National
Cyber
Deception
Laboratory

cyberdeception.org.uk

The Why, What and How of the NCDL

Rob Black, Deputy Director NCDL
Rich Munslow, CTO NCDL

National
Cyber
Deception
Laboratory
cyberdeception.org.uk

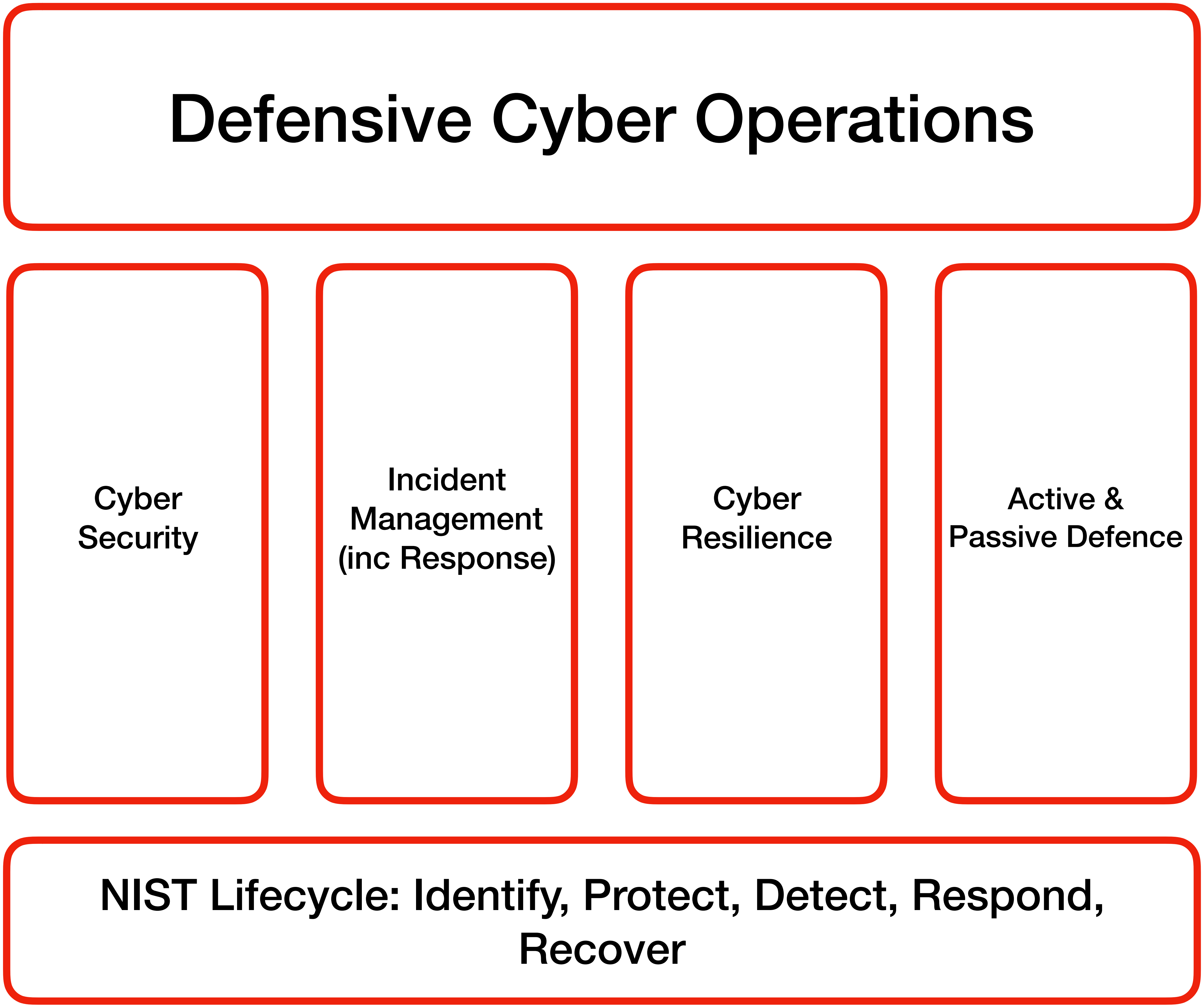
THALES

Principal Sponsor

Objectives

- Why a National Cyber Deception Lab?
- What is the NCDL?
- How will the NCDL deliver against the mission statement?

Why a National Cyber Deception Lab?



Defensive Cyber Operations

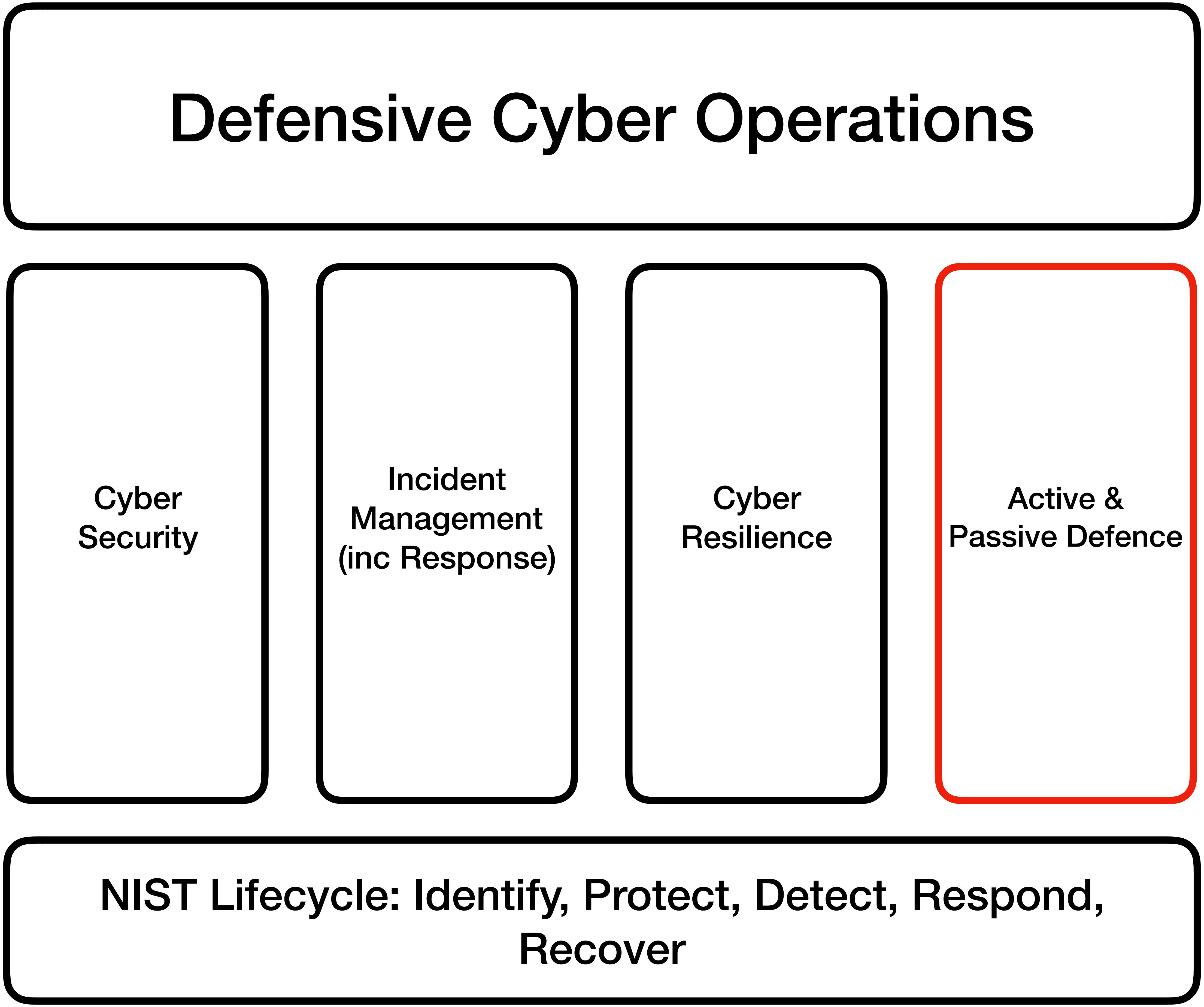
Cyber Security

Incident Management (inc Response)

Cyber Resilience

Active & Passive Defence

NIST Lifecycle: Identify, Protect, Detect, Respond, Recover



Defensive Cyber Operations

Cyber Security

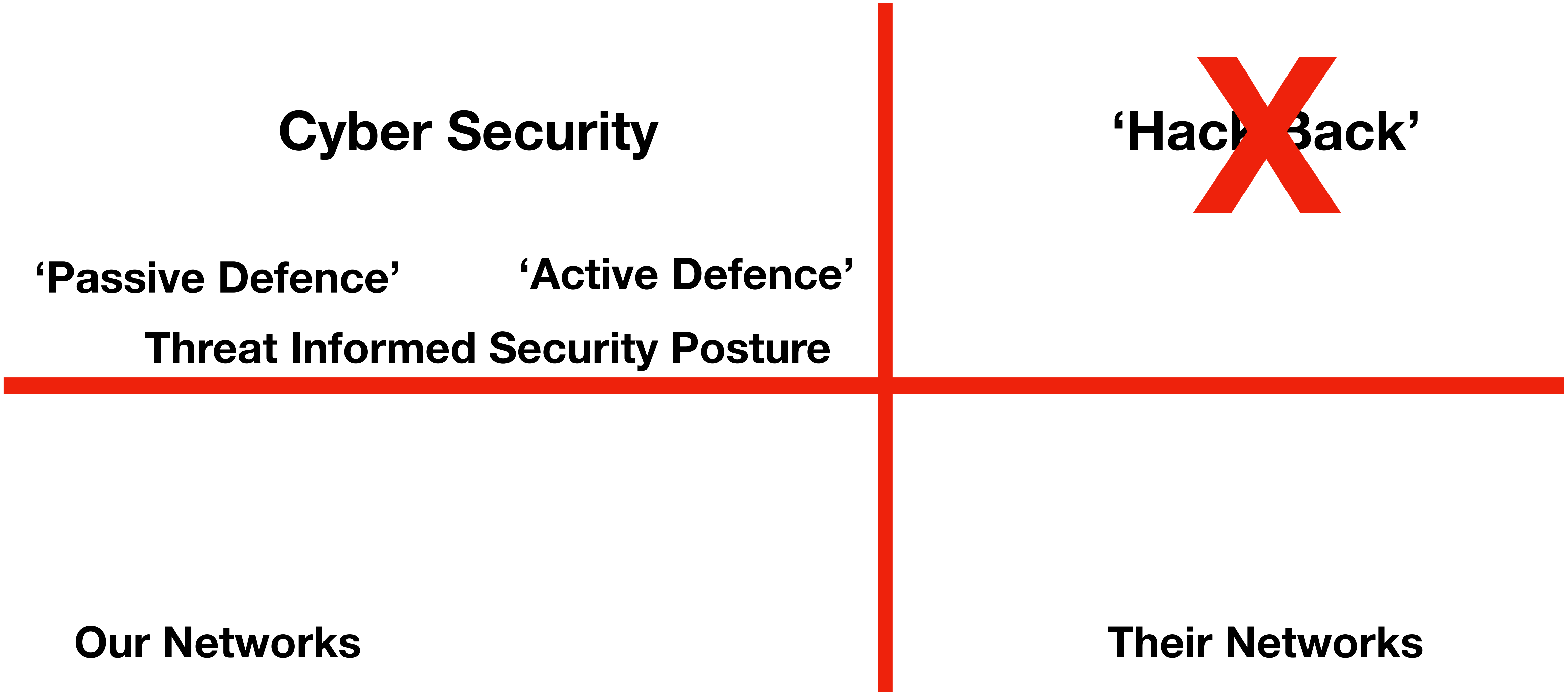
Incident Management (inc Response)

Cyber Resilience

Active & Passive Defence

NIST Lifecycle: Identify, Protect, Detect, Respond, Recover

Current View of Cyber Defence Ops Spectrum



Cyber Security

'Hack Back'

'Passive Defence'

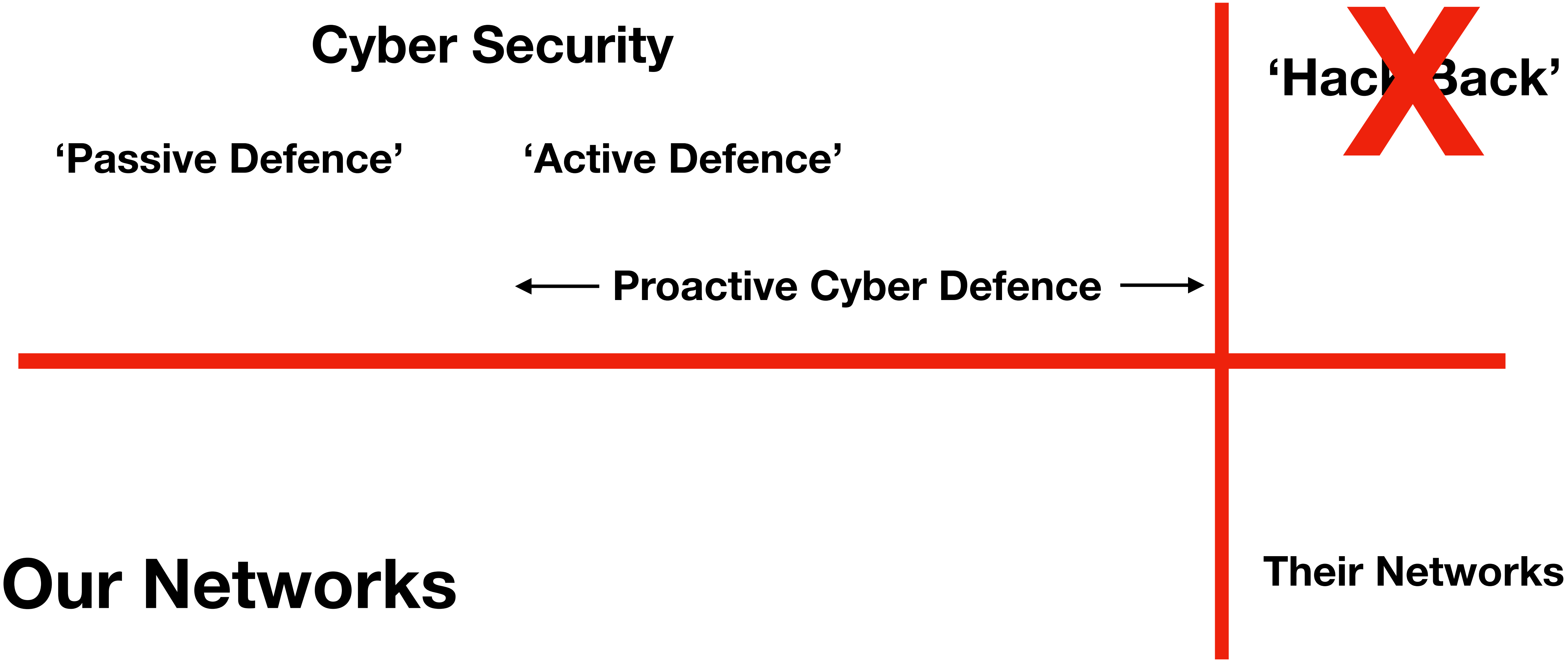
'Active Defence'

Threat Informed Security Posture

Our Networks

Their Networks

Cyber Defence Ops Spectrum



Cyber Security

‘Passive Defence’

‘Active Defence’

← Proactive Cyber Defence →

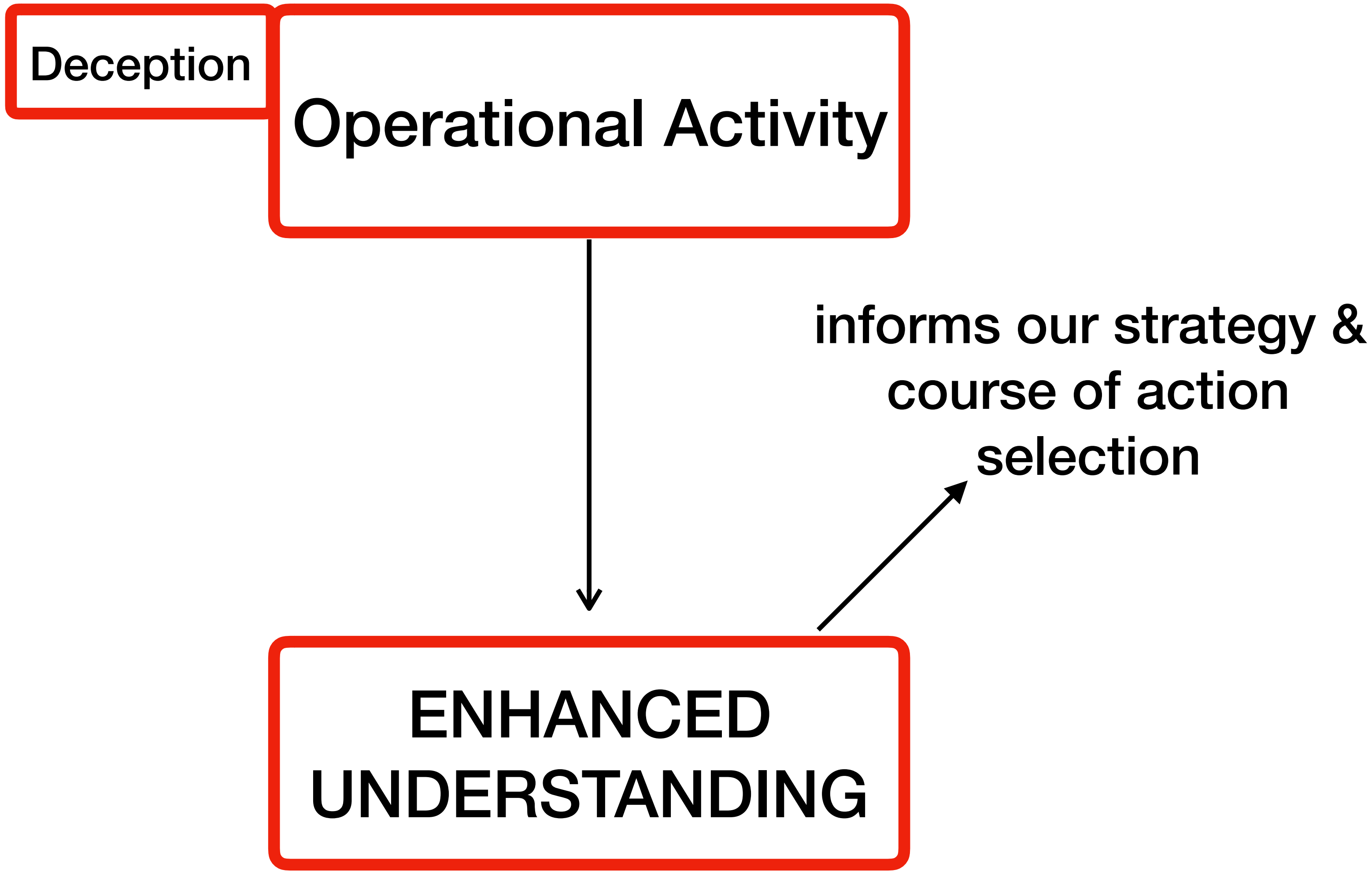
‘Hack Back’

Our Networks

Their Networks

Intelligence vs Warfighting

Intelligence Operations



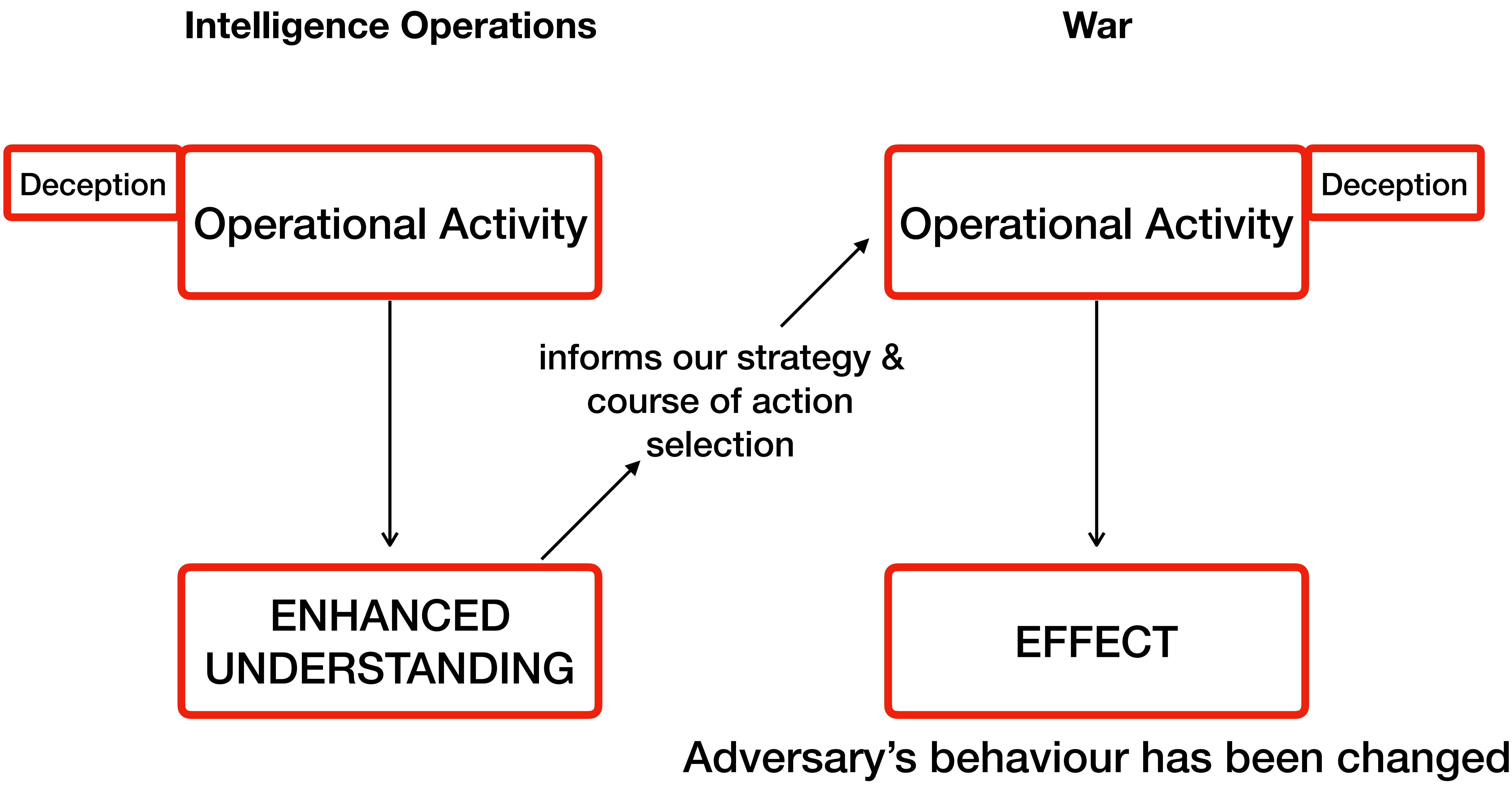
Deception

Operational Activity

informs our strategy & course of action selection

ENHANCED UNDERSTANDING

Intelligence vs Warfighting



Intelligence Operations

War

Deception

Operational Activity

ENHANCED UNDERSTANDING

informs our strategy & course of action selection

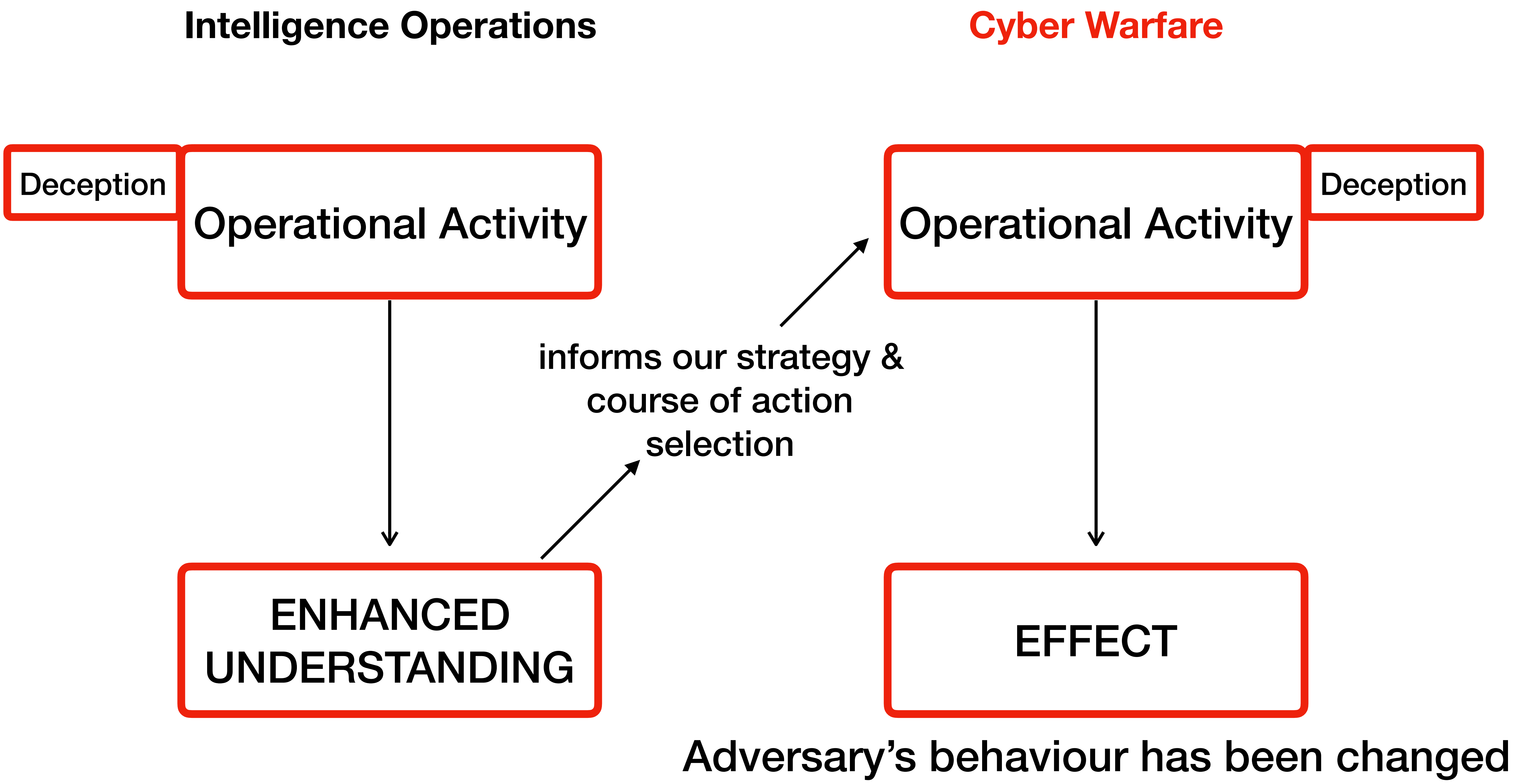
Operational Activity

Deception

EFFECT

Adversary’s behaviour has been changed

Adversarial Behaviour Change in Proactive Cyber Defence



Intelligence Operations

Cyber Warfare

Deception

Operational Activity

ENHANCED UNDERSTANDING

informs our strategy & course of action selection

Operational Activity

Deception

EFFECT

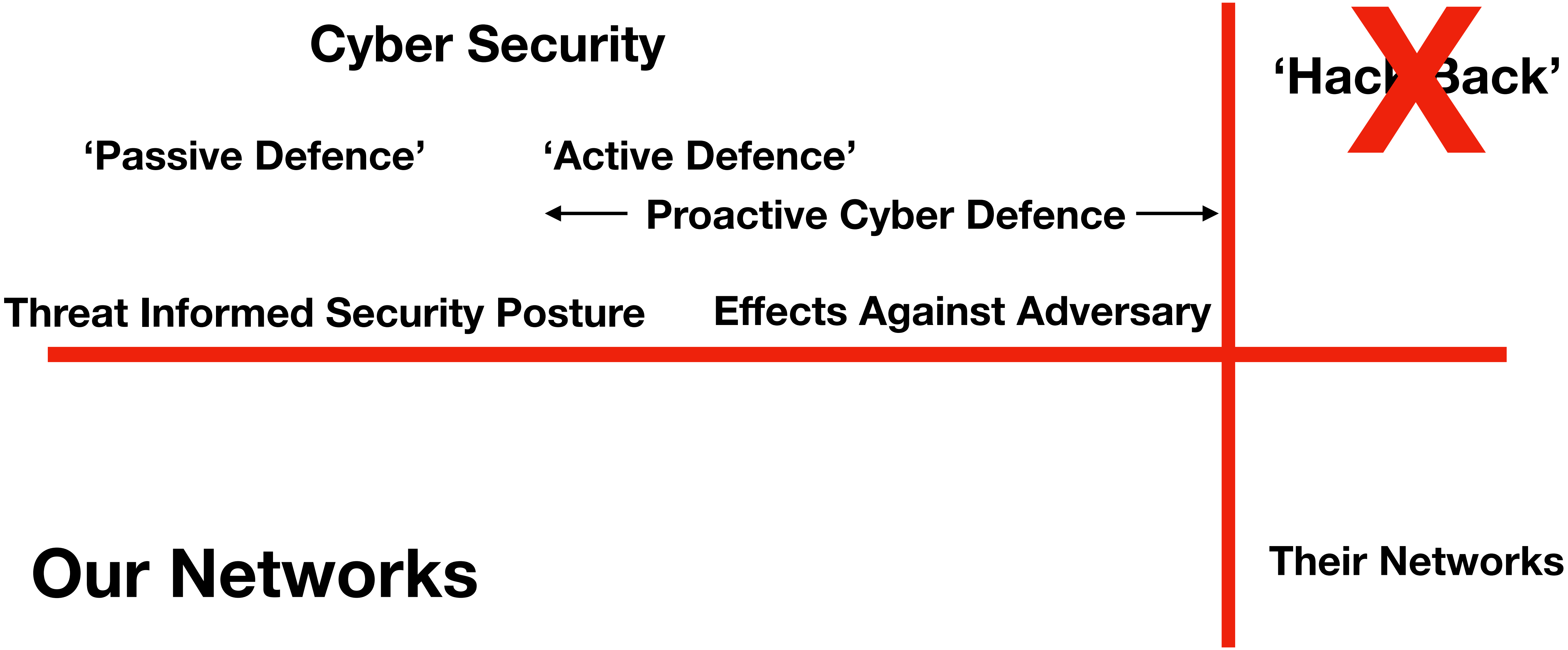
Adversary’s behaviour has been changed

Manipulating the Enemy's Sensemaking

- What's going on?
- What does it mean?
- What should I do about it?

Manipulating their reality

Cyber Defence Ops Spectrum



Cyber Security

‘Hack Back’

‘Passive Defence’

‘Active Defence’

Proactive Cyber Defence

Threat Informed Security Posture

Effects Against Adversary

Our Networks

Their Networks

What is the NCDL?

National
Cyber
Deception
Laboratory
cyberdeception.org.uk

NCDL Mission Statement

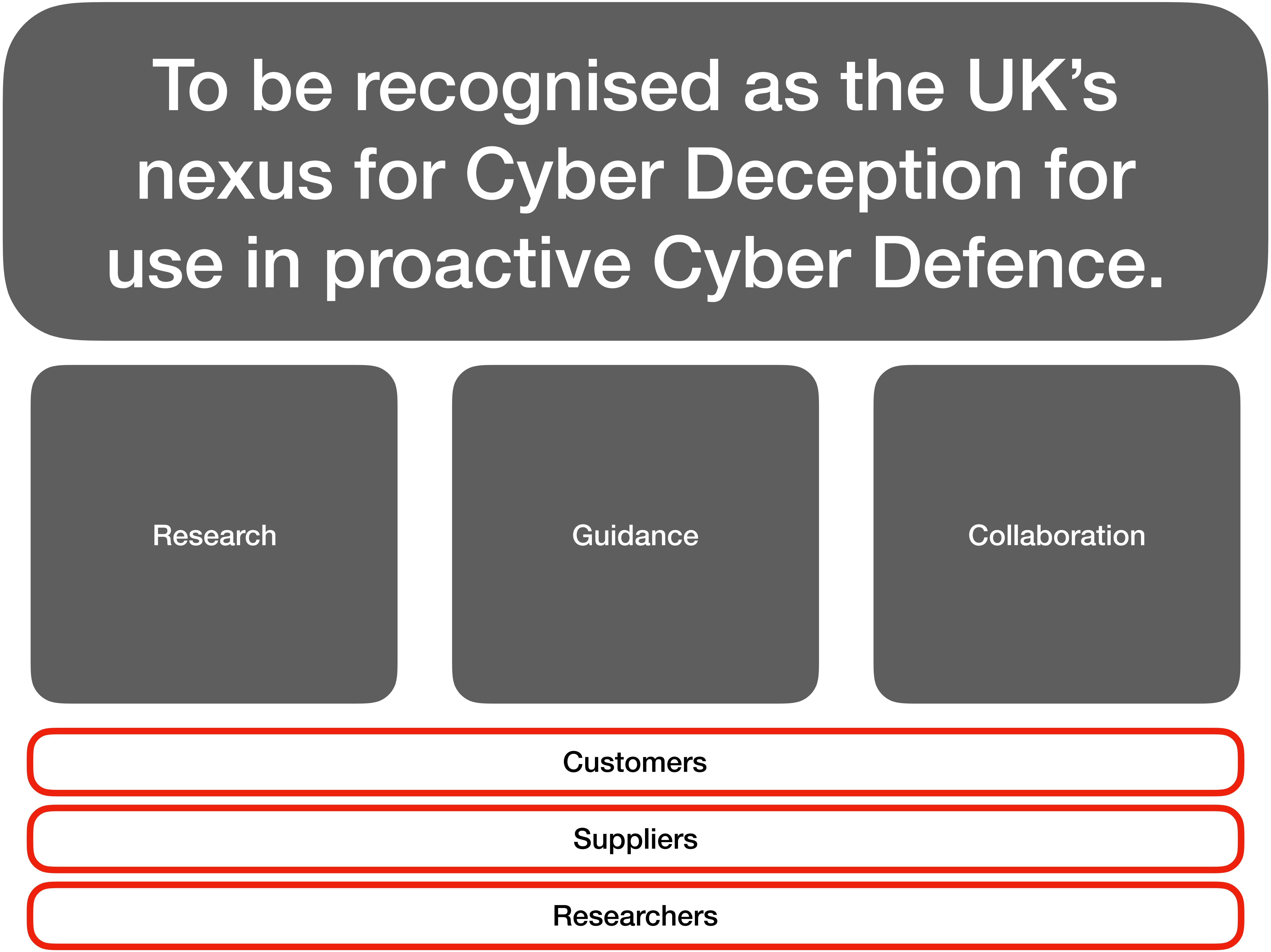
To be recognised as the UK's nexus for Cyber Deception for use in proactive Cyber Defence.

To be recognised as the UK's nexus for Cyber Deception for use in proactive Cyber Defence.

Research

Guidance

Collaboration



To be recognised as the UK's nexus for Cyber Deception for use in proactive Cyber Defence.

Research

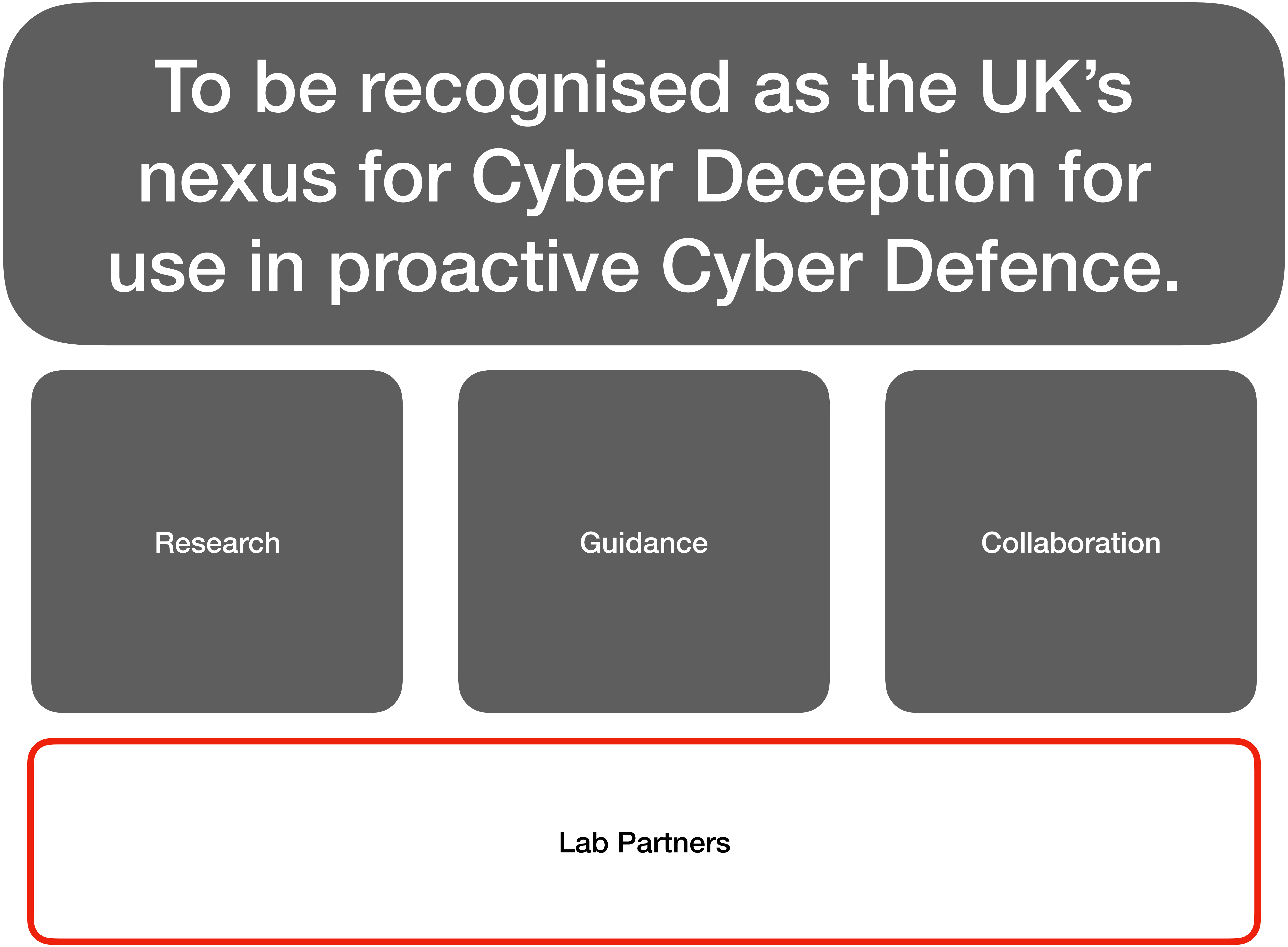
Guidance

Collaboration

Customers

Suppliers

Researchers



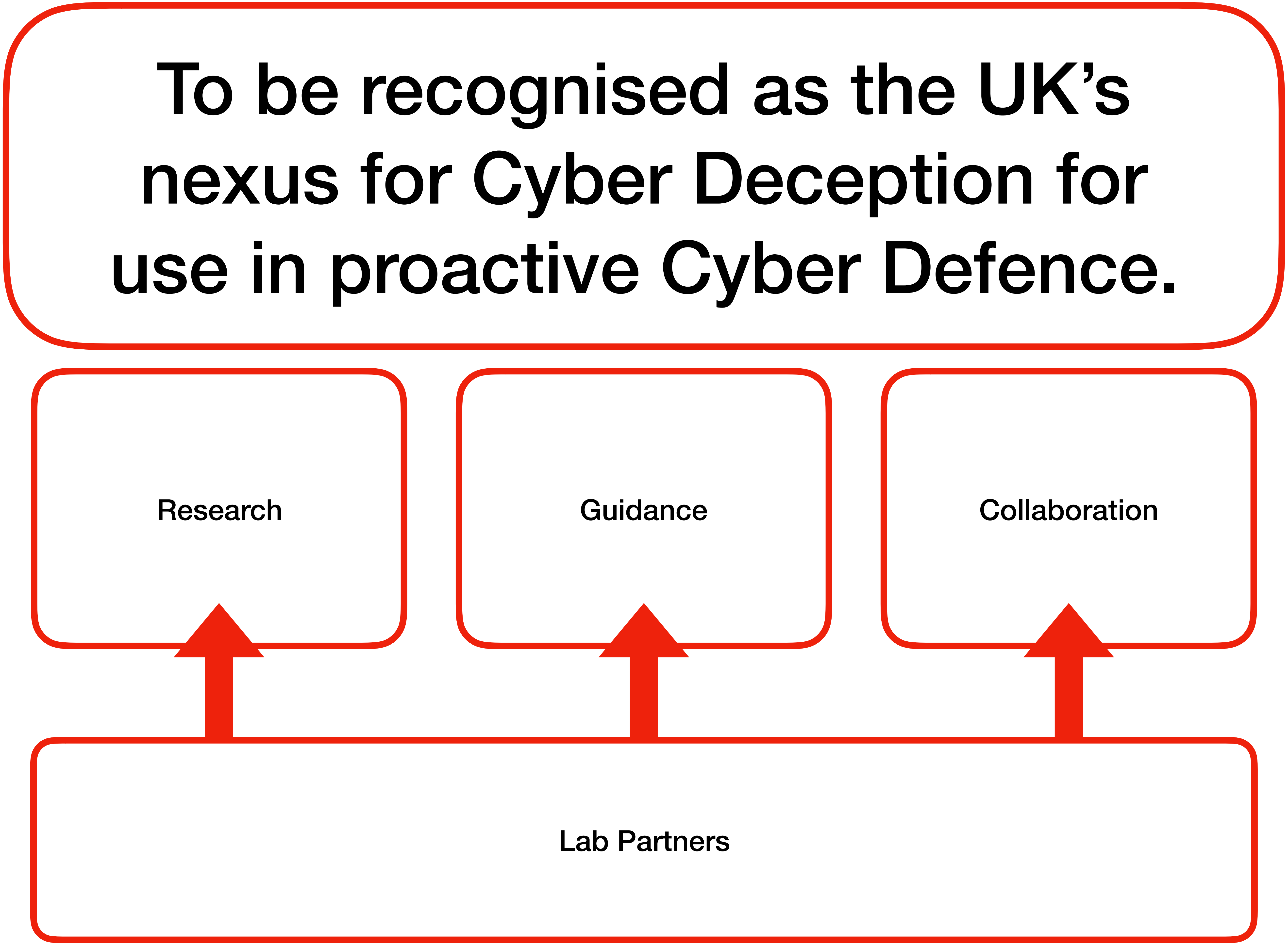
To be recognised as the UK’s nexus for Cyber Deception for use in proactive Cyber Defence.

Research

Guidance

Collaboration

Lab Partners



To be recognised as the UK's nexus for Cyber Deception for use in proactive Cyber Defence.

Research

Guidance

Collaboration

Lab Partners

Ministry of Defence

[dstl]

National Cyber Security Centre

CounterCraft

Aves netsec

Attivo NETWORKS

IMMERSIVELABS

VERTICAL KNOWLEDGE
ACTIONABLE INSIGHT

ACALVIO

artifice

ROKE

BAE SYSTEMS

THALES

FireEye™

GLOBAL CYBER ALLIANCE.

BU
Bournemouth University

Cranfield University

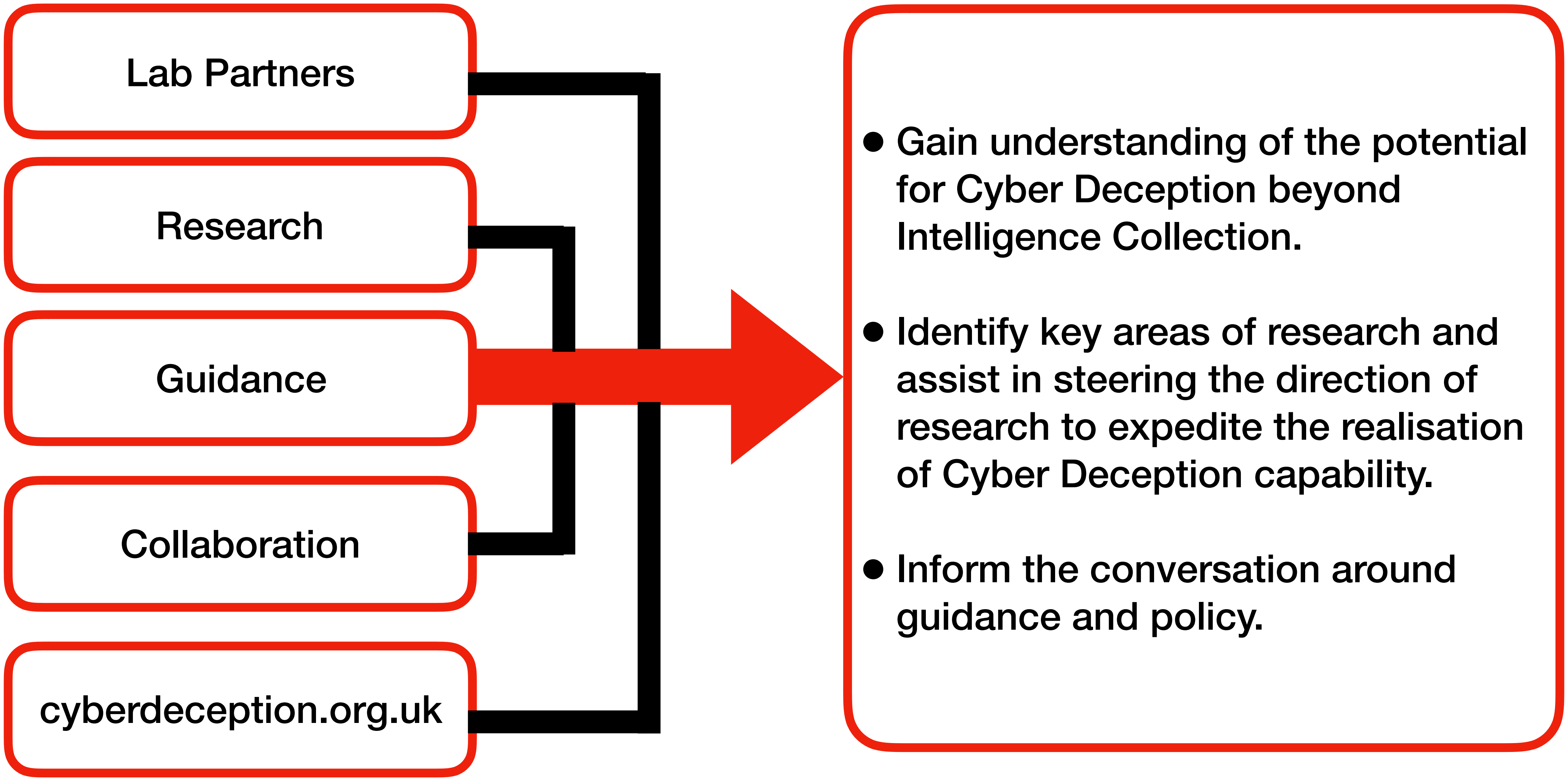
OIS

UEA
University of East Anglia

UNIVERSITY OF PORTSMOUTH

MACQUARIE University
SYDNEY·AUSTRALIA

DEAKIN UNIVERSITY



Lab Partners

Research

Guidance

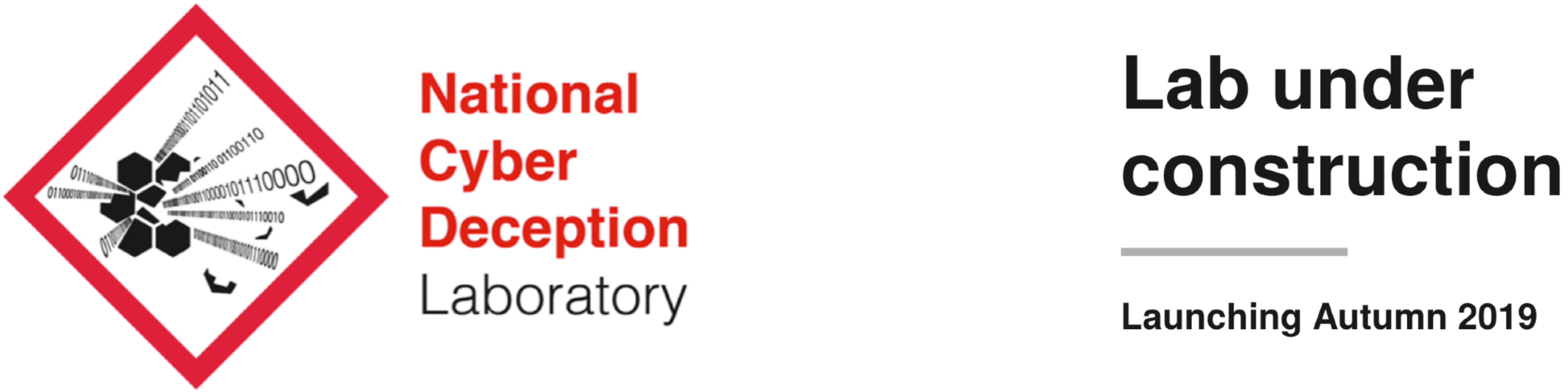
Collaboration

cyberdeception.org.uk

- Gain understanding of the potential for Cyber Deception beyond Intelligence Collection.
- Identify key areas of research and assist in steering the direction of research to expedite the realisation of Cyber Deception capability.
- Inform the conversation around guidance and policy.

How will the NCDL deliver?

cyberdeception.org.uk



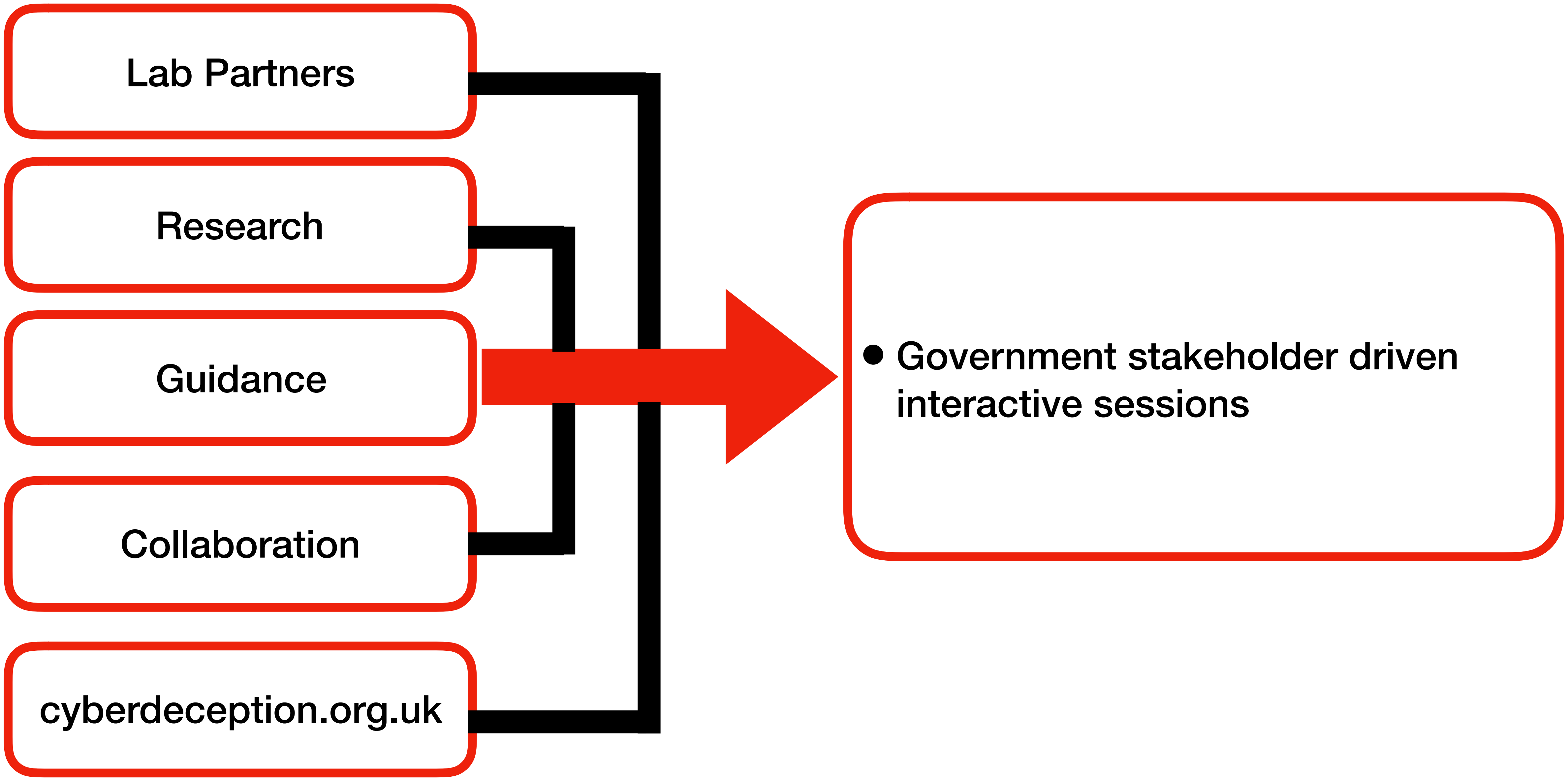
National Cyber Deception Laboratory

Lab under construction

Launching Autumn 2019

- Primary portal into the lab community.
- Opportunity for Lab Partners to publish current research objectives and findings.
- Links to live research, opportunities to contribute to experiments.
- Future intent is to house and curate a peer reviewed e-journal for Cyber Deception.

GOAL to become the nexus for Cyber Deception in proactive cyber defence



Lab Partners

Research

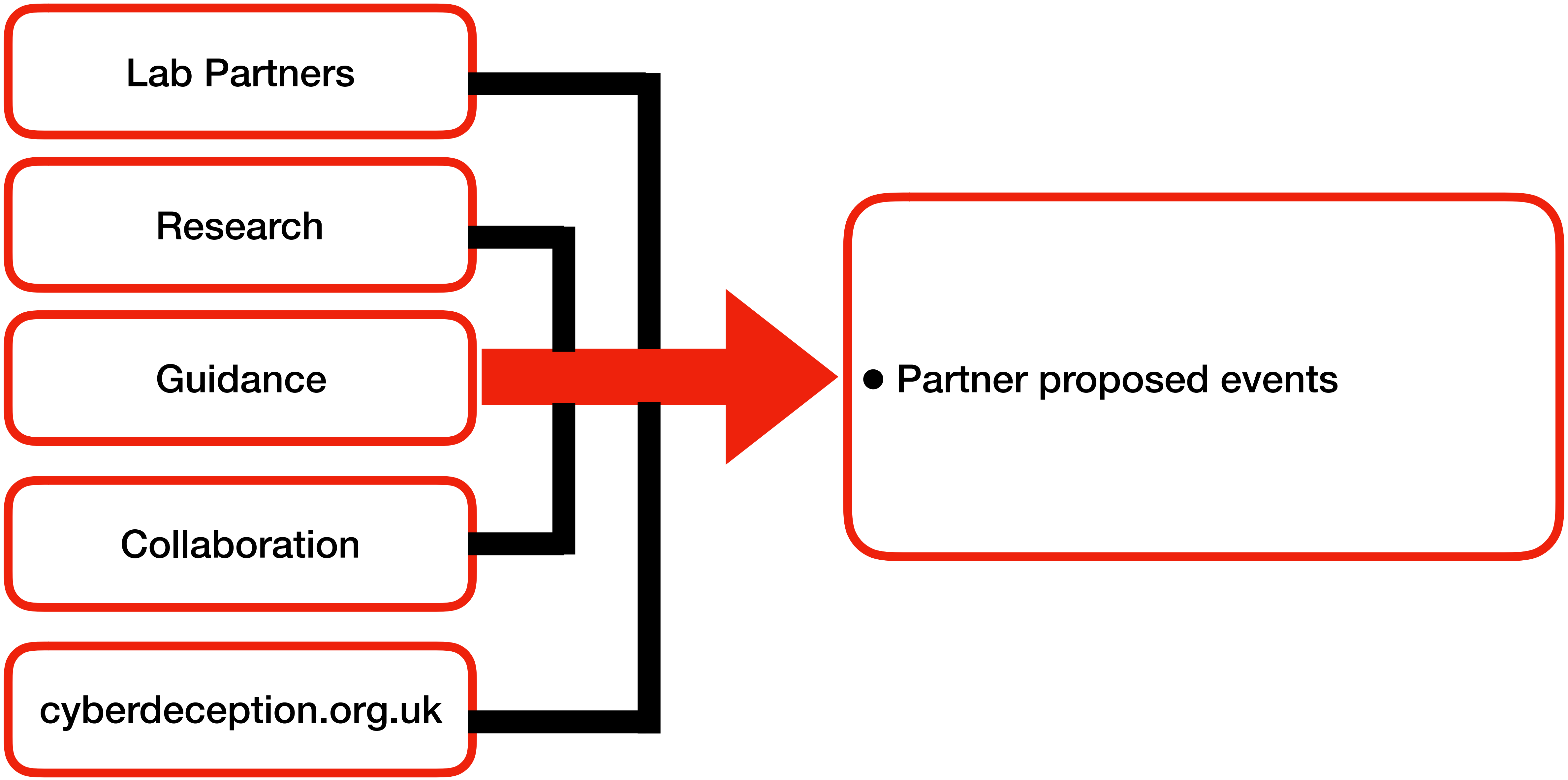
Guidance

Collaboration

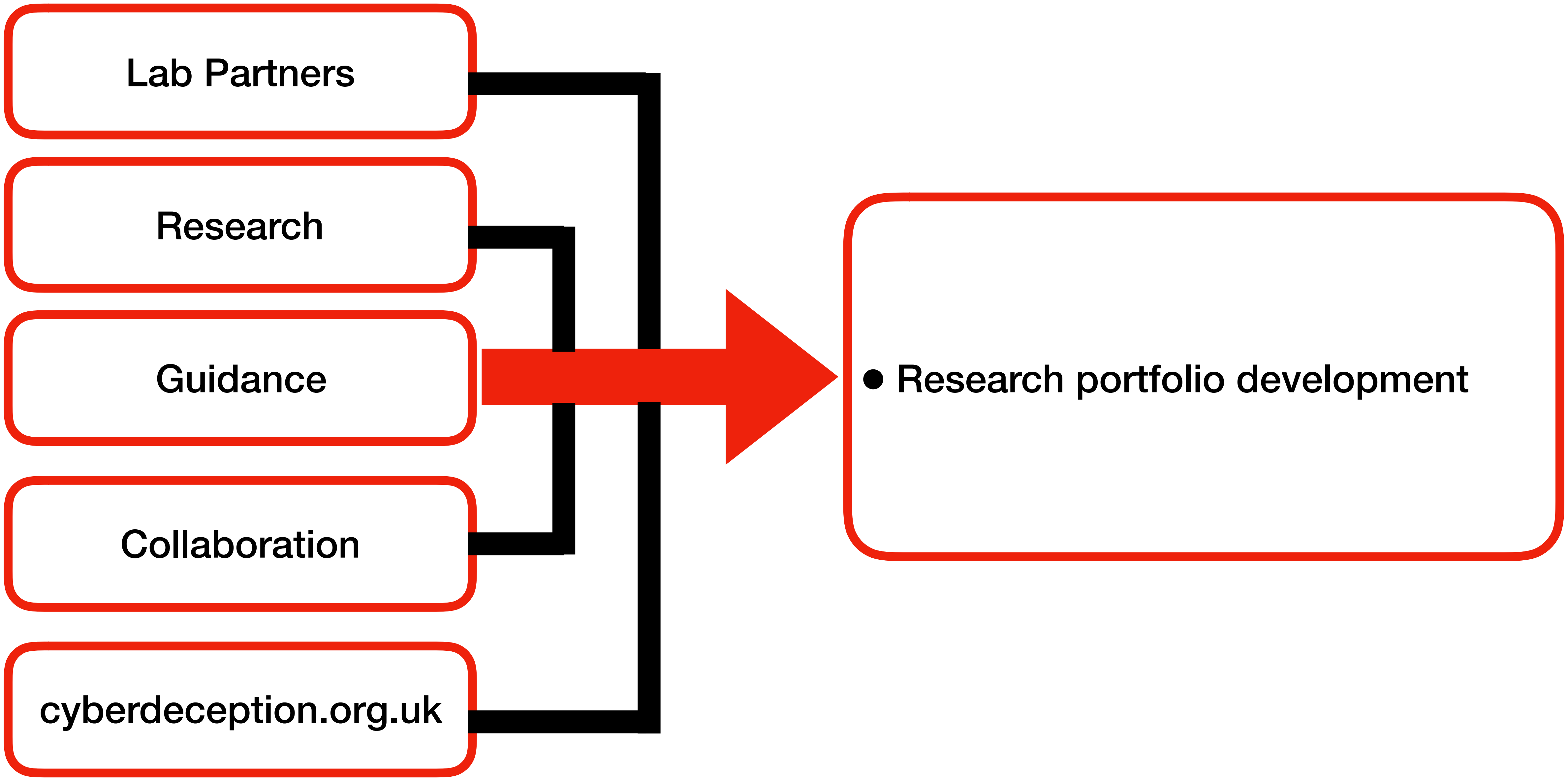
cyberdeception.org.uk

- Government stakeholder driven interactive sessions

GOAL to become the nexus for Cyber Deception in proactive cyber defence



GOAL to become the nexus for Cyber Deception in proactive cyber defence



Lab Partners

Research

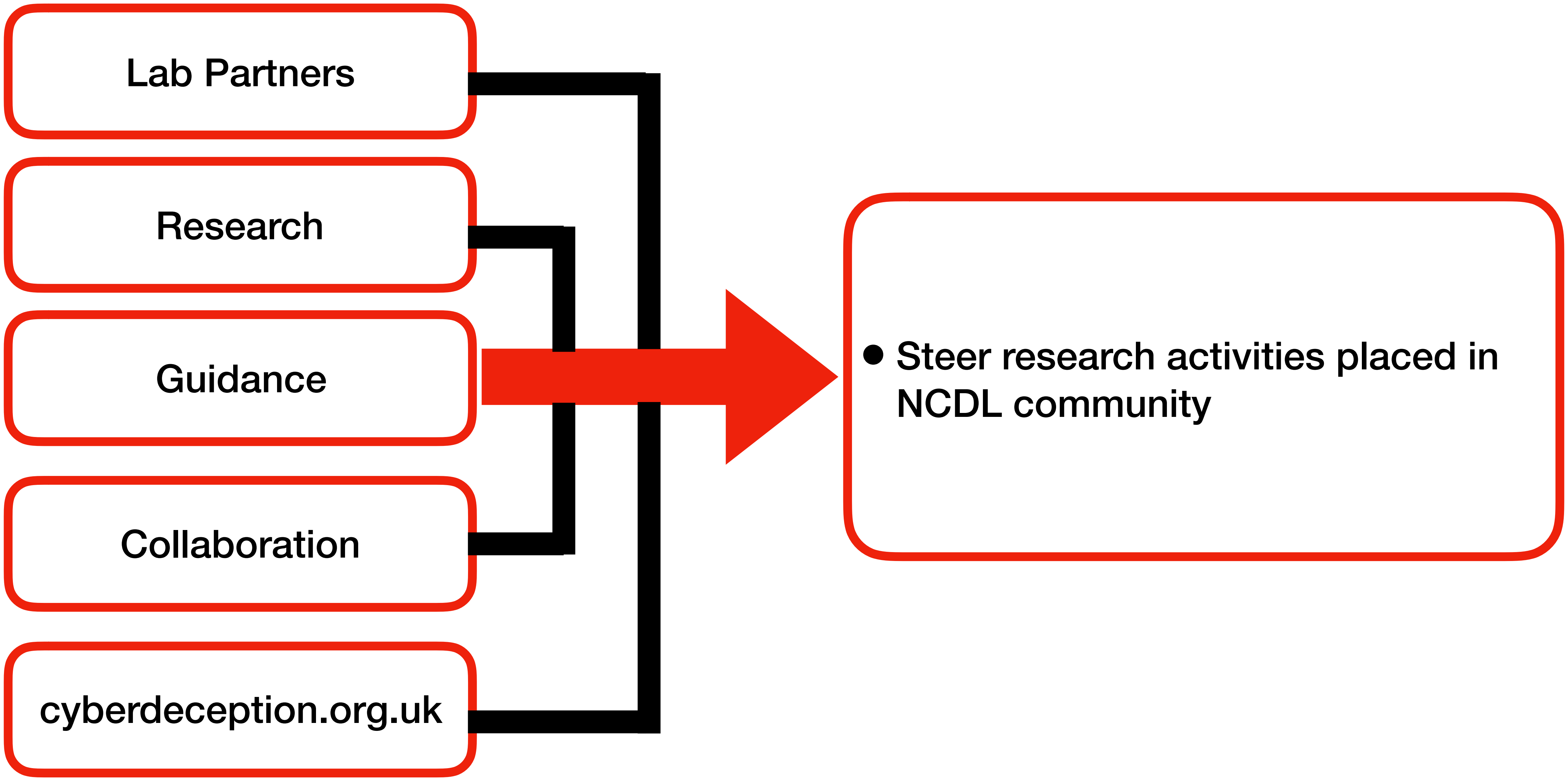
Guidance

Collaboration

cyberdeception.org.uk

- Research portfolio development

GOAL to become the nexus for Cyber Deception in proactive cyber defence



Lab Partners

Research

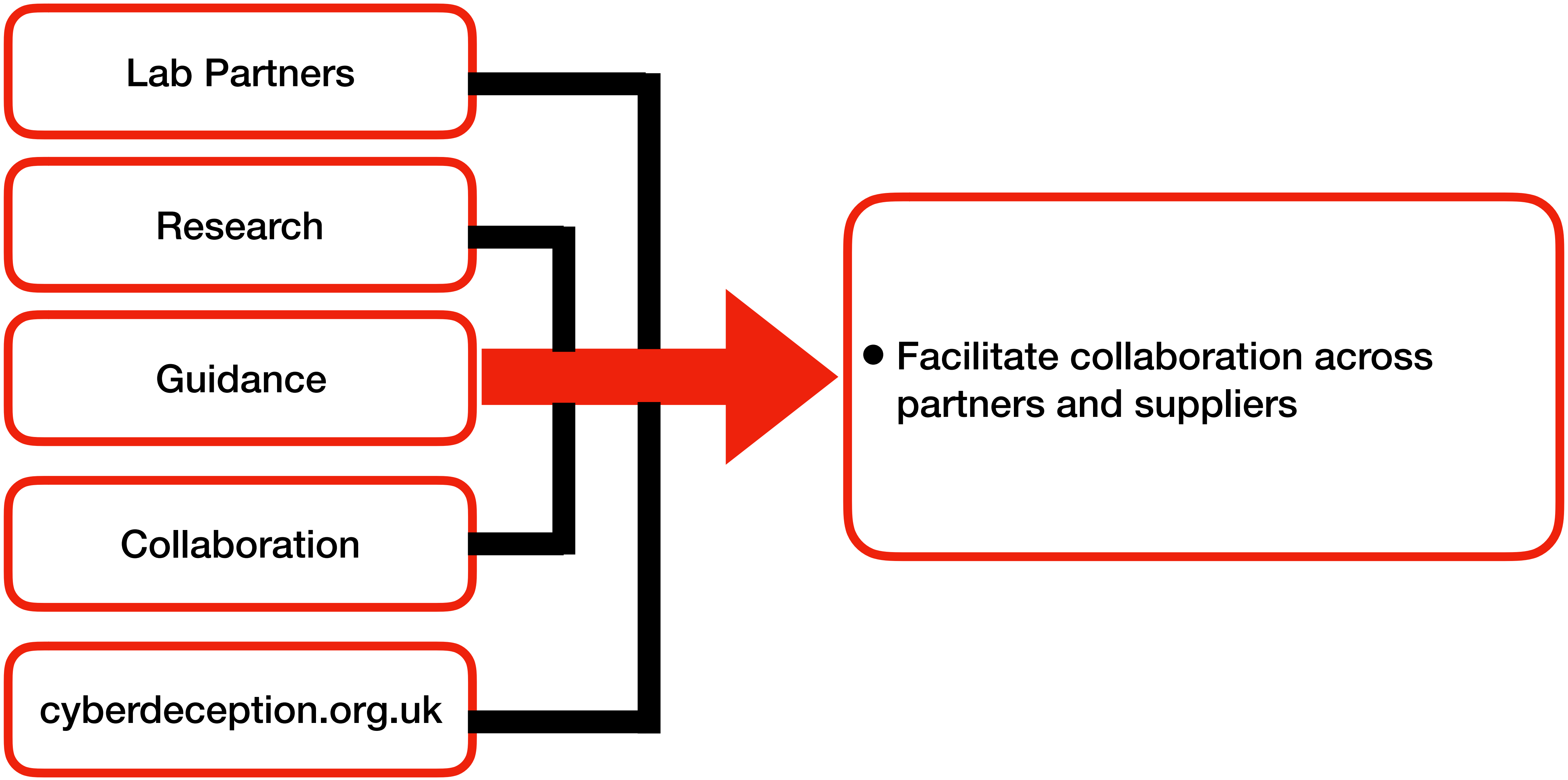
Guidance

Collaboration

cyberdeception.org.uk

- Steer research activities placed in NCDL community

GOAL to become the nexus for Cyber Deception in proactive cyber defence



Lab Partners

Research

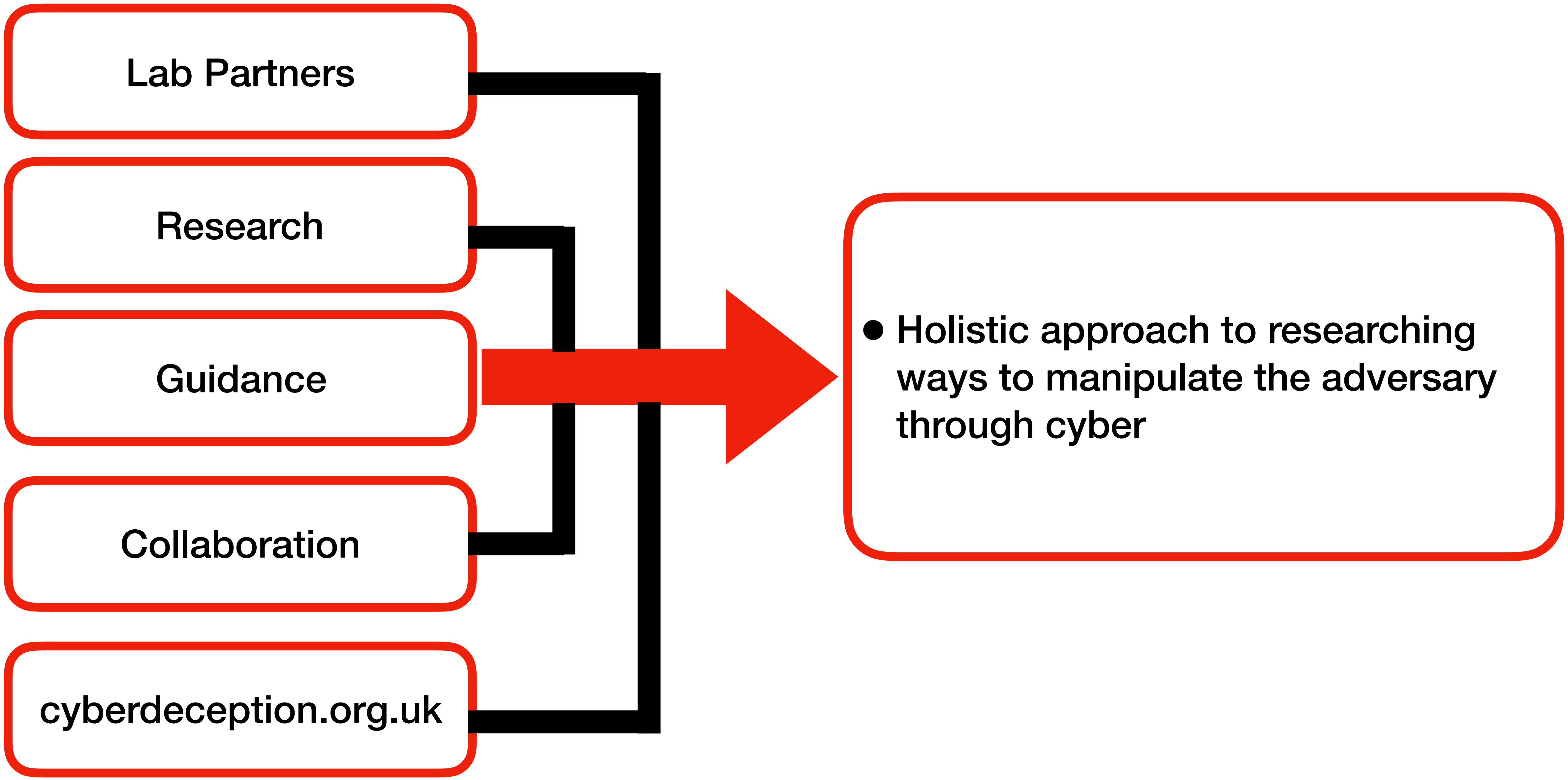
Guidance

Collaboration

cyberdeception.org.uk

- Facilitate collaboration across partners and suppliers

GOAL to become the nexus for Cyber Deception in proactive cyber defence



- Holistic approach to researching ways to manipulate the adversary through cyber

Some Upcoming Events

- 1 Day Event - “Legalities of Cyber Deception” (late FY19/20)
- 1 Day Event - “What is a Defensive Payload?” (early FY20/21)
- 1 Day Event - “Deception in the Cyber Supply Chain” (FY20/21)
- National Cyber Deception Symposium (October 2020)

info@cyberdeception.org.uk

Warfare in the Information Age

- The need to defend against the unprecedented
- The reality of likely defeat when defending of our home territory
- The need to change the rules of combat and to realise the costs and sacrifices that cannot be avoided in our attempts to fight back within our home territory

This is the real ‘Warfare in the Information Age’

Thoughts for Today

- Adversarial Behaviour Change without the traditional reliance on kinetic force
- Cyber domain provides a new dimension through which to shape adversary’s sensemaking
- Cyber capabilities not tied to traditional physical considerations
- Virtual violence in network defence
- Our own networks become a killing ground for our attackers

NCDL to pioneer efforts to manipulate our adversaries’ behaviour in the home territory of our networks

National
Cyber
Deception
Laboratory
cyberdeception.org.uk

Questions?

info@cyberdeception.org.uk

Closing Remarks

- Digitally Based Warfare
- Warfare in Our Home Territory
- Turning Our Networks into Digital Killing Grounds
- Warfare is about achieving outcomes (at a cost) rather than not getting caught
- Cyber provides opportunities to manipulate attacker’s reality
- Virtual violence in network defence
- This the real ‘Robot Wars’ for grown-ups

Thanks to Our Sponsors

FIREEYE™

BAE SYSTEMS

VERTICAL KNOWLEDGE
ACTIONABLE INSIGHT

Counter
Craft

National
Cyber
Deception
Laboratory
cyberdeception.org.uk

See you at Cyber Deception 2020!

cyberdeception.org.uk