Back to the Future

Cyber Intelligence and Counterintelligence

Brett van Niekerk

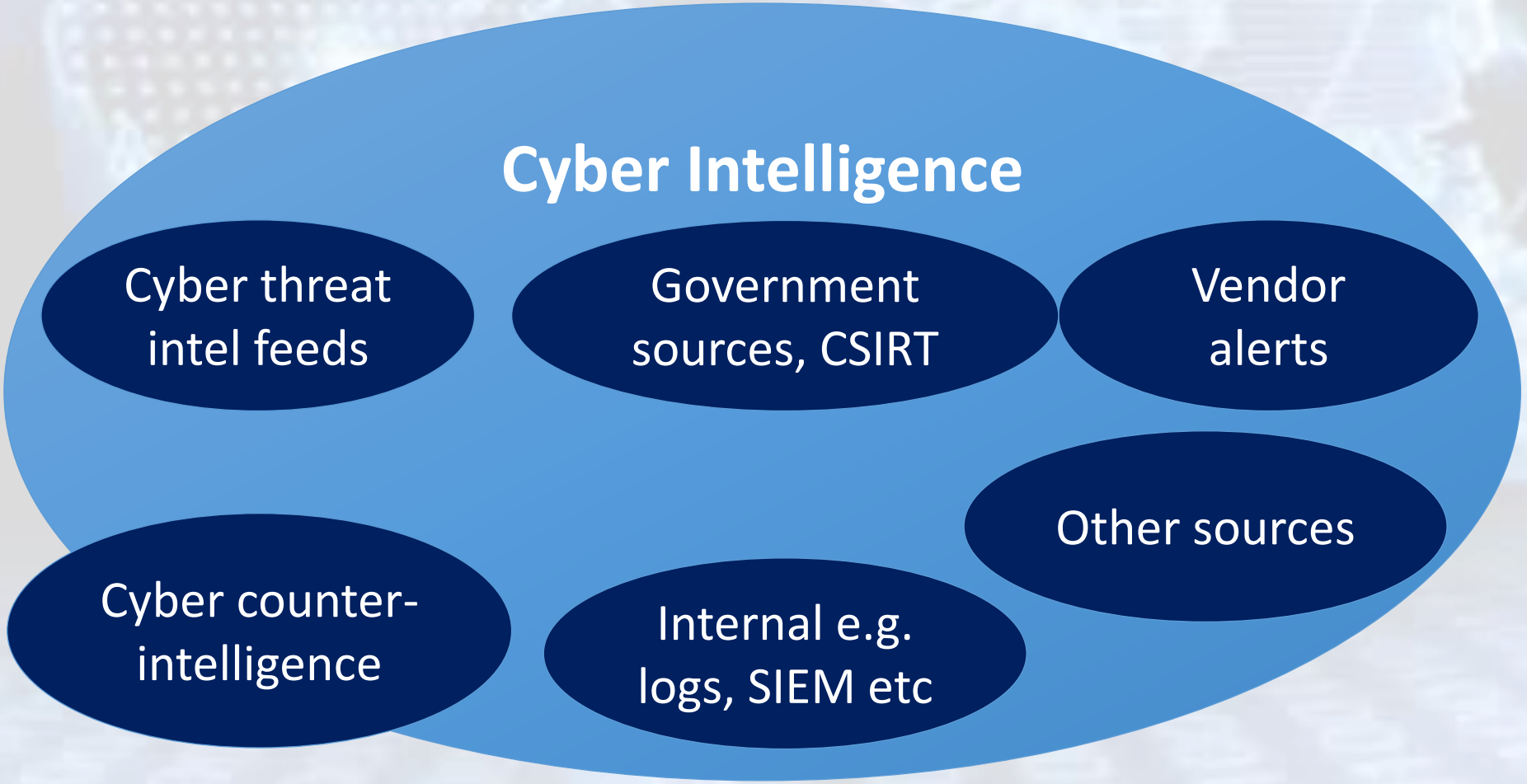
Petrus “Beer” Duvenage

ISACA®
Trust in, and value from, information systems
South Africa Chapter

MISCONCEPTIONS

- Myth #1: Cyber intelligence is only about threat feeds
- Myth #2: Cyber intelligence is only about the consumption of information
- Myth #3: Cyber intelligence is cyber espionage
- Myth #4: You need to get the security basics right first

SO THEN WHAT IS CYBER INTELLIGENCE?



SO THEN WHAT IS CYBER INTELLIGENCE?

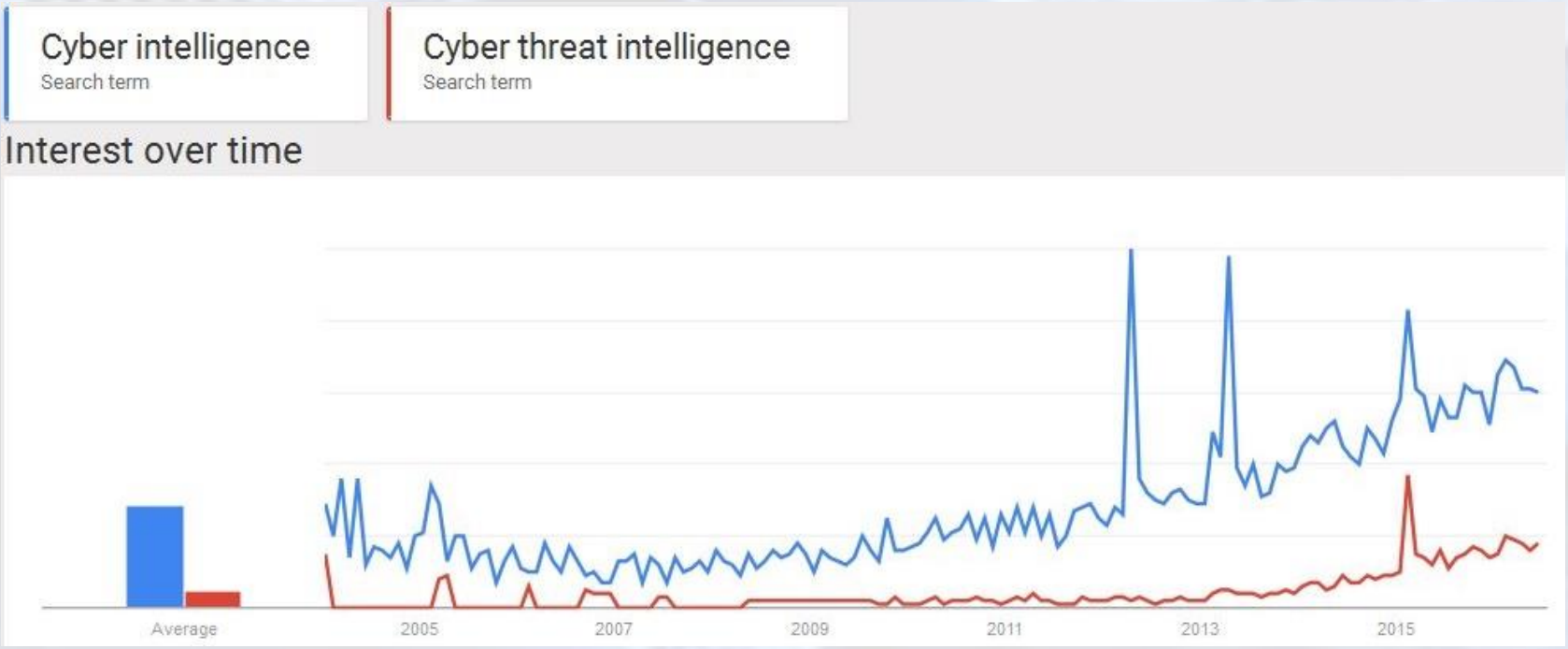
- **Cyber Intelligence is about analysis, not the source of data**
  - Examples:
    - Human Intelligence (HUMINT) – human source
    - Signals Intelligence (SIGINT) – signal source
  - Source is important, but does not define it
  - Needs to be **actionable**
  - Refer to Myths #1 & #2

LEVELS OF INTELLIGENCE

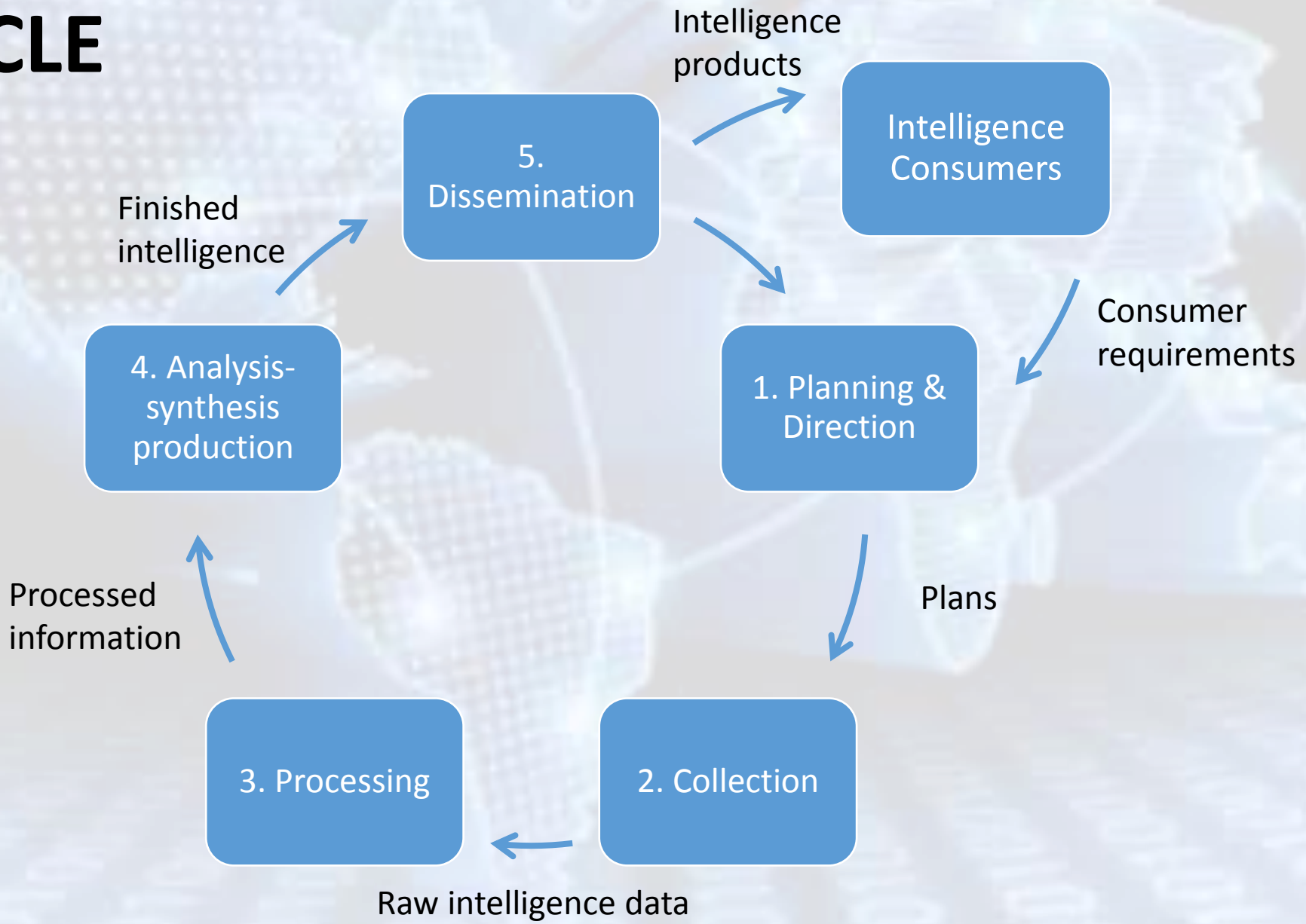
	Strategic	Operational	Tactical
Scope	General	Industry sector	Company - internal
Focus	Political, social, behavioral	Adversary campaigns	In the network
Audience	C-level	Executive management	Sec Ops / response
Purpose	Maintain competitive advantage	Avoid disruption	Remediate / recover
Posture	Proactive	Proactive	Reactive
Time frame	Far	Near	Immediate
Types of intel	Estimative, general, scientific & technical	Warning & counter-intelligence	Current intelligence
Nature	Non-technical, contextual indicators, defence-in-depth approach		Technologies (IDS, SIEM etc)
Sharing	Public/private partnerships / Cyber security hub		Automated (e.g. feeds – STIX, TAXII, IOC)
Decisions	Driven by company strategy	Driven by risk-based resource allocation	Driven by restoration / evidence collection

Intelligence and National Security Alliance, *Operational Cyber Intelligence*

THE PREVALENCE OF CYBER INTELLIGENCE

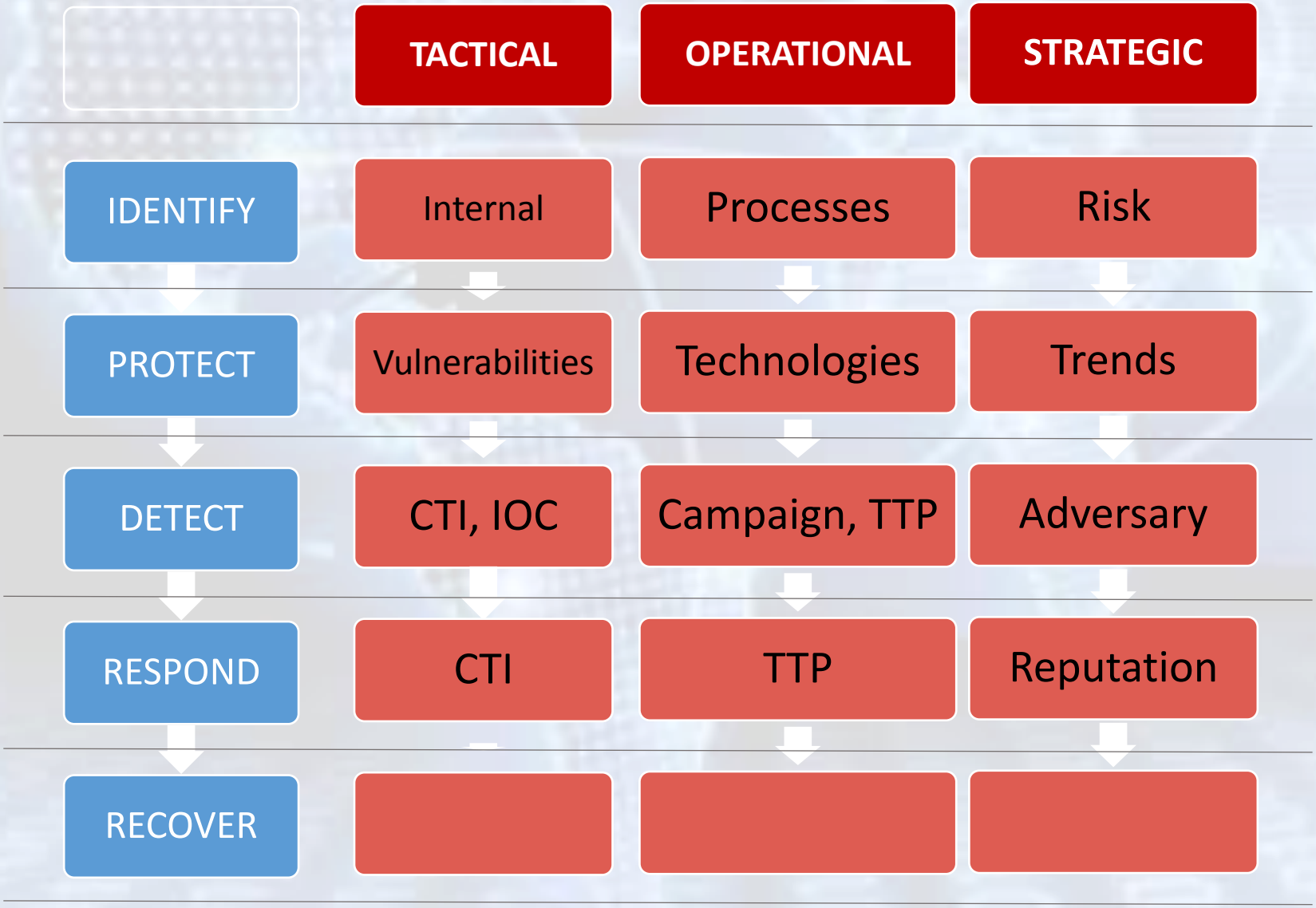


THE INTELLIGENCE CYCLE



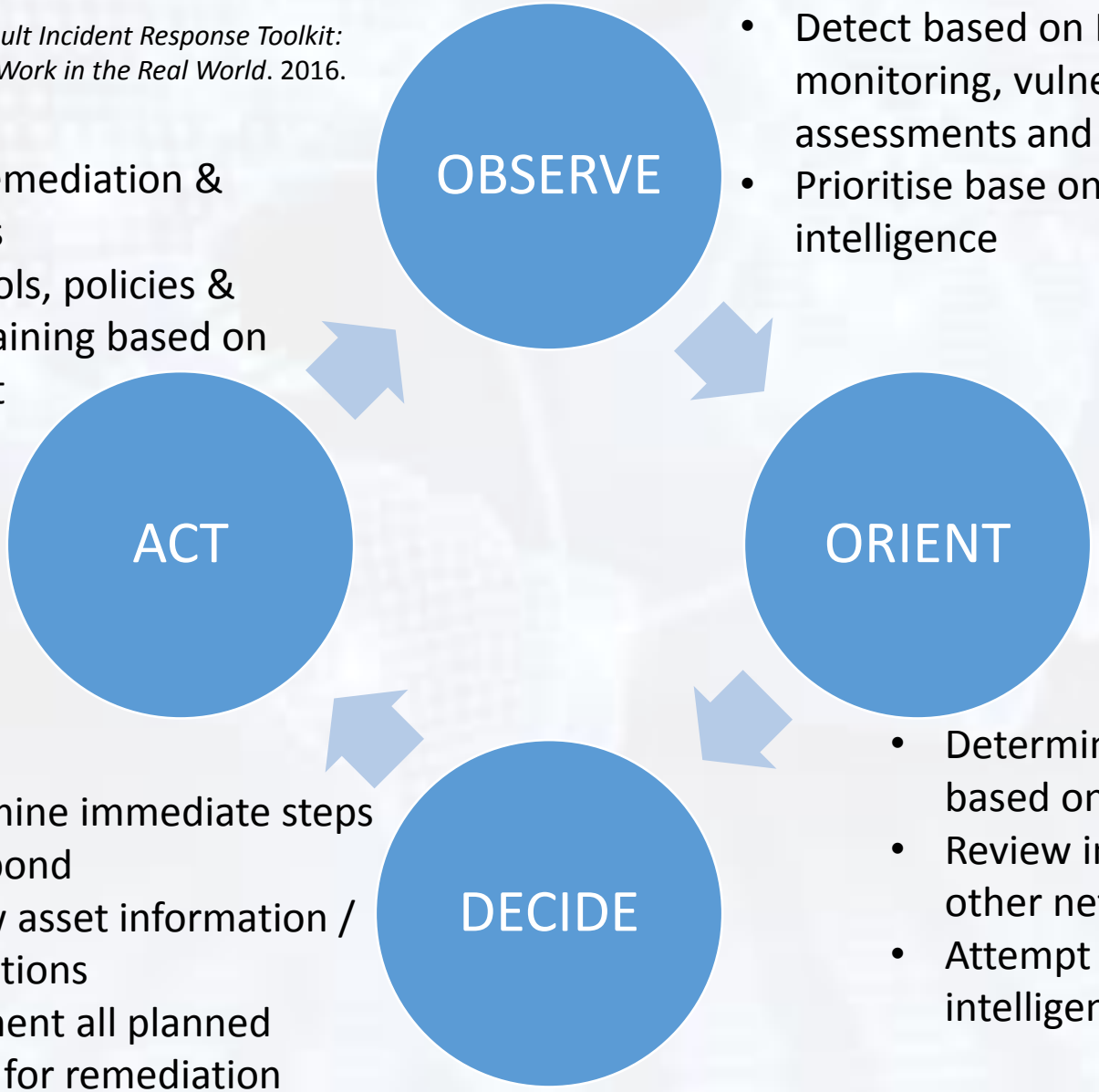
Edward Waltz. *Knowledge Management in the Intelligence Enterprise*. Artech House: Boston & London. 2003.

CYBER INTELLIGENCE: NIST CSF



CYBER INTELLIGENCE: OODA

Adapted from: *The AlienVault Incident Response Toolkit: Putting the OODA Loop to Work in the Real World*. 2016.



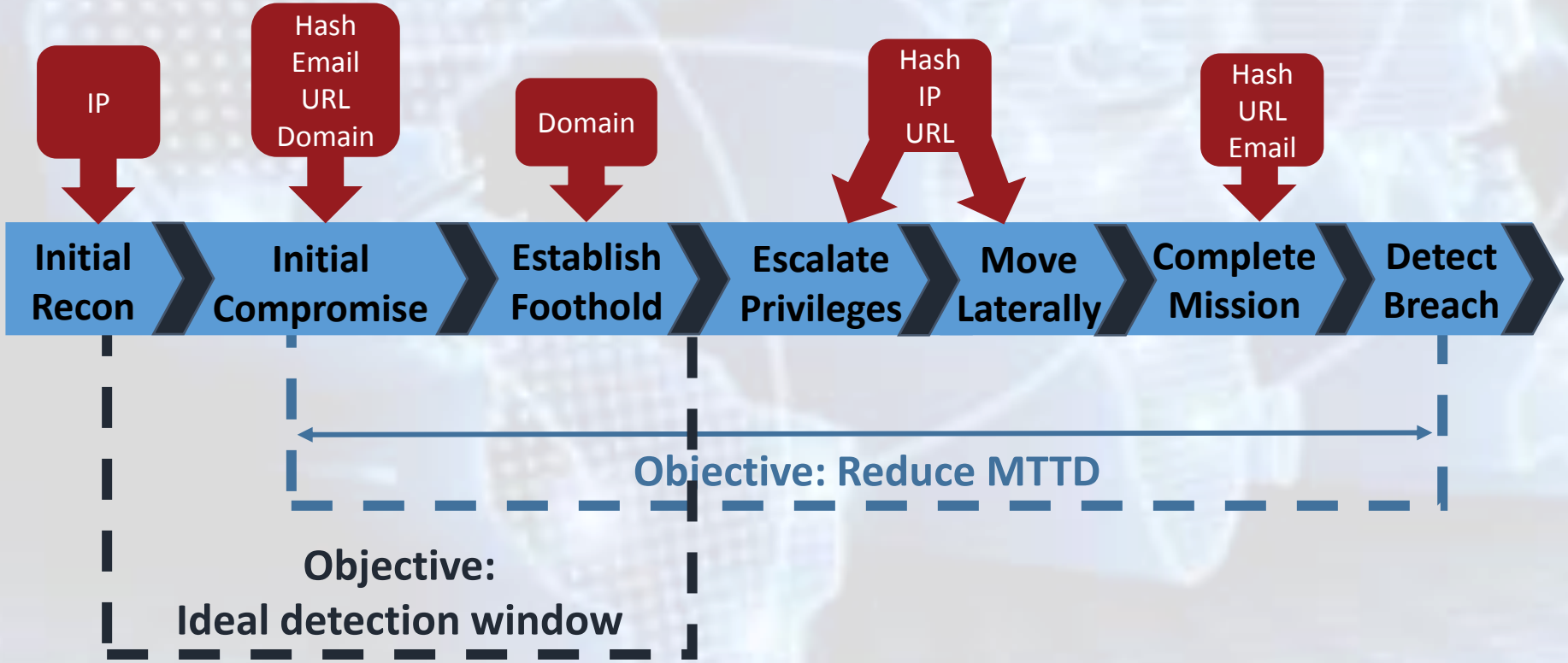
- Detect based on IOCs, behavioural monitoring, vulnerability assessments and SIEM
- Prioritise base on threat intelligence

- Determine scope/impact based on threat intel
- Review in context of other network activity
- Attempt attribution / intelligence gathering

- Determine immediate steps to respond
- Review asset information / instructions
- Document all planned tactics for remediation

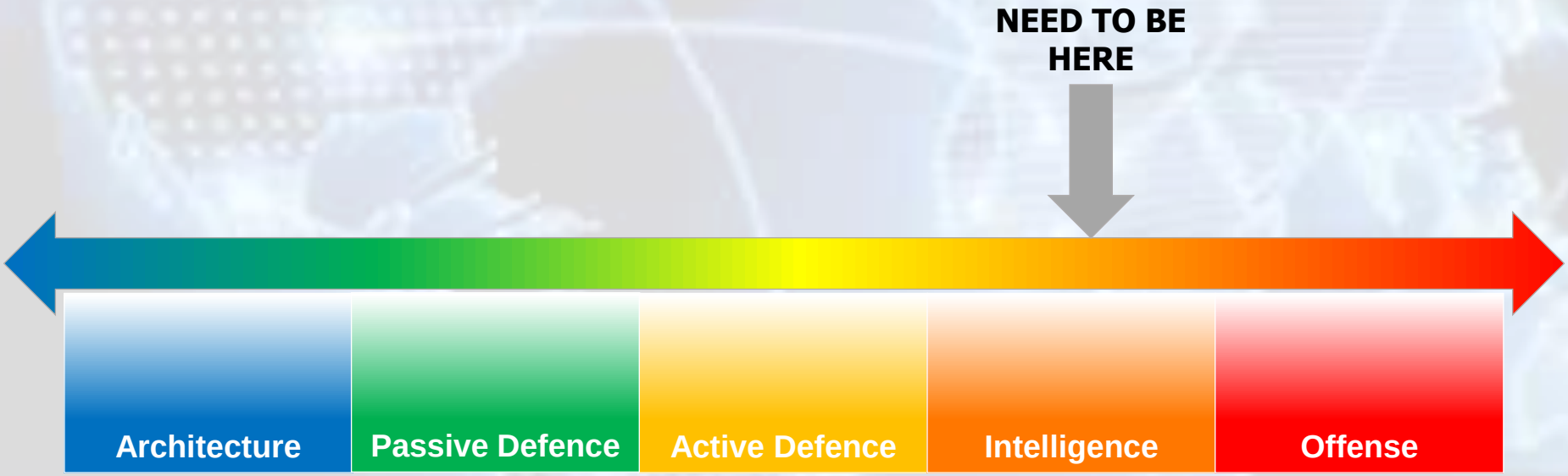
- Implement remediation & verify success
- Review controls, policies & awareness training based on lessons learnt

CTI APPLICATION TO THE KILL CHAIN



Adapted from: Mark Seward. *Addressing the New Threat Intelligence Problems of Scale and Relevance*. Anomali/Dark Reading/UBM Webinar. 2016.

CYBER INTELLIGENCE MATURITY



Architecture	Passive Defence	Active Defence	Intelligence	Offense
The planning, establishing, and upkeep of systems with security in mind	Systems added to the Architecture to provide reliable defence or insight against threats without consistent human interaction	The process of analysts monitoring for, responding to, and learning from adversaries internal to the network	Collecting data, exploiting it into information, and producing Intelligence	Legal countermeasures and self-defence actions against an adversary

Lee, R.M. *The Sliding Scale of Cyber Security*. SANS Institute. 2015.

CYBER INTELLIGENCE MATURITY

Security Operations Maturity Model (HP Enterprise, 2015)

0: Incomplete	Non-existent operational elements
1: Performed	Meet minimum compliance requirements for security monitoring
2: Managed	Repeatable operational tasks, meeting business goals
3: Defined	Well-defined, subjectively evaluated, and flexible operations
4: Measured	Operations are quantitatively evaluated, continuous review & improved
5: Optimizing	Implemented operational improvement program tracking deficiencies and lessons learnt drive improvement

Security Intelligence Maturity Model (LogRhythm, 2015)

0: Blind	1: Minimally compliant	2: Securely compliant	3: Vigilant	4: Resilient

- Capability, organizational characteristics, risk characteristics
- MTTD / MTTR

CYBER COUNTERINTELLIGENCE

- Cyber Intelligence is clearly critical to Information Security governance, risk and assurance in order to address exponentially increasing threats: Kaspersky, Merrill Lynch

  - ✓ In **1994**, a new threat was discovered each **hour**.
  - ✓ In **2006**, a threat was discovered each **minute**.
  - ✓ By **2012**, this had grown to a threat per **second**.
  - ✓ By **2014**, leaped to over **three** per **second**.
  - ✓ In **2015** nearly **seven** per **second**.
  - ✓ Estimated that **70 % undetected**.

Current Information Security Approaches + Cyber Threat Intelligence

=

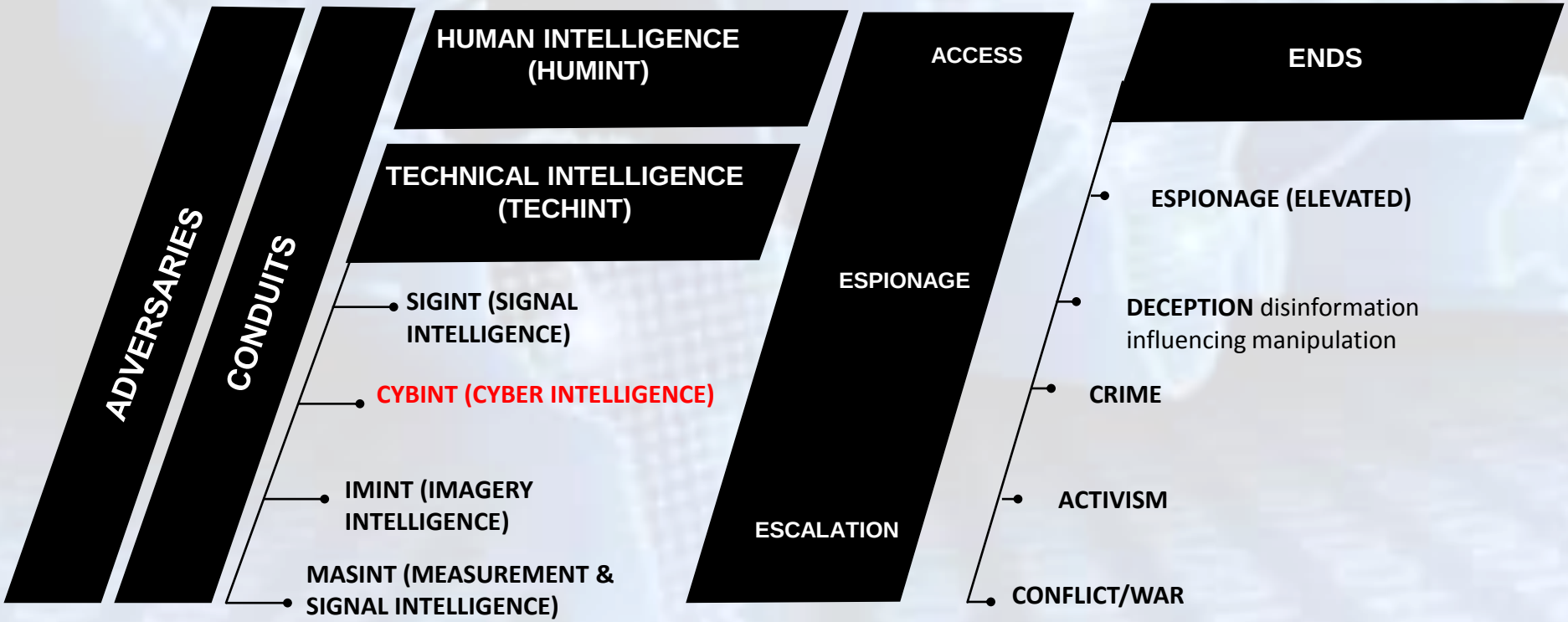
Gaining the Edge - Shaping the Future ???

CYBER COUNTERINTELLIGENCE

- What about high-end threats in a complex environment?
- High-end threats are increasingly multi-vectored, interlinked and intelligence driven.
- What else is needed to 'Gain the Edge and Shape the Future'?
- This part of the presentation briefly examines
  - The nature of high-end threats (threat landscape).
  - Cyber-security responses in general.
  - What Cyber Counterintelligence is and why it is needed.
  - As a 'takeaway' , a CCI-meta model to inform the configuration of organisational Information Security posture.

CYBER COUNTERINTELLIGENCE
– Threat landscape

Multi-vectored intelligence (inclusive of HUMINT) is the name of the game

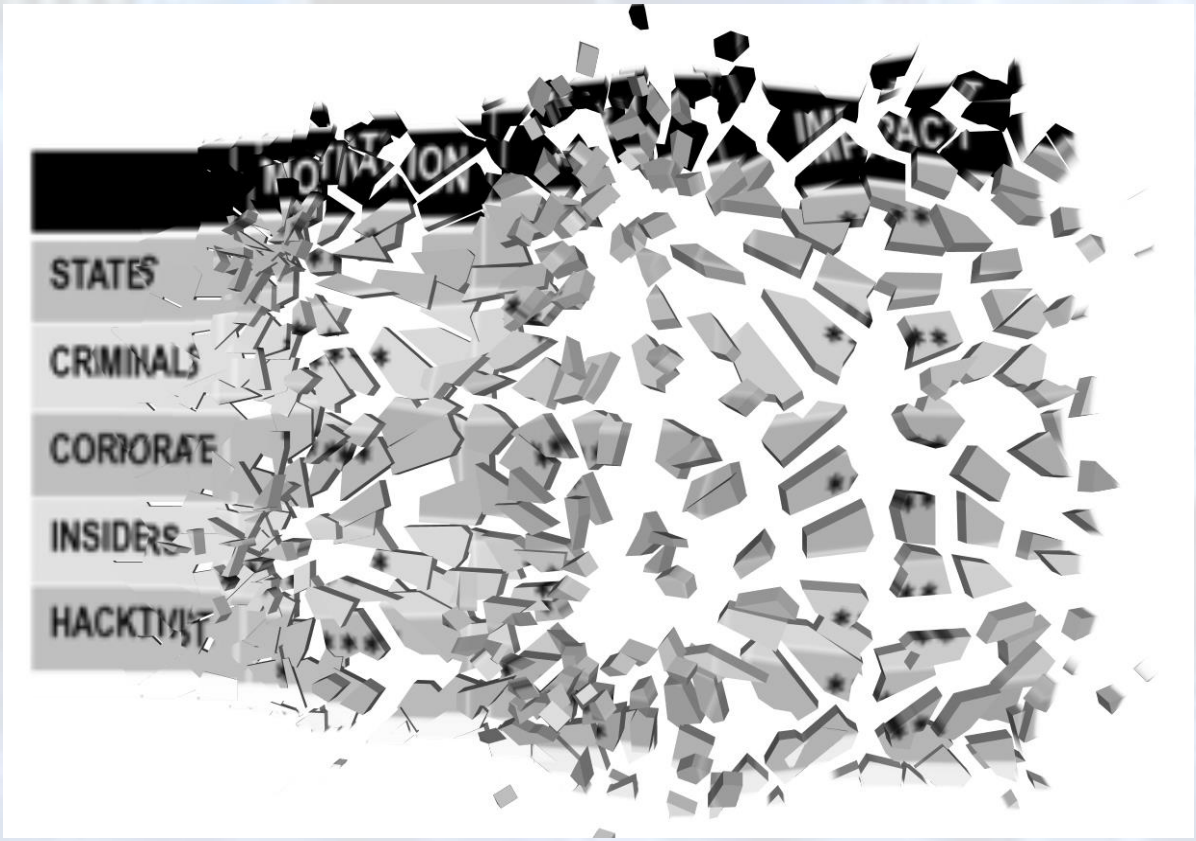


CYBER COUNTERINTELLIGENCE

– Threat landscape

CYBER COUNTERINTELLIGENCE
– Threat landscape

- Conventional ‘thinking-in-boxes’ no longer holds.



CYBER COUNTERINTELLIGENCE
– Threat landscape

Some recent quotes on threat actors :

- **"Nonstate entities**, including international terrorist groups and transnational organized crime organizations, will continue to employ and potentially improve their **intelligence capabilities**, which include **human, cyber, and technical means** ... These entities recruit human sources and conduct physical and technical surveillance to facilitate their activities and avoid detection and capture." USA Intelligence Community (2016)

- **"distinguishing criminal gangs from nation-state actors (is) a challenge**.... Tools and tradecraft become harder to tell apart … some financial threat groups that we track exhibit traits that **look more like state-sponsored APT activity**." Mandiant – FireEye (2015)

- "The **primary motivation** behind global cyber activity has now **shifted from disparate activities** carried out by individuals, groups and criminal gangs pursuing short-term financial gain, to **skilled adversaries driven by broader agendas**." Crowdstrike (2015)

CYBER COUNTERINTELLIGENCE
– Cybersecurity responses

Some quotes on our responses during the past three years:

- "Regardless of how much we are spending to keep the adversaries out, they are still getting in. If we continue to think of our defences in a **check box, technology specific** and project-based, nothing is going to change for us ...." HP 2013

- "Cybersecurity experts know well that **the perimeter defence approach doesn't work**. All such defences can eventually be penetrated or bypassed. And even without such breaches, systems can be compromised … when **bad guys are already inside** the perimeter." Minister Mahlobo 2015

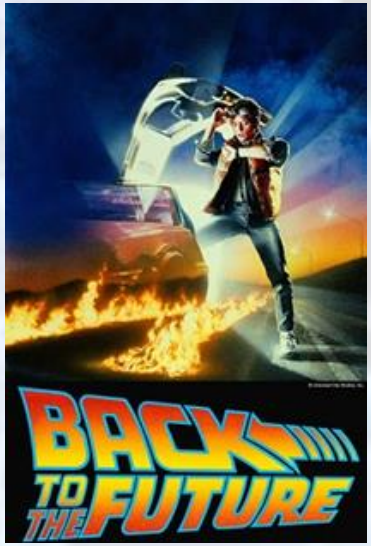
- "While information security risks have dramatically evolved, **security strategies ... have not kept pace** … Most organisations are now **defending yesterday**, even as their adversaries look to **exploit** the **vulnerabilities of tomorrow**."PwC 2013

- "**Cyber security goes to the offensive**, governments, intelligence agencies, law enforcement and private companies" are increasingly considering "an offensive approach to defend their assets from cyber attacks or to assert its supremacy." Infosec 2014

WHY WE NEED CYBER COUNTERINTELLIGENCE ?

- What type of approach do we then need ?

- Five key inter-related requirements
  - ✓ **Defences**: robust and smarter
  - ✓ **Offensive**: pro-active identification and engagement of adversaries
  - ✓ **Intelligence** at the centre.
  - ✓ **Multi-vectored**
  - ✓ **Integrated** with organisational DNA and Cyber Intelligence.



- To **'Gain the Edge – Shape the Future'** we have to go **'Back to the Future'**.

- Counter+ intelligence = counterintelligence.

- Counterintelligence a premise for modelling aspects of our organisational approach.

WHAT IS CYBER COUNTERINTELLIGENCE ?

- Counterintelligence's three core **missions**:
  - **Defensive**: prevent, deter and detect.
  - **Offensive**: detect, disrupt, deceive and degrade through active engagement.
  - **Intelligence**: on environment, adversaries and own vulnerabilities.

- A nation-state's CI functions summarised in **D^9**: Defend, Deter, Detect, Deflect, Derail, Disrupt, Deceive, Degrade and Destroy.

- Counterintelligence **methods** range from physical security to offensive ops.

- Since Cyber Counterintelligence is a subset of Counterintelligence it is also multi-vectored.

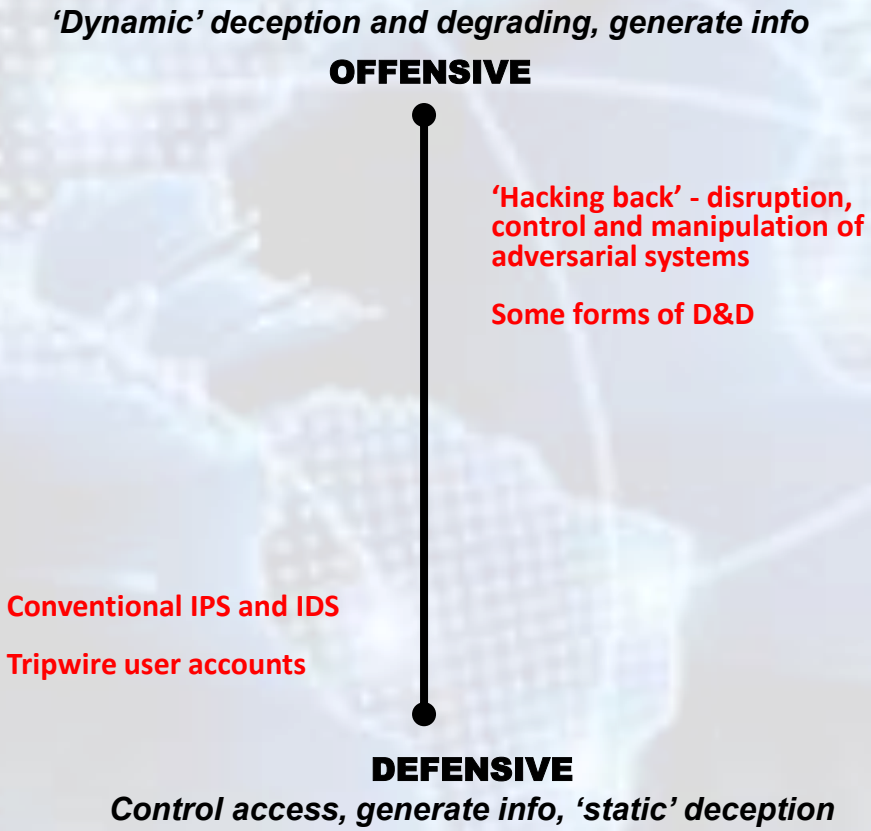
WHAT IS CYBER COUNTERINTELLIGENCE?

'CONVENTIONAL' COUNTERINTELLIGENCE	CYBER COUNTERINTELLIGENCE
Perimeter security and access control	**Firewall and validation**
'Fences' and CCTV	**IDS and IPS** Monitor and inspect traffic with complementary aims. IPS is a control tool ('fence'), IDS is a visibility tool ('CCTV').
Honeypots, dangle, agent/ double agent operations	**A honeypot, honeynet and honeywall** Network set up to 'invite' intrusion or transgression, so that internal and/or external attacker activities, MO and aims can be determined.
Cover and False flags	**Sock puppets** Online identity used for purposes of deception and collection.
All-source CI gathering platforms and services	**Threat Intelligence engines/platforms** Pool open, deep and dark web sources to analyse threats and trends.
HUMINT network	**'Virtual' agents** Penetration of certain hackers forums, closed groups, Darknet

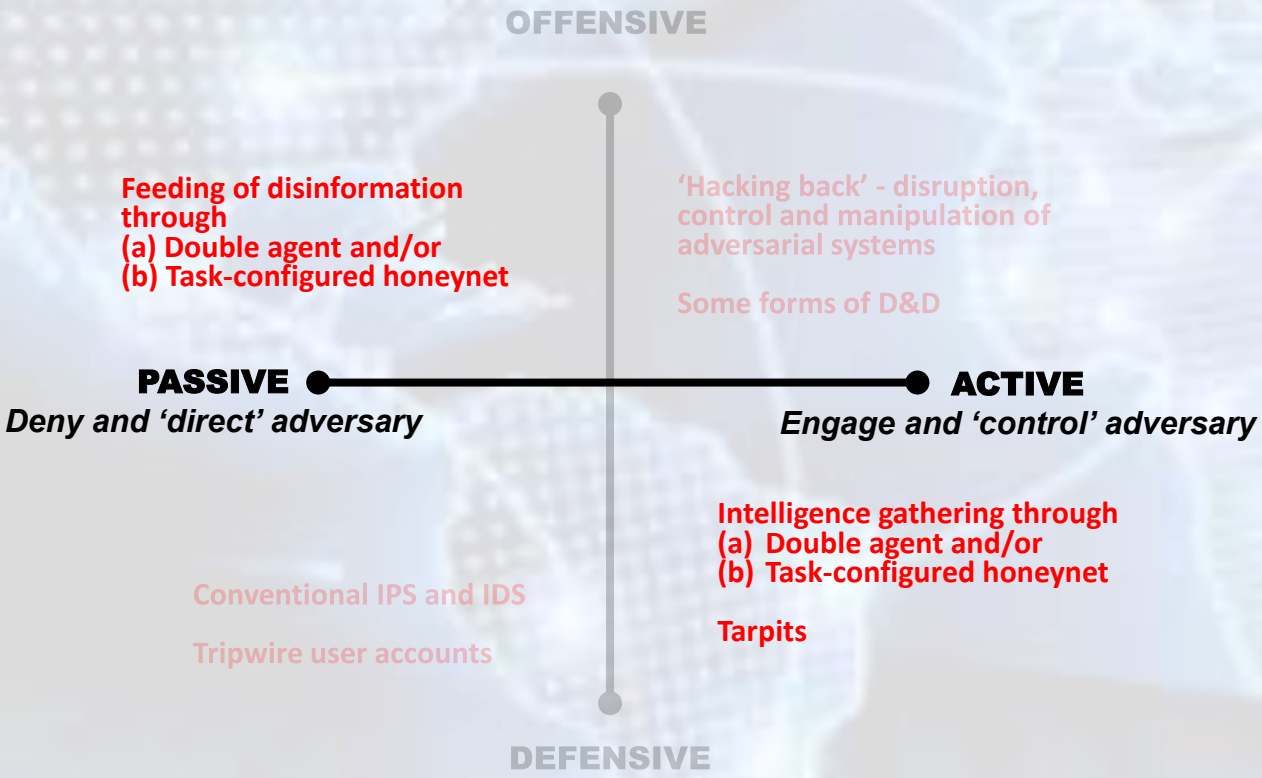
WHAT CYBER COUNTERINTELLIGENCE IS AND IS NOT?

- Cyber Counterintelligence **is not**?
  - ✓ 'Hacking back' in a Cyber Wild West.
    - There are very real legal, organisational and practical limitations.
  - ✓ Plug-in / add-on service or product.
  - ✓ Always a dedicated organisational structure.
- A **Cyber Counterintelligence Model** provides a starting point to configure and demarcate an organisational approach.

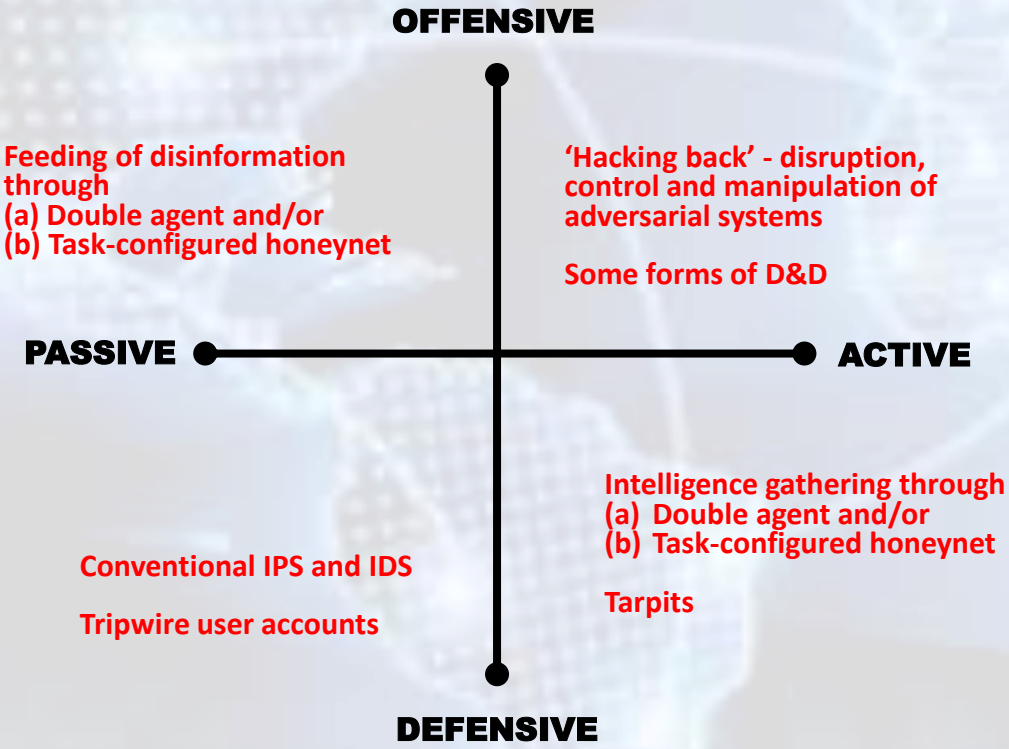
CYBER COUNTERINTELLIGENCE MODEL



CYBER COUNTERINTELLIGENCE MODEL



CYBER COUNTERINTELLIGENCE MODEL



CCI MODEL FOR AN INTEGRATED APPROACH

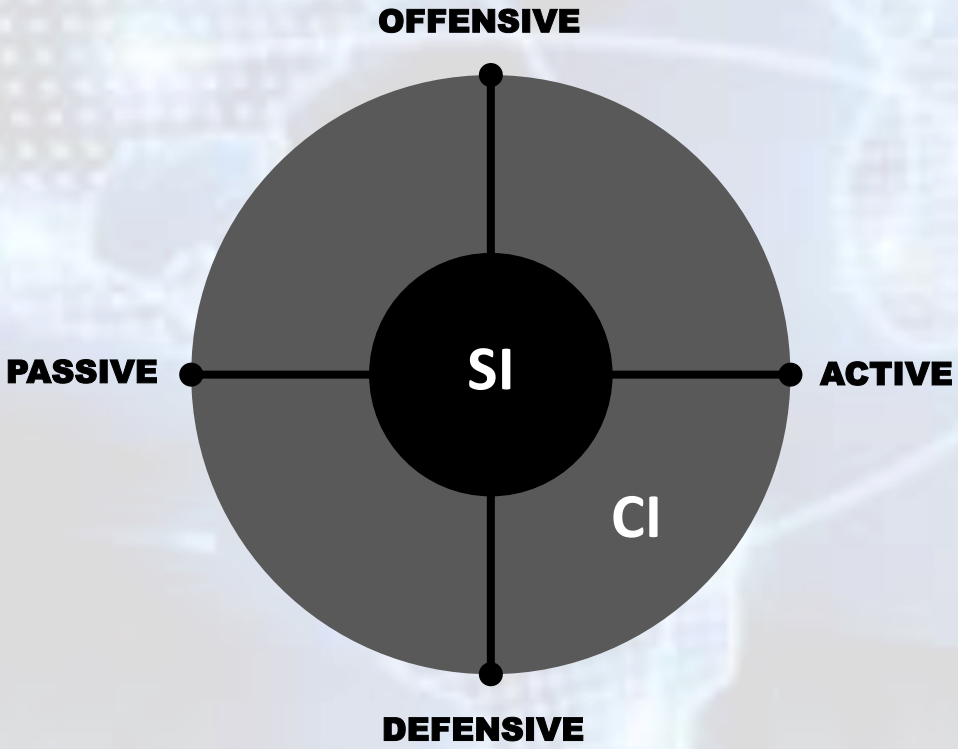
OWN STRATEGY & INTELLIGENCE

CCI MODEL FOR AN INTEGRATED APPROACH

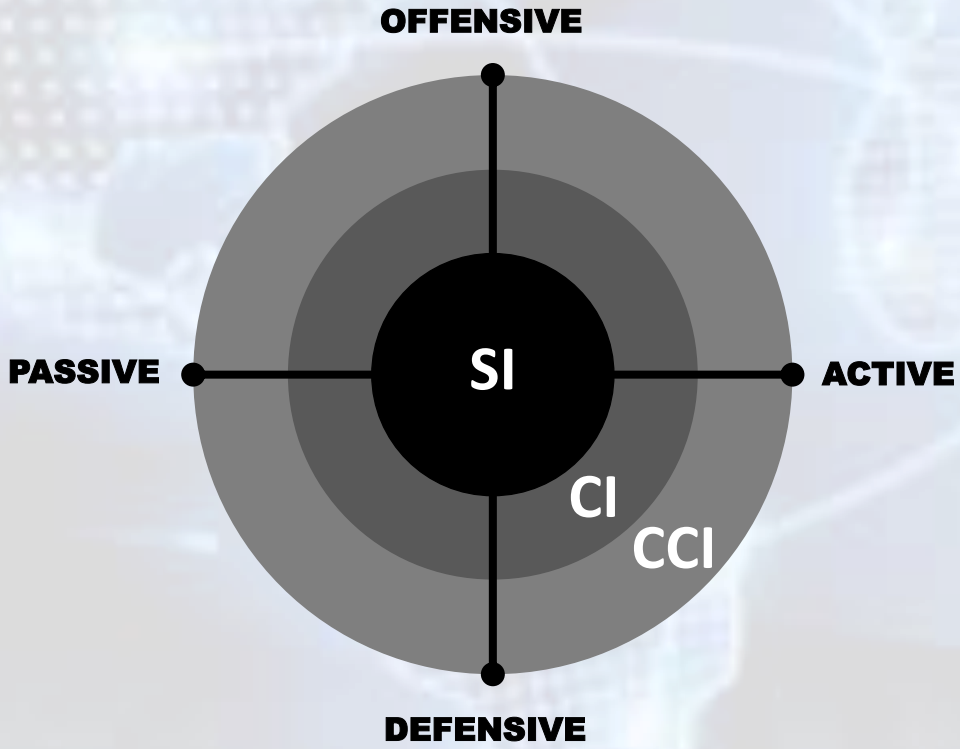
STRATEGY & INTELLIGENCE

+

COUNTERINTELLIGENCE



CCI MODEL FOR AN INTEGRATED APPROACH



STRATEGY & INTELLIGENCE

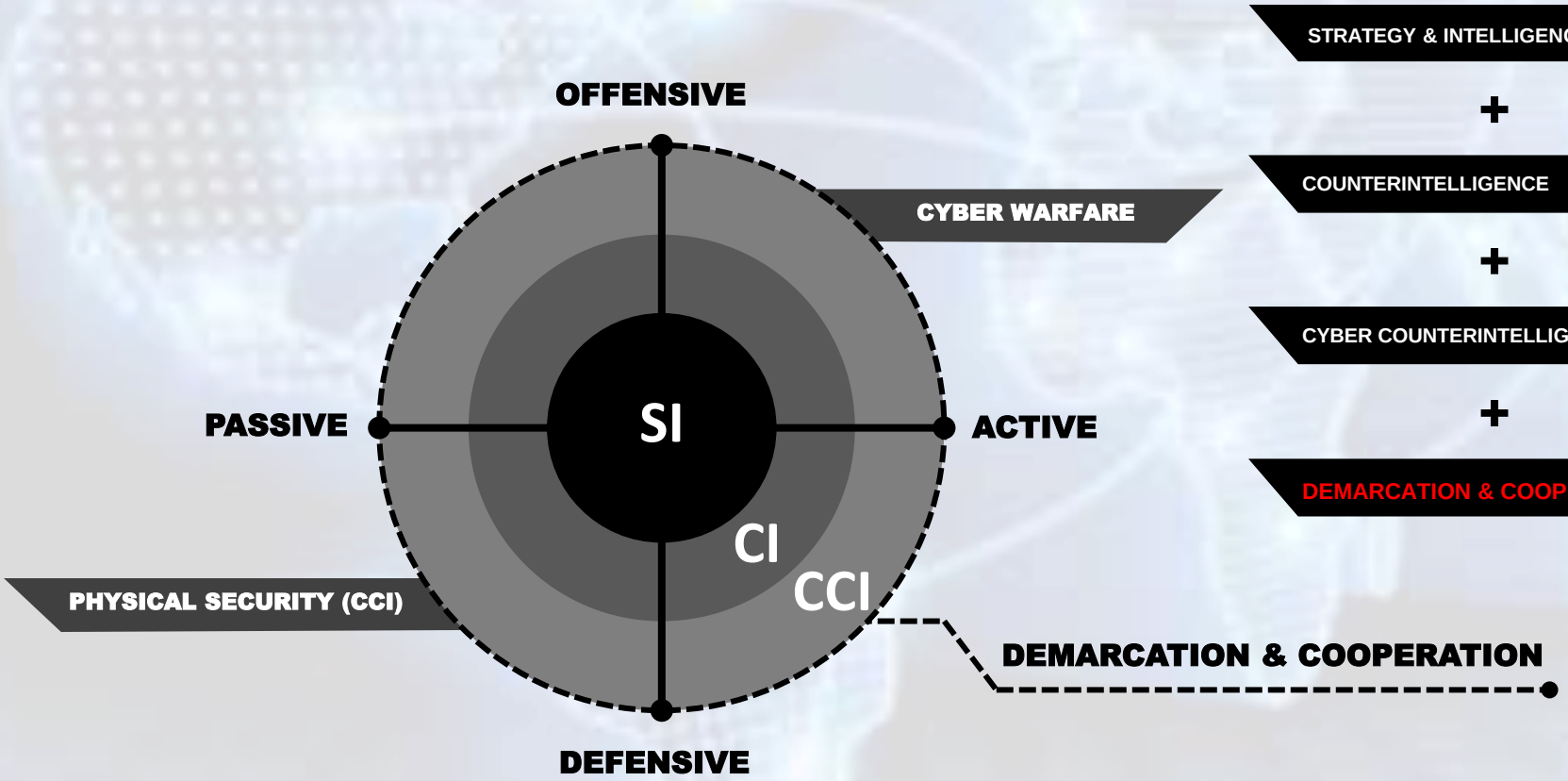
+

COUNTERINTELLIGENCE

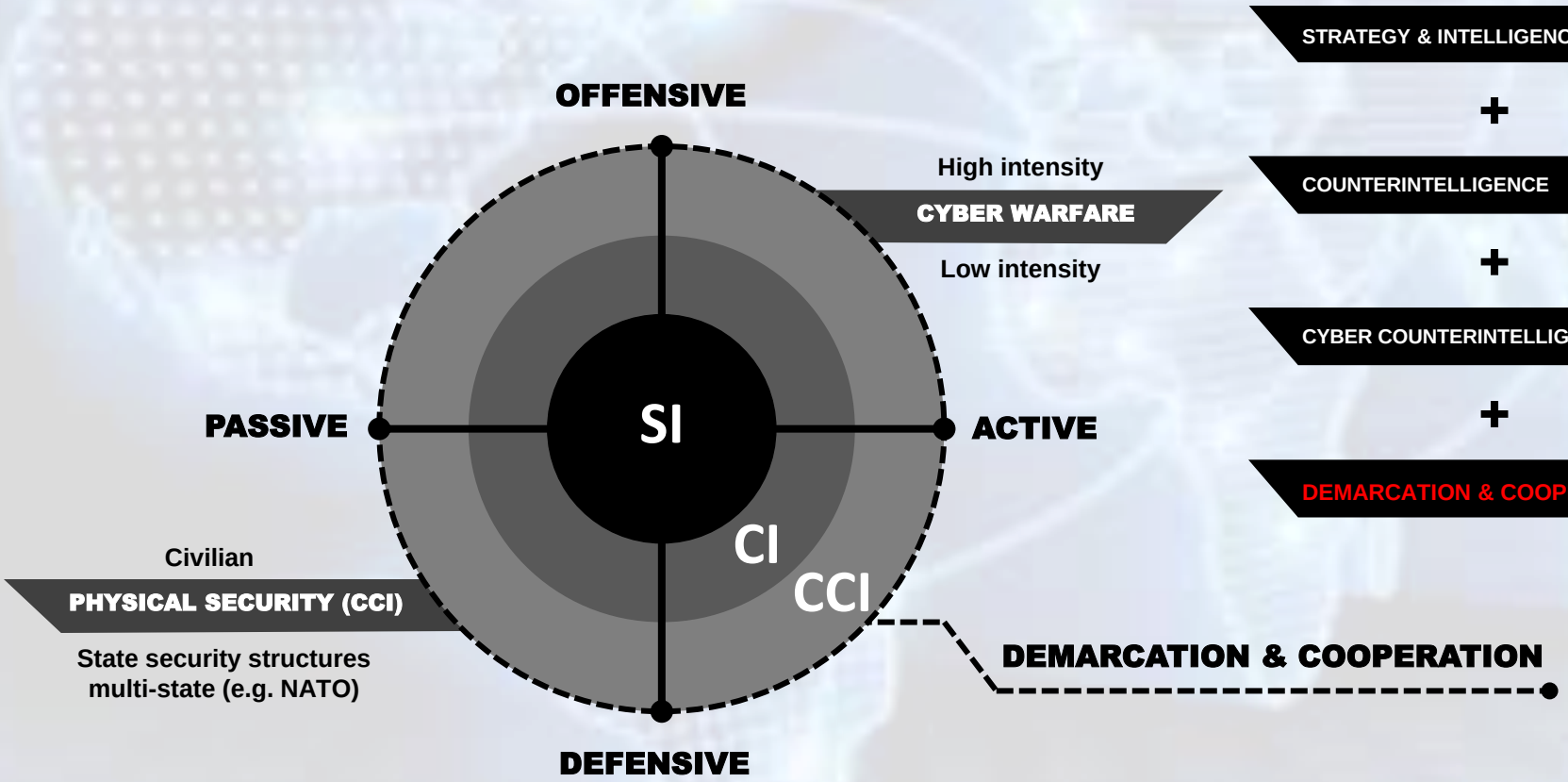
+

CYBER COUNTERINTELLIGENCE

CCI MODEL FOR AN INTEGRATED APPROACH



CCI MODEL FOR AN INTEGRATED APPROACH



CCI MODEL FOR INTEGRATED APPROACH

- ‘Theoretical’ model with real practical application.
- Postures will differ.
- Ensures integration and maximise resources.
- Summarised: Bad news can be good news.

CONCLUSION

- Cyber Intelligence and Counterintelligence are interlinked.

STRATEGY & INTELLIGENCE

- Cyber intelligence and counterintelligence about innovatively applying time-tested practices to the cyber realm.

COUNTERINTELLIGENCE

- Going ‘Back to the Future’ to ‘Gain the Edge - Shape the Future’

CYBER COUNTERINTELLIGENCE

- Both relate to strategic, operational and tactical levels across the organization.

- We need to further developed cyber intelligence and counterintelligence in the South African context.

- Ongoing project at the University of Johannesburg.

http://adam.uj.ac.za/csi/CyberCounterintelligence.html

UNIVERSITY OF JOHANNESBURG

Thank you

Questions / Comments?

Petrus ‘Beer’ Duvenage duvenage@live.co.za

Brett van Niekerk academic.relations@isaca.org.za