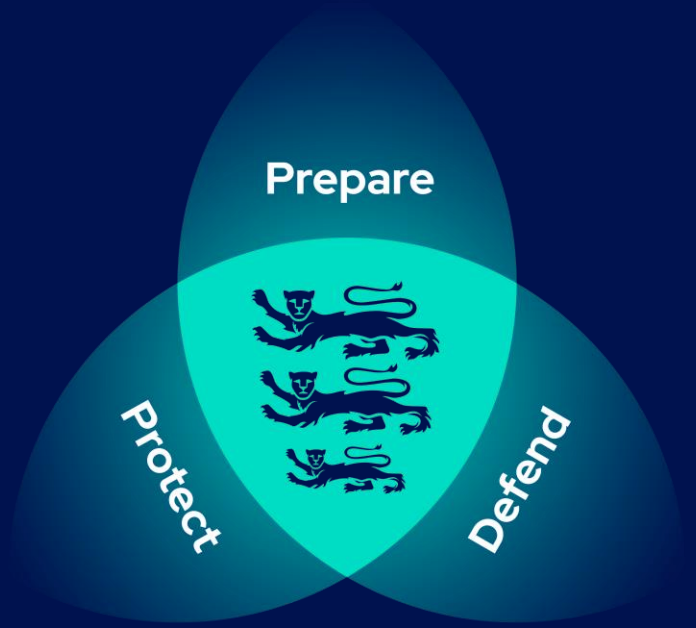
Aligning Incident Response with Emergency Response using JESIP

15 January 2023

TLP: CLEAR

Your presenter

- Ex-UK civil service (from a doughnut-shaped office in Gloucestershire)
- Ex-managed security service
- Lately senior analyst at JCSC
- *Not* a tech…
- Family and local history/OSINT (same thing)
- My grandsons call me Grumpy…



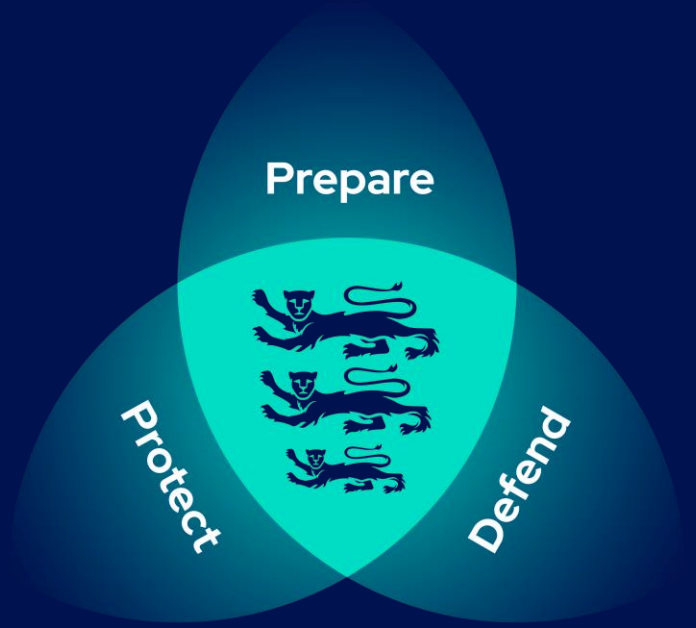
Where this started

"Emergency services have been doing what they do for a lot longer than CSIRTs have, and we should learn from them rather than trying to reinvent the wheel."

(Olivier Caleff, TRANSITS 1, Haarlem, April 2024)

"Emergency Planning are running JESIP training w/c 13th May, and JCSC staff are all attending."

(Matt Palmer, Director of JCSC)



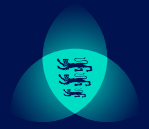
JESIP

- Started with the Pollock Report (2013)…
- …which surveyed 30+ reports on major incidents (1986-2010)
- The same issues kept coming up…
- Four cross-cutting themes:
  - Doctrine
  - Operational communications
  - Situational awareness
  - Training and exercising

- Interoperability: *'the extent to which organisations can work together coherently as a matter of course.'*

Parked question

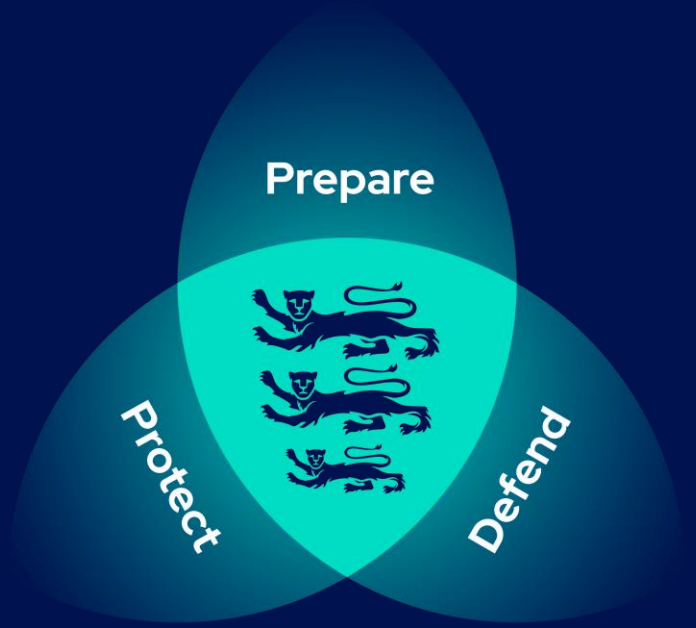
- Is this something the UK is uniquely bad at?



Poor working practices/organisational planning	Inadequate training	Ineffective communication
No system to ensure lessons learned and disseminated	**Lack of Leadership**	Blame culture
Failure to learn lessons	No monitoring/audit mechanism	Previous reports not acted upon

Principle 1: Colocate

- Enormously important when you're fighting a fire with casualties and a potential crime scene.
- Less obviously so in a cyber-incident, BUT…
- We still need to know where all stakeholders are and what they are doing
- We need information sharing
- Everyone needs a common understanding of the situation.
- Easy secure comms is *vital*.



2: Communicate

Meet Carla…our comms expert with no history in cyber or IR.

Having to explain how malware, or passkeys, or specific cyber technology works in simple terms is *brilliant* preparation for emergency comms that need to be

- clear
- jargon-free
- acronym/abbreviation-free

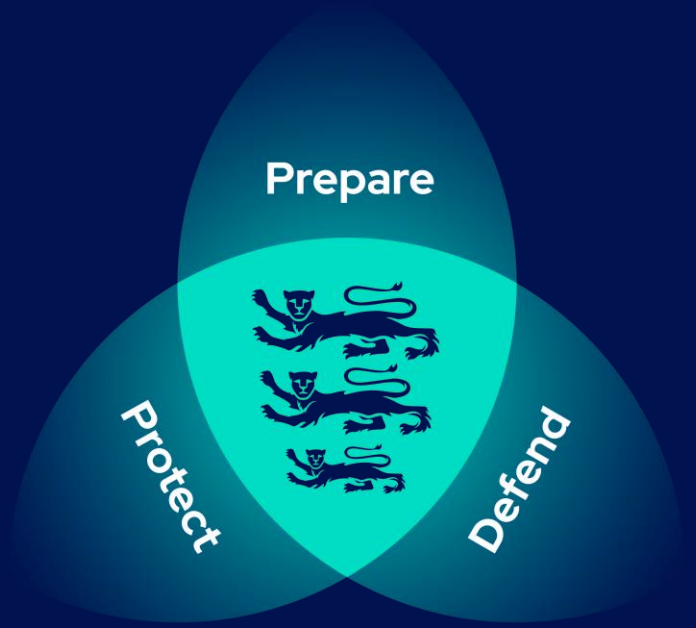
… something which, as mainly tech people, we are *not* always good at.

3: Coordinate

WHO IS RUNNING THE SHOW? (Not always who you think)

They need to agree:

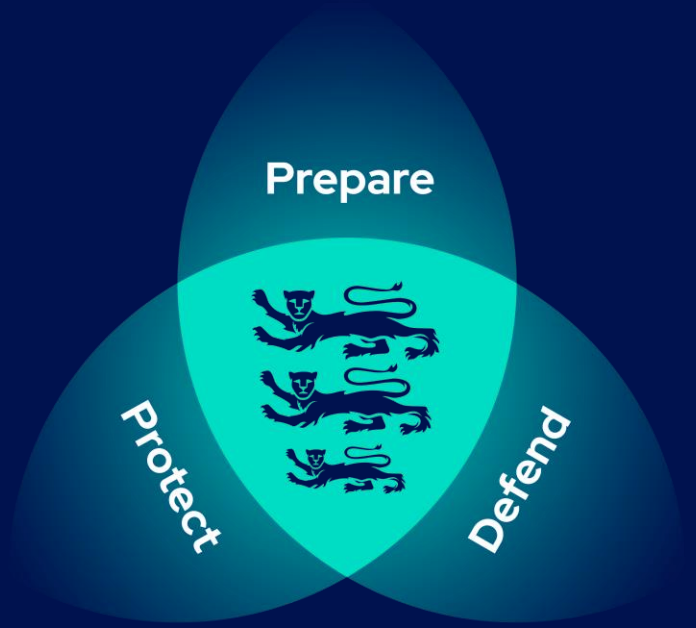
- Identify priorities
- and resources
- and capabilities
- and limitations
- Aim is an effective response – so that also means keeping people talking… you need to TALK (inviting response) not TELL.



4: Jointly understand risk

- Sharing information…
- about the likelihood and potential impact of threats and hazards…
- to agree appropriate control measures.

No different from cyber incident response.



5: Shared Situational Awareness (1)

Structured comms: (M/ETHANE shown; also IIMARCH for briefings) have benefits:

- Anyone can convey a M/ETHANE message – not just seniors.
- People know what to listen for/can prompt for missing details.
- Helps people with (eg) language barrier.
- What might an IR team want instead?

5: Shared Situational Awareness (2)

And this is IIMARCH

- Information comes from M/ETHANE and updates
- Intent is what we are trying to achieve
- Method is how we are trying to achieve it
- What do we need to implement the plan?
- What are the relevant risks – how can we mitigate them?
- How are we going to communicate – both between ourselves, and with interested parties?
- What humanitarian/human rights issues might arise? (Info sharing and disclosure for two)

Joint Decision Model

Best way to visualise? A bit like morris dancing.

More seriously: it's a 5-step loop with a centre turn at every stage:

- Gather info and intelligence
- Assess threats, risks; build working strategy
- Consider powers policies and procedures
- Identify options and contingencies
- Take action; review what happened

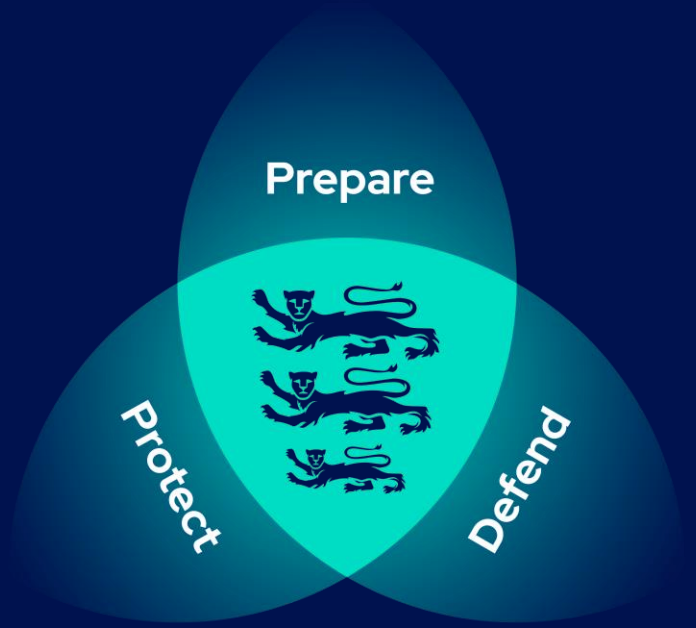
The centre turn: *is* what is being planned

Working together, saving lives, reducing harm?

Bringing things together

- No one party ever has all the answers – hence “talk don’t tell”.
- All decision-making is provisional – capture not just what decision was made, when, and what was the basis at that time.
- Base options and contingencies on:
  - Suitability (*would* we?)
  - Feasibility (*could* we?)
  - Acceptability (*should* we?)
- Brief agreed actions – and briefs should be brief.

REMEMBER - THIS IS HUMAN-CENTRED



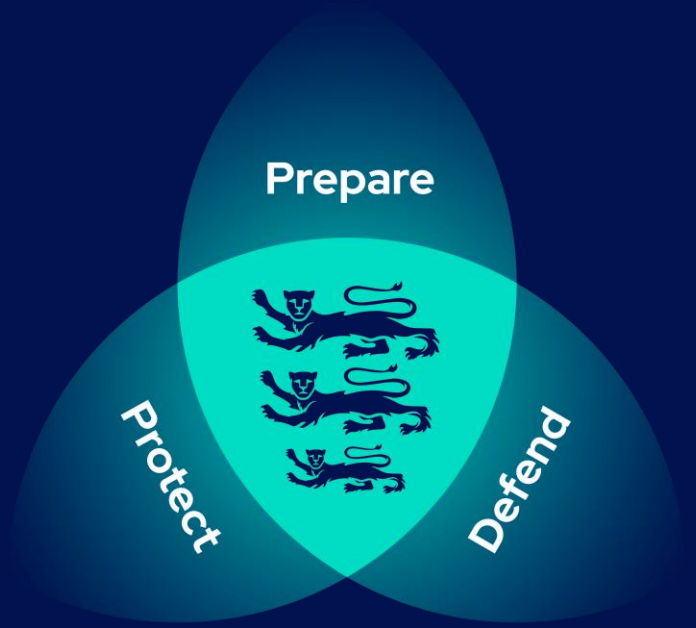
A bit about us…

Jersey is small:

- Major incidents are rare (though they're like London buses – none for ages, then three come at once)

But being small, *we know each other*

- Trust in each other is almost universal
- The ER community isn't just police/fire/ambulance
- We have access to external reviewers to challenge us.



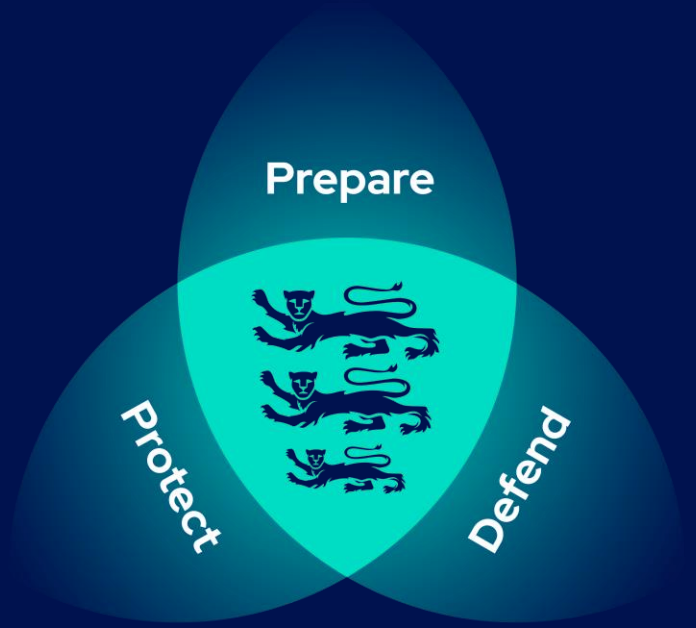
What might we do?

Two bad ideas:

- Create CyberJESIP (just no)
- Cherry-pick good ideas (tempting, but no)

And one (possibly) better idea: *alignment*

- We don't do the exact same thing, but we want the same ends, and we want to go the same way.
- We need clarity on coordination
- We need to be better at comms. Structure helps.
- We need to record decision making better.
- We need to train. Exercise. Have someone external review us (and doing it with others keeps us honest)
- And we need to remember. This is about humans. Human victims, and human responders - US



You?

We know that the 3-blue system isn't universal:

- Eg in France SAMU and Sapeurs-Pompiers overlap; Gendarmerie and Police Nationale relationship can be tricky.
- French ORSEC plans are well-established; but to my limited knowledge they don't include cyber threats
- Public perception of cyber risks varies across Europe…
- …and so does the degree of trust in emergency services.

We'd like to know more… How might it work for YOU?

M**è**rcie bein des fais!

TLP: CLEAR