Presenting
Intelligence Engineering:
Operating Beyond the Conventional

Bridgehead Institute
Research & Consulting

Adam D.M. Svendsen, PhD
Intelligence & Defence Strategist, Researcher, Educator & Consultant
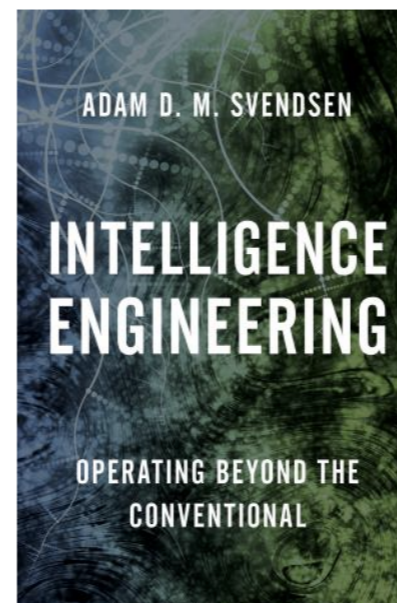Bridgehead Institute (Research & Consulting)
adam@asgonline.co.uk
@intstrategist

Introduction: Advancing IE #1

- **IE framework** (aka. the *'Bridgehead Methodology'*) **= relevant for:**

  1. *risk analysis* **&** *assessment* **to**

  2. *risk management* **& for**

  3. **helping facilitate** *resilience*.

- Done for much-needed sophisticated:

  ➡ **(a) '***context appreciation***'** (analysis + assessment - G/J2 work) **+ then**

  ➡ **(b) improved '***solution-fashioning***'** (engineering + building/synthesis - G/J3 tasks)

Bridgehead Institute
Research & Consulting

ADAM D. M. SVENDSEN

INTELLIGENCE ENGINEERING

OPERATING BEYOND THE CONVENTIONAL

Introduction: Advancing IE #2

- Aim = For **better understanding & then addressing** complex **uncertainty** experienced **now & that anticipated** in future - e.g. in battlespaces.

- Both *a priori* (before) **& *post facto*** (after) **concerns & considerations** feature.

- Strong focus on **positioning:**

  - e.g. better getting 'ahead of' **event & development 'curves'** as they unfold, at times rapidly.

Source: http://www.defence.gov.au/news/raafnews/editions/4802/images/10-P12-Main-graphic.jpg

Introduction: Advancing IE #3

- **Value:** IE boasts many **operational & strategic *ways*, *means*, & *ends***.

- **IE encompasses**:

  1. intelligence-associated **collection/gathering & analysis/ assessment (estimate)** work; to

  2. the **further operationalised implementation of plans & intents** generated by commanders & other **high-level leaders** & policy- to decision-makers.

ADAM D. M. SVENDSEN

INTELLIGENCE ENGINEERING

OPERATING BEYOND THE CONVENTIONAL
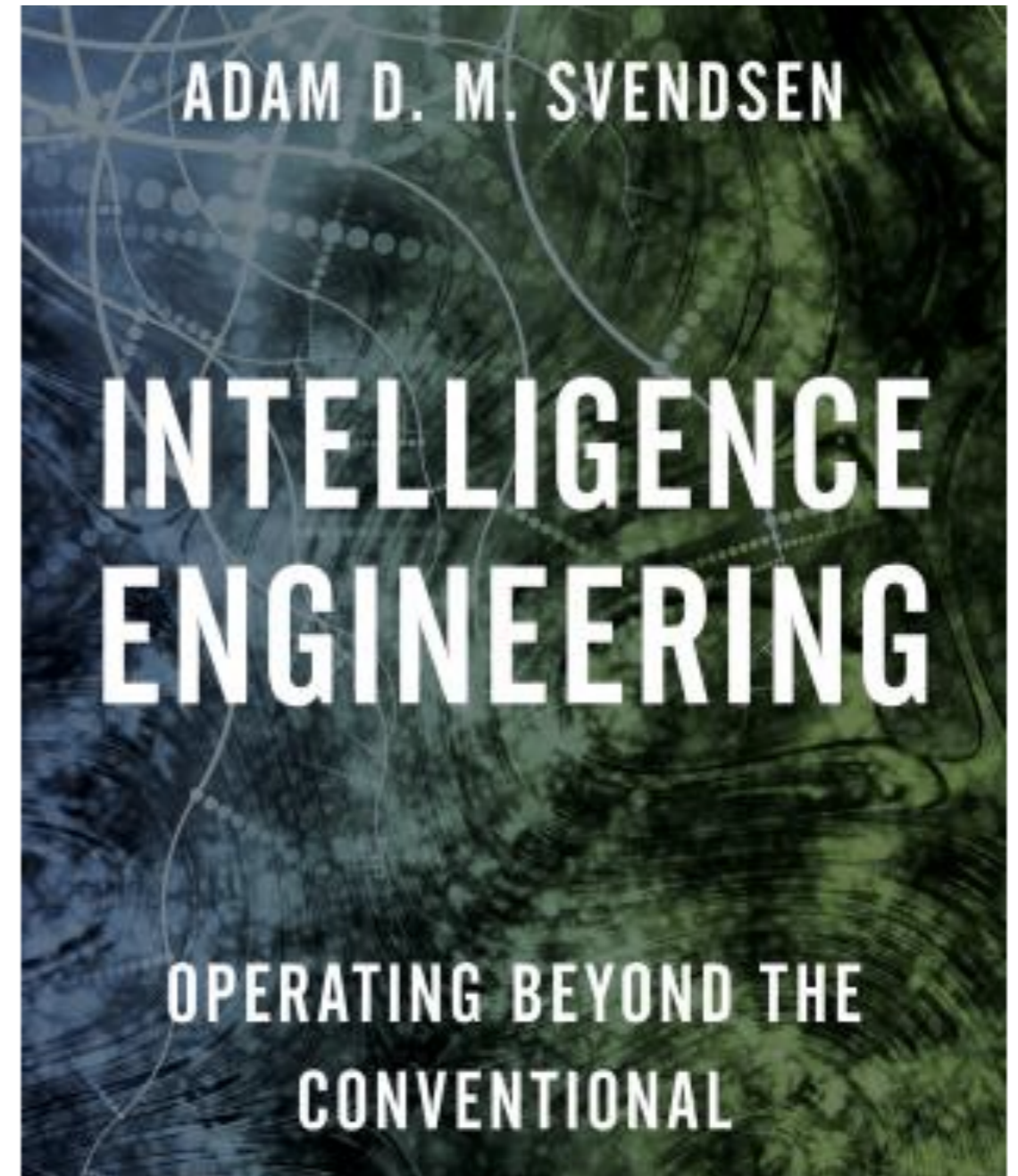
Introduction: Advancing IE #4

- **Several 'edges' benefit from their 'extra sharpening'** to gain advantage:

    - e.g. competition over adversaries + rivals.

- IE offers several **tools, toolboxes & toolsets** - e.g. harnesses SoS (e.g. PMESII, PESTLE, HSCB, etc.).

- IE also guides which = best to select & apply (whatever context)

- Demonstrates **added value + USPs** IE overall brings to multiple **defence & security enterprises**.
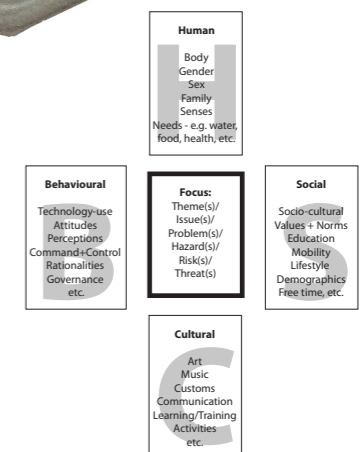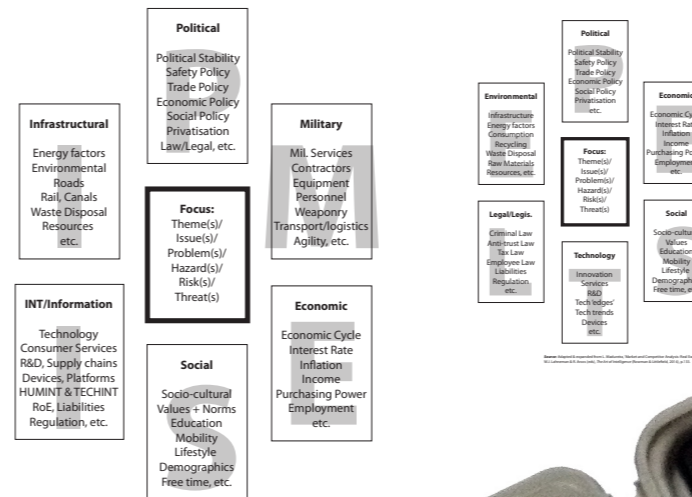
Introduction: Advancing IE #5

- **IE 'toolbox'** consists of:

  ➡ 5x **'toolsets'** offering 'tools'

  ➡ Each **'toolset'** = a **bite-sized IE process 'step'**

  ➡ In turn, **each 'step' = progressed linearly** in a 'building' manner.

  ➡ Overall IE process = arranged as a **(semi-)structured analytical framework** for risk.

(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.]

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

Specific

?

Clear   **Timely**

Meeting STARC criteria

Relevant   **Accurate**

(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

Each of factors included in STEPS 2-4 can be listed/ mapped **via grids/matrices** for transparency, traceability & accountability - see e.g. next slides…

(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

See book: A.D.M. Svendsen, *Intelligence Engineering*, p.71, 91-92.

An example of **fusion**: ISIS

Overall '**Situational Awareness**' Evaluation (**SoSA/G-J2**)
CONTEXT APPRECIATION - **Observe + Orient**

System attributes/ variables > e.g. inc. captures + covers...? > - - - - - - - - - - - - - - SoSA units (e.g. PMESII):	Internal influences / factors 'Who?' / 'Which?'	Rationale 'Why?'	Types + Forms 'What?'	Conditions + Terms 'When?'	Trends (+ dynamics/ flows) 'Where?'	Functions 'How?'	External influences / factors 'Who?' / 'Which?'	Effects + Outcomes 'What?' / 'S.W.O.T.'
Political (inc. law/legislation)	Sharia law / alternative hierarchies	Unrep. elsewhere/ power-play	Strong leadership	Fill governance vacuum	Exploiting Iraq/Syria weaknesses	Ruthless / kill off opposition	Sympathisers	Imposing regime
Military	Tight, well-disciplined C2	Got weapons / tactics	e.g. Heavy+auto matic weaponry	Succeed vs. weaker/ disorg. oppo	Good at capturing; less so at holding?	Agile / flexible / fast-lightfoot	Ex-military personnel	Competent committed adversary
Economic	Profitable/ employed	Make profit - e.g. oil	Steady supply funding	Exploit existing/new markets	Exploiting oil-refineries	Able to sell, e.g. oil	Resp to consumer demands	Self-sustaining/ autarky?
Social (inc. sociological + cultural)	Camarad-erie/ purpose	Romance	Bonding/ band-bros/ marriage	Links/ties - e.g. friends/ passions	Native + Foreign fighters	Quasi-religious/ smashing activities	'Call of the wild'/ share adventurism	Soft + not just hard factors
Informational/ Intelligence (inc. technological)	Good / soc media / BYOD	Able to influence	Social media/ propaganda	INFO/ PSYOPS = work	Use internet - e.g. Twitter	Access to electronic devices	Acquiescence support thru intimidation	Shifting frames of reference
Infrastructural (inc. environment[al])	Good networks/ comms	Can seize/ control/ trade/nego	Training camps/bases	Using what is there - e.g. roads...	Urban/settled/ travel-able areas	Travel on roads / oil refinery use	Unwitting(?) private service prov	Too depend on what have already?

STEP 3

STEP 4

CYBINT ANALYSIS INSIGHTS FUSION EXAMPLE: ISIS

Overall 'Situational Awareness' Evaluation (SoSA/G-J2)
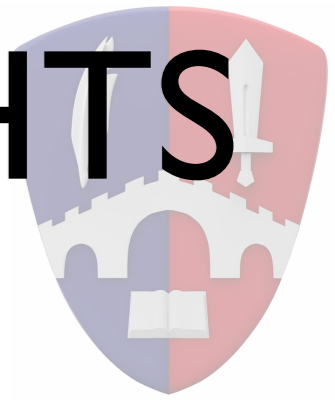
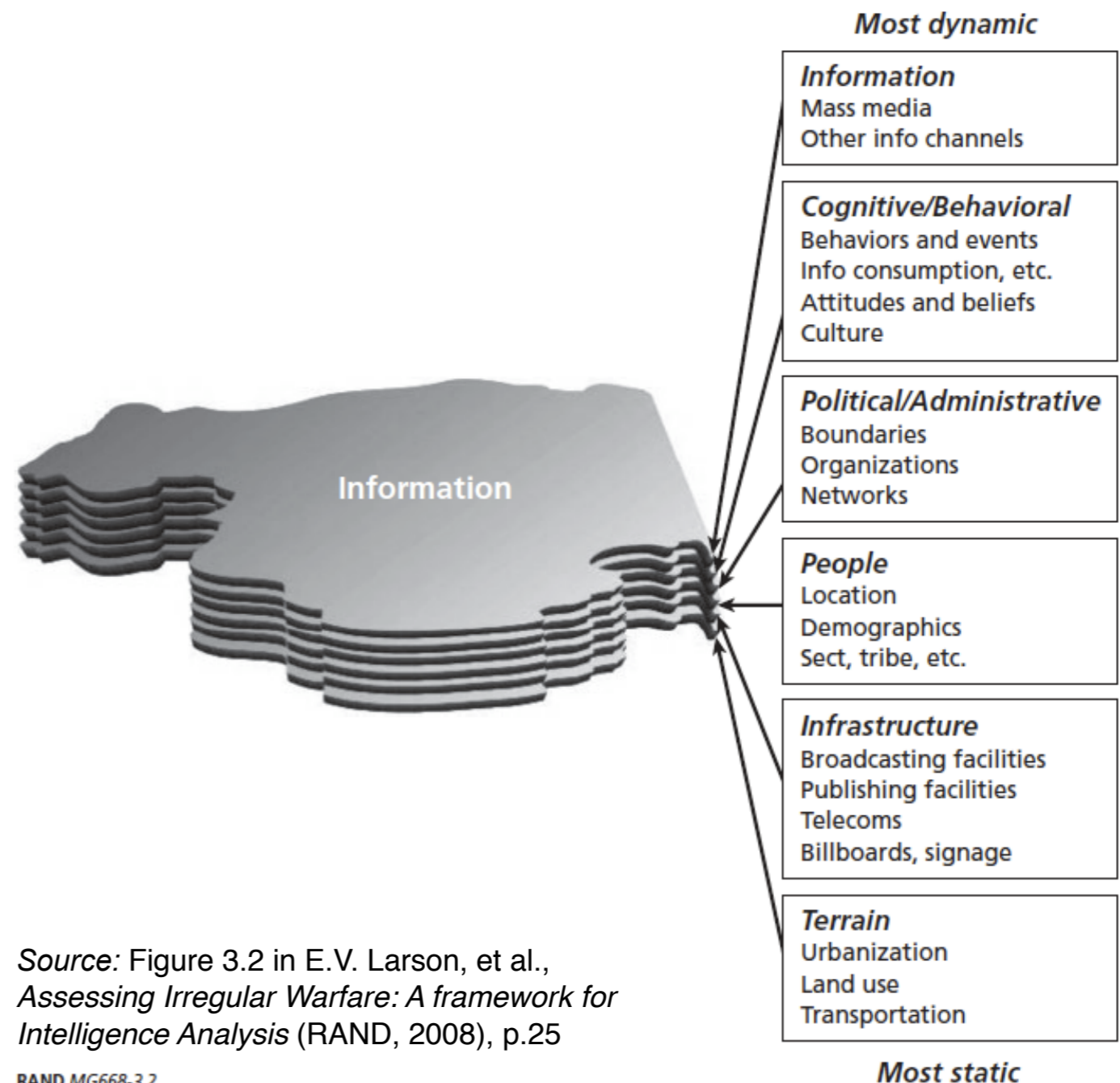### CONTEXT APPRECIATION - Observe + Orient

System attributes/ variables > e.g. inc. captures + covers...? > ---------- SoSA units (e.g. PMESII):	Internal influences / factors 'Who?' / 'Which?'	Rationale 'Why?'	Types + Forms 'What?'	Conditions + Terms 'When?'	Trends (+ dynamics/ flows) 'Where?'	Functions 'How?'	External influences / factors 'Who?' / 'Which?'	Effects + Outcomes 'What?' / 'S.W.O.T.'
Political (inc. law/legislation)	Sharia law / alternative hierarchies	Unrep. elsewhere/ power-play	Strong leadership	Fill governance vacuum	Exploiting Iraq/Syria weaknesses	Ruthless / kill off opposition	Sympathisers	Imposing regime
Military	Tight, well-disciplined C2	Got weapons / tactics	e.g. Heavy +automatic weaponry	Succeed vs. weaker/ disorg. oppo	Good at capturing; less so at holding?	Agile / flexible / fast-lightfoot	Ex-military personnel	Competent committed adversary
Economic	Profitable/ employed	Make profit - e.g. oil	Steady supply funding	Exploit existing/new markets	Exploiting oil-refineries	Able to sell, e.g. oil	Resp to consumer demands	Self-sustaining/ autarky?
Social (inc. sociological + cultural)	Camarad-erie/ purpose	Romance	Bonding/ band-bros/ marriage	Links/ties - e.g. friends/ passions	Native + Foreign fighters	Quasi-religious/ smashing activities	'Call of the wild'/ share adventurism	Soft + not just hard factors
Informational/ Intelligence (inc. technological)	Good / soc media / BYOD	Able to influence	Social media/ propaganda	INFO/ PSYOPS = work	Use internet - e.g. Twitter	Access to electronic devices	Acquiescence support thru intimidation	Shifting frames of reference
Infrastructural (inc. environment[al])	Good networks/ comms	Can seize/ control/ trade/nego	Training camps/bases	Using what is there - e.g. roads...	Urban/settled/ travel-able areas	Travel on roads / oil refinery use	Unwitting(?) private service prov	Too depend on what have already?

N.B.: main CYBINT concerns not isolated from the other aspects encounter + need to consider more widely

Conclusions #1

- IE effectively **captures & then addresses** the complexity of **'multi-everything' nature** of op. environments:

  - e.g. for *'**M4IS2: multiagency, multinational, multidisciplinary, multidomain information sharing & sense making**'*

- Ranges across & involves: *'**eight entities [of] commerce, academic, government, civil society, media, law enforcement, military & non-government/non-profit.**'* (Segell, 2012)

- **Business + enterprise relevance** >>> increasingly self-evident.

Figure 3.2
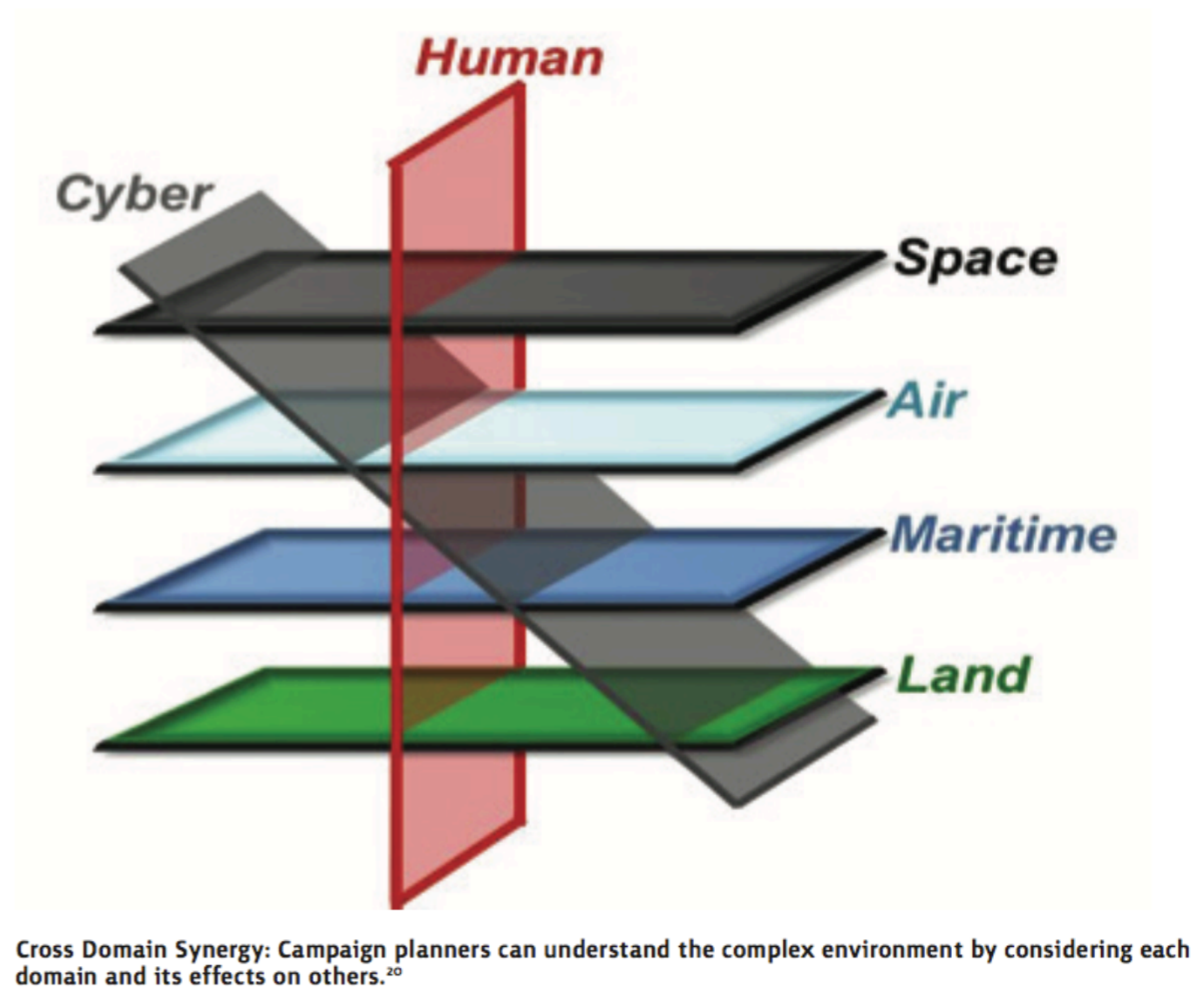**Geospatially Oriented Aspects of the Information Domain of the Operating Environment**

Most dynamic

Information
Mass media
Other info channels

Cognitive/Behavioral
Behaviors and events
Info consumption, etc.
Attitudes and beliefs
Culture

Political/Administrative
Boundaries
Organizations
Networks

Information

People
Location
Demographics
Sect, tribe, etc.

Infrastructure
Broadcasting facilities
Publishing facilities
Telecoms
Billboards, signage

Terrain
Urbanization
Land use
Transportation

Most static

Source: Figure 3.2 in E.V. Larson, et al., *Assessing Irregular Warfare: A framework for Intelligence Analysis* (RAND, 2008), p.25

RAND *MG668-3.2*

9/

Conclusions #2

- Helps **find + fill 'gaps' / 'missing dimensions'** & **'join/connect-the-dots'** in + across all domains of activity.

- **IE 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.

Cross Domain Synergy: Campaign planners can understand the complex environment by considering each domain and its effects on others.[20]

*Source: PRISM, 6, no. 3 (2016), p.16.*

10/

Conclusions #3

- 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.

- **So What?** IE **added value & USPs** =

  1. **Intelligence optimisation** tasks & then

  2. best **event + development transformation**.
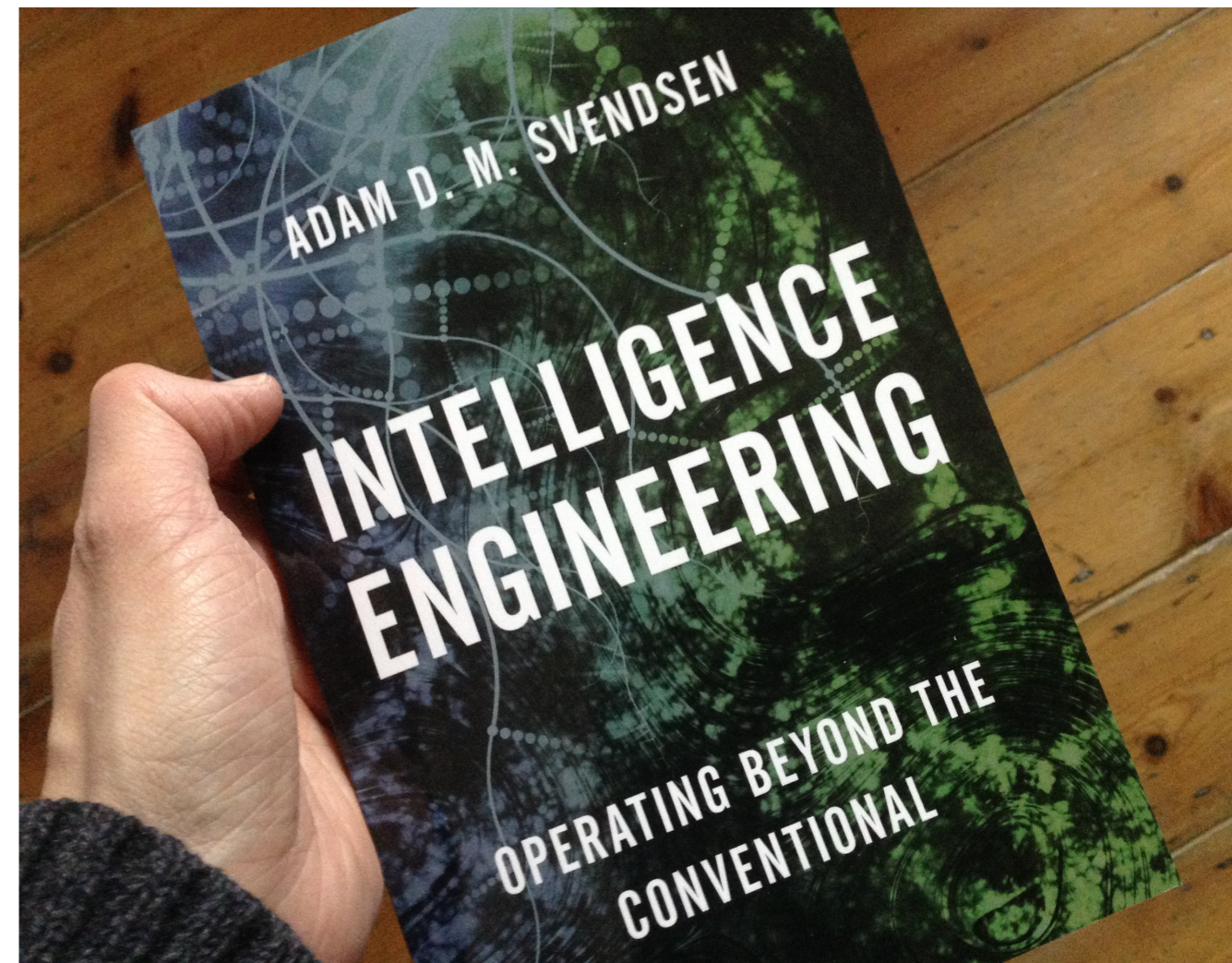
Further Insights
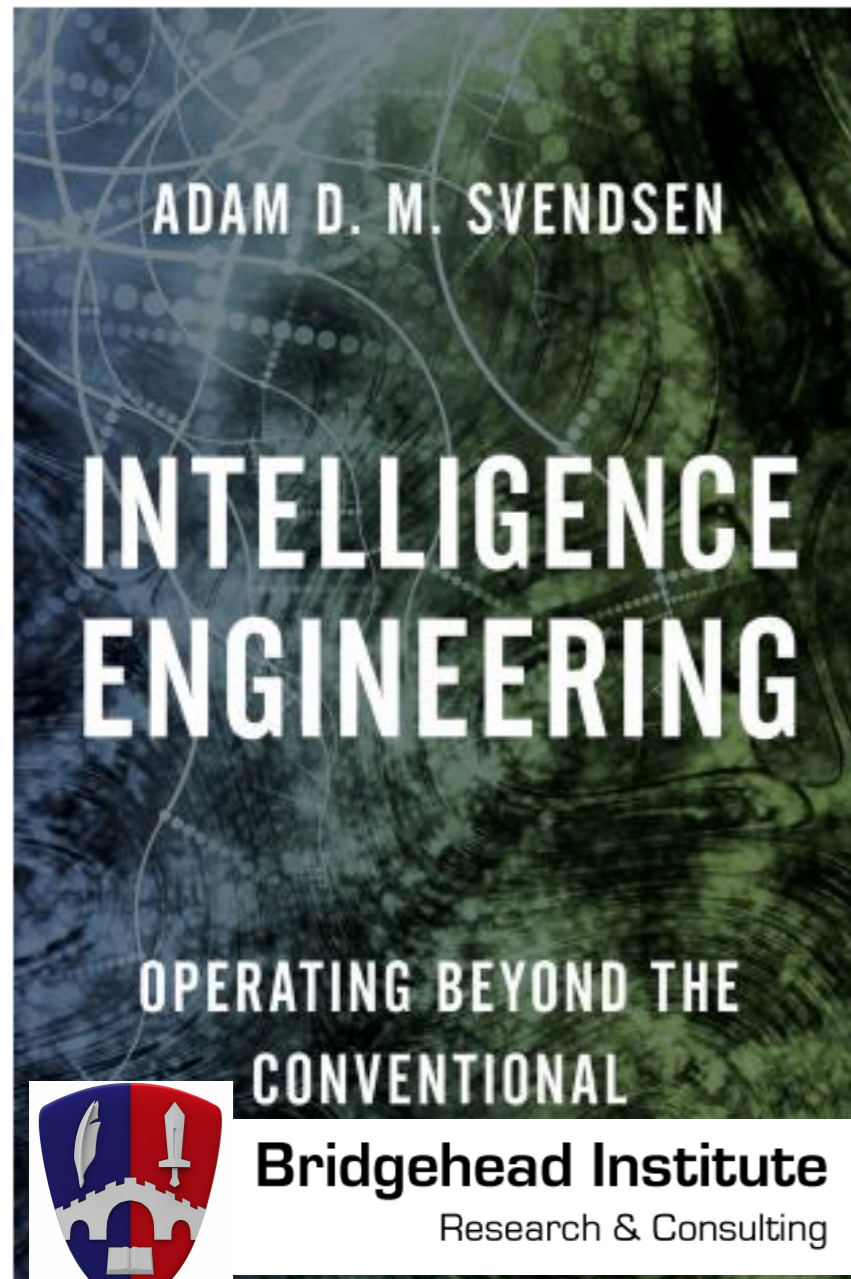
Adam D.M. Svendsen, **Intelligence Engineering: Operating Beyond the Conventional** (Rowman & Littlefield / SPIES - Security & Professional Intelligence Education Series, 2017)

Adam D.M. Svendsen, **'Advancing Intelligence Engineering: Operating Beyond the Conventional'**, *Kungl Krigsvetenskapsakademiens: Handlingar och Tidskrift (The Royal Swedish Academy of War Sciences: Proceedings and Journal)*, Nr.2 (Stockholm, Sweden: April/June 2018), pp.178-181

A.D.M. Svendsen (with M. Kruse), **'Foresight and the Future of Crime: Advancing Environmental Scanning Approaches'**, chapter in H.L. Larsen, J.M. Blanco, R. Pastor Pastor, & R.R. Yager (eds.), **Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime** (Springer, 2017)

Also available from online retailers, e.g. Amazon.