Discovering
'**unknown-unknowns**'
& beyond

Adam D.M. Svendsen, PhD

Intelligence & Defence Strategist, Researcher, Educator & Consultant
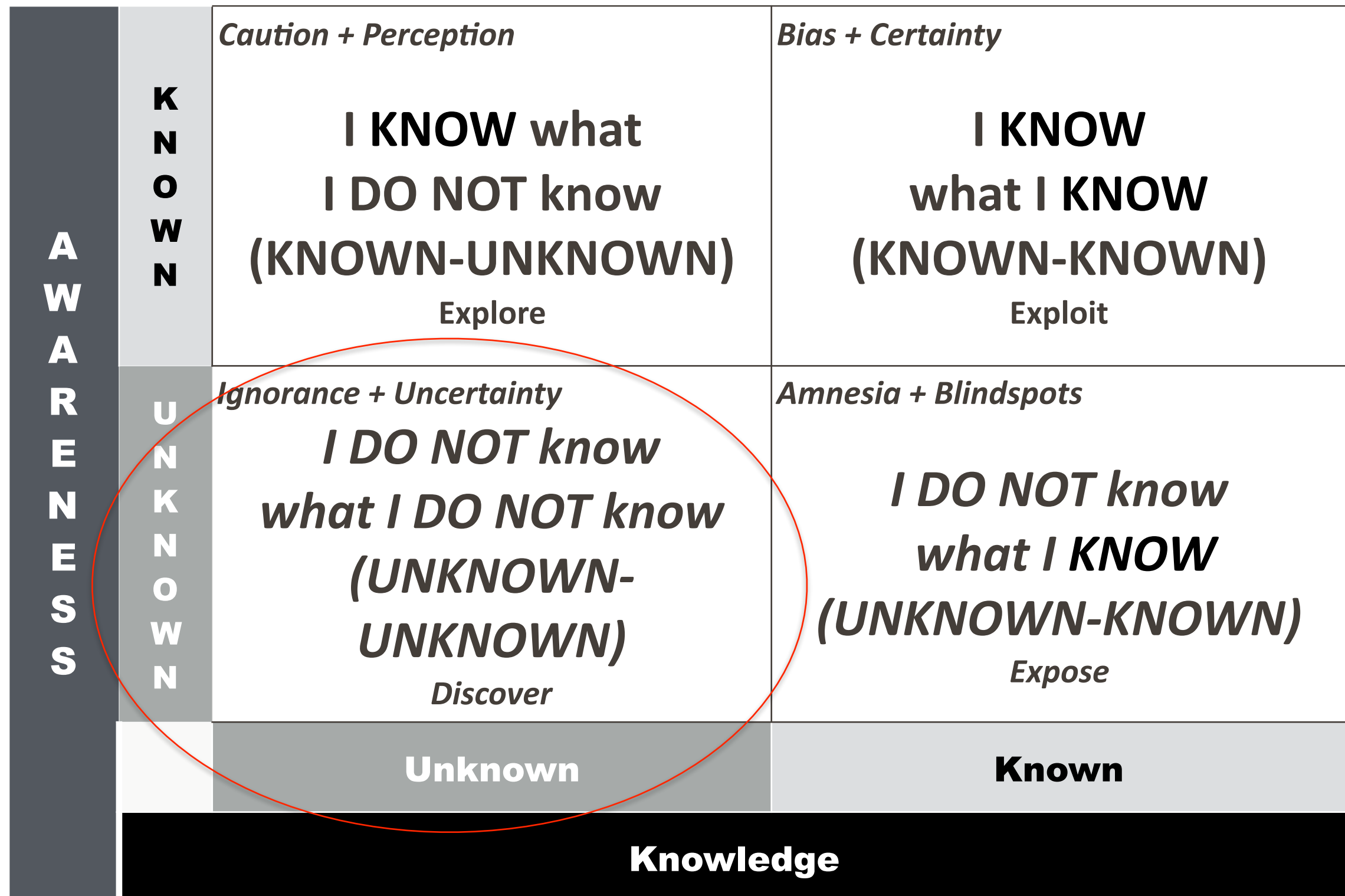
adam@asgonline.co.uk / twitter: @intstrategist

Kick-off

'The environment the Army will operate in is **unknown***. The enemy is* **unknown***, the location is* **unknown***, and the coalitions involved are* **unknown***. The problem we are focusing on is how to "Win in a Complex World."'*

- US Army Operating Concept, 2020-2040 (31 October 2014), p.iii (h/t: Prof. B.M. Linn).

Overall landscape scene-setting

		Caution + Perception I **KNOW** what I DO NOT know (KNOWN-UNKNOWN) Explore	Bias + Certainty I **KNOW** what I **KNOW** (KNOWN-KNOWN) Exploit
A W A R E N E S S	**K N O W N**		
	U N K N O W N	Ignorance + Uncertainty *I DO NOT know* *what I DO NOT know* *(UNKNOWN-* *UNKNOWN)* *Discover*	Amnesia + Blindspots *I DO NOT know* *what I* ***KNOW*** *(UNKNOWN-KNOWN)* *Expose*
		Unknown	**Known**
		Knowledge	

Big Data INT challenges

- When dealing with **distributed Big Data, devs + events** … + their assoc. patterns, **'4Vs' standout**.

- These inc. **'quantitative considerations'** of:

    (i) **'Volume'** - e.g. *'scale/size of data/devs + events'*; +

    (ii) **'Velocity'** - e.g. *'analysis of streaming/flows of data/devs + events'*; as well as

- evaluating **'qualitative factors'** of:

    (iii) **'Variety'** - e.g. *'differentiated forms of data/devs + events'*; +

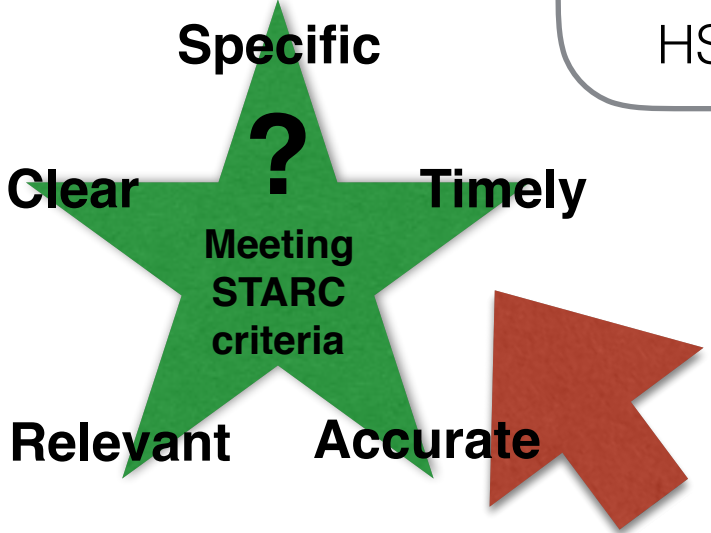   (iv) **'Veracity'** - e.g. *'uncertainty of + relating to data/devs + events'*.

(1) Choose focus:
Theme(s)/
Issue(s)/
Problem(s)/
Hazard(s)/
Risk(s)/
Threat(s)

(2) Select which 'System of Systems Dynamics' (SoSD) to use:
STEEP(L) [B.I.]/
PESTLE [EUROPOL]/
PMESII [NATO]/
DIME [USMIL.]/
HSCB [USMIL.]

(3) Each 'system' in SoSD has following variables/attributes:
(i) *internal influences/factors*;
(ii) *rationale*;
(iii) *types & forms*;
(iv) *conditions & terms*;
(v) *trends (inc. SWOT)*;
(vi) *functions*;
(vii) *external influences/factors*;
+
(viii)
effects & outcomes

A comprehensive, structured analytical framework for helping address & better manage UNCERTAINTY

Specific

?
Meeting STARC criteria

Clear   **Timely**

Relevant   **Accurate**

Each of factors included in STEPS 2-4 can be **listed/mapped via grids/matrices** for transparency, traceability & accountability

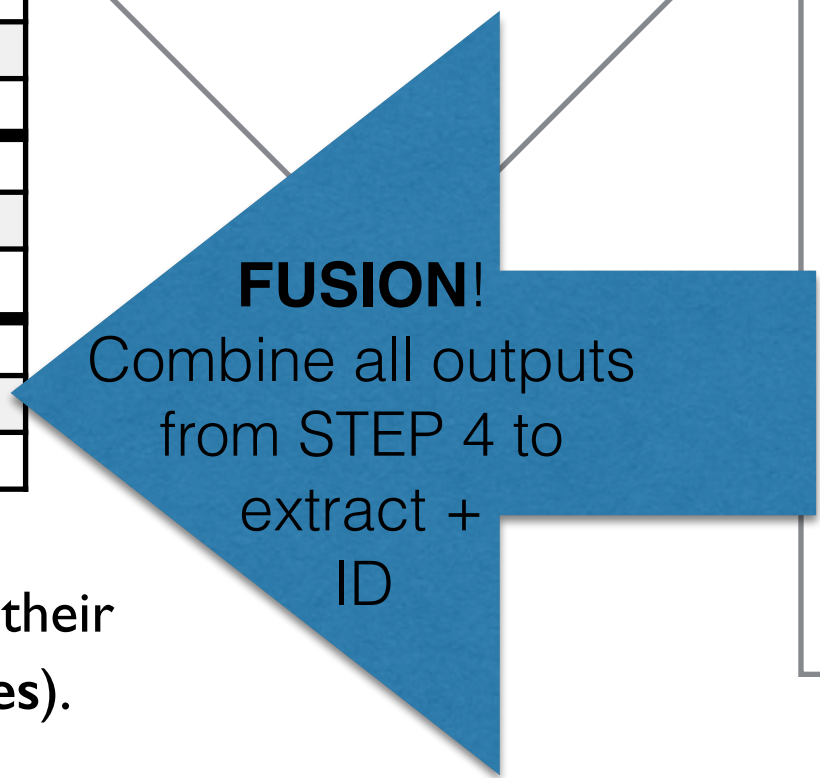**(4) In turn, each 'system variable/attribute' has following 'levels':**
(i) Ideological
(ii) Theoretical
(iii) Strategic
(iv) Policy
(v) Operational
(vi) Tactical
(vii) Individual (as 'professional')
+
(viii) Personal
(high-low; macro-micro ranging)

(5) Identify A+B+C = 'Signifier Node':

(A) 'Key Actors' - e.g. who? (e.g. OC groups, individuals, other 'targets', etc.)	**(A1) Events** - e.g. what? when?
	(A2) Patterns - e.g. how?
	(A3) Drivers - e.g. why?
(B) 'forces/factors of change' - e.g. what activity? (e.g. SOC areas, etc.)	**(B1) Events** - e.g. what? when?
	(B2) Patterns - e.g. how?
	(B3) Drivers - e.g. why?
(C) 'possible change over time' - e.g. when? / where? (e.g. environment, PESTLE/PMESII [SoSD] indicators, SWOT, etc.)	**(C1) Events** - e.g. what? when?
	(C2) Patterns - e.g. how?
	(C3) Drivers - e.g. why?

Aim = capture:
(i) the **players**; (ii) their **relationships**; (iii) their **drivers** (means, motives & opportunities).

FUSION!
Combine all outputs from STEP 4 to extract + ID

Generate 'Signifier Node(s)' = Building-blocks for Contextualisation

OVERVIEW SNAPSHOT SUMMARY
At a minimum for context consider + fuse:

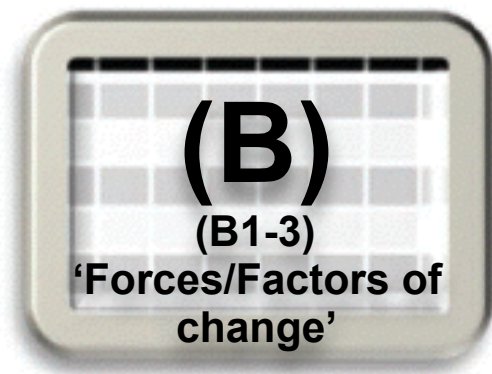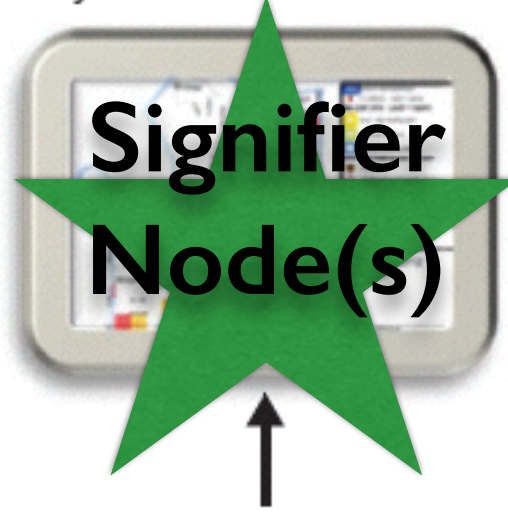|	
(A) 'Key Actors' - e.g. who? (e.g. OC groups, individuals, other 'targets', etc.)	**(A1) Events** - e.g. what? when? where? **(A2) Patterns** - e.g. how? **(A3) Drivers** - e.g. why?
(B) 'forces/factors of change' - e.g. what activity? (e.g. SOC areas, etc.)	**(B1) Events** - e.g. what? when? where? **(B2) Patterns** - e.g. how? **(B3) Drivers** - e.g. why?
(C) 'possible change over time' - e.g. when? / where? (e.g. environment, PESTLE/PMESII [SoSD] indicators, SWOT, etc.)	**(C1) Events** - e.g. what? when? where? **(C2) Patterns** - e.g. how? **(C3) Drivers** - e.g. why?

Aim = capture: (i) the **players**; (ii) their **relationships**; (iii) their **drivers** (e.g. their **means, motives & opportunities**).

How to put it all together?

130 Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations
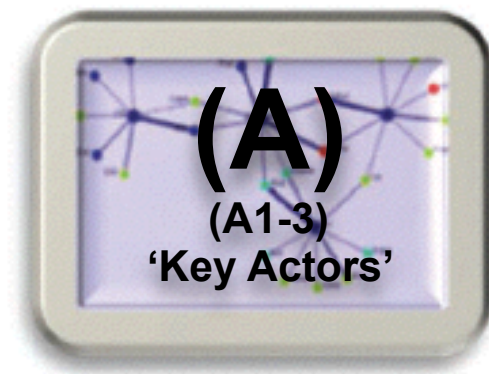
Figure 5.5
Tools to Create Shared Situational Awareness

From '**Signifier Node(s)**' to **n e x t moves**…

Common Operational Picture
Near-term key information and decision support

Signifier Node(s)

Generation of '**Signifier Node(s)**' for positioning on triage-related/colour-coded '**indicator board(s)**' = for **context appreciation** + **situation awareness** generation >>> help for making '**where next?**' + **response decisions (SEW potent.)**

(B)
(B1-3)
'**Forces/Factors of change**'

Narrative Tools
Records and notes on entities and events of interest

RAND RR233-5.5

(A)
(A1-3)
'**Key Actors**'

Network Analytics
Analysis related to persons, other entities, and relationships of interest

(C)
(C1-3)
'**Possible change over time**'

Spatiotemporal Analytics
Analysis related to where and when crime might occur

From **the known** to **the unknown**

130 Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations

Figure 5.5
Tools to Create Shared Situational Awareness

A = 'key actors'
B = 'forces/factors of change'
C = 'possible change over time'

For each, consider:
1. Events
2. Patterns
3. Drivers

(Source: Quarmby, 2003)

Signifier 'Node'
(A,B,C = based on data from triangulated selected sources - 'what?' >>> 'what does it mean?' = information)

(information >>> approx. 'knowledge' / 'understanding' - e.g. of impact - when Signifier Node(s) positioned on 'Indicator Board', e.g. at / in region of X)

P
Political

E₂
Environment

E₁
Economic

L
Legis./Legal

S
Social

T
Technology

Scenario #1
Scenario #2
Scenario #3

Indicator board positioning work provides outputs in the form of insights - e.g. for input into the generation of different **future scenarios** to discover **UNKNOWN-UNKNOWNS +** expose **UNKNOWN-KNOWNS,** + to turn them into **KNOWN-UNKNOWNS** so can explore more
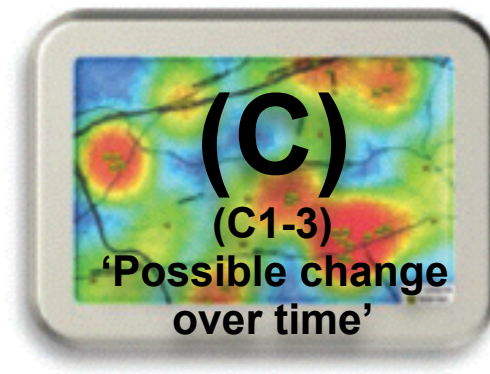
Common Operational Picture
Near-term key information and decision support

Signifier Node(s)

B
(B1-3)
'Forces/Factors of change'
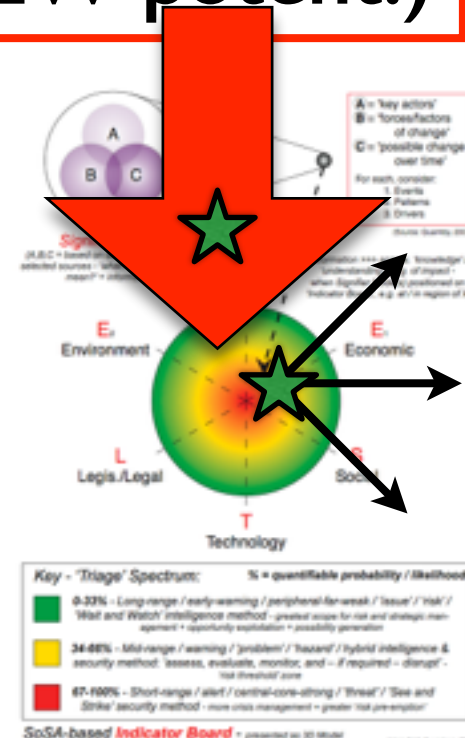Narrative Tools
Records and notes on entities and events of interest

A
(A1-3)
'Key Actors'
Network Analytics
Analysis related to persons, other entities, and relationships of interest

C
(C1-3)
'Possible change over time'
Spatiotemporal Analytics
Analysis related to where and when crime might occur

RAND RR233-5.5

Key - 'Triage' Spectrum: % = quantifiable probability / likelihood

0-33% - Long-range / early-warning / peripheral-far-weak / 'issue' / 'risk' / 'Wait and Watch' intelligence method - greatest scope for risk and strategic management + opportunity exploitation + possibility generation

34-66% - Mid-range / warning / 'problem' / 'hazard' / hybrid intelligence & security method: 'assess, evaluate, monitor, and – if required – disrupt' - 'risk threshold' zone

67-100% - Short-range / alert / central-core-strong / 'threat' / 'See and Strike' security method - more crisis management + greater 'risk pre-emption'

SoSA-based **Indicator Board** - presented as 3D Model

Adam D.M. Svendsen, PhD

Key **conclusions** & **takeaways** #1

- Tools + frameworks = help us move from:

  ➡(i) merely exploiting **KNOWN-KNOWNs** ('what we know we know') >>>

  ➡(ii) exploring **KNOWN-UNKNOWNs** ('what we know we do not know') >>>

  ➡(iii) exposing **UNKNOWN-KNOWNs** ('what we do not know we know') +

  ➡(iv) discovering (potential) **UNKNOWN-UNKNOWNs** ('what we do not know we do not know') domains.

Key **conclusions** & **takeaways** #2

- This INT + knowledge work = useful for:

  - operational-to-strategic early **warning**;

  - **over-the-horizon** insights;

  - better keeping 'ahead of curve of **events + developments**';

  - distinguishing (weak-strong) **'signals' from** (overall/ background) **'noise'**;

  - maintaining **'edge' + 'initiative'**;

  - better **filtering, targeting, prioritisation**, etc.

@intstrategist

Find out more via Twitter!