INTRODUCING INTELLIGENCE ENGINEERING: OPERATING BEYOND THE CONVENTIONAL

Adam D.M. SVENDSEN *

Abstract

Contemporary defence and security efforts can be viably improved. With an overarching focus on 'ways', 'means', up and across to realising operational and strategic-ranging 'ends', this article advances a substantially-structured, multi-scaler 'intelligence engineering' (IE)-based framework and 'step-by-step' toolbox useful for both deployment and employment for a multitude of purposes - essentially whatever is to be accomplished. As this article goes on to reveal, the IE framework can contribute towards helping progress several intelligence and knowledge-related tasks. Both 'situational awareness' to deeper-ranging 'contextualisation' assistance value is offered. Demonstrating how they can be best harnessed, the different process 'steps' cover diverse areas such as, inter alia: 'focus/topic selection' through to the fashioning of 'signifier node(s)' for helping in decision-making both now and into the future. Concluding, this article highlights that the entire process involved facilitates: (i) greater risk appreciation; and then (ii) subsequent risk management; as well as even advancing (iii) risk engineering to resilience qualities, in overall defence and security enterprises and endeavours during an era when much uncertainty is encountered.

Keywords: *intelligence, intelligence engineering, 'step-by-step' toolbox.*

Introduction

This article introduces and further advances the concept of '*Intelligence Engineering*' (IE).[1] At its most diverse, IE is defined as:

> *the use of scientific and technical knowledge to artfully bring about (deliver or implement) the design, building, and use of engines, machines, and structures, and equally the study and activity related to the modification or development of those*

* PhD (Warwick, UK) is an intelligence & defence strategist, educator, researcher, and consultant, adam@asgonline.co.uk

[1] Due to the constraints of limited space in this short introductory article, for more detailed insights into 'Intelligence Engineering', readers are directed to see as discussed throughout the book, A.D.M. Svendsen, *Intelligence Engineering: Operating Beyond the Conventional* (New York: Rowman & Littlefield / Security & Professional Intelligence Education Series - SPIES, 2017).

> *entities, in order to imagine, design, create, make, operate, maintain, and dismantle complex devices, machines, structures, systems, and processes that support and/or disrupt human endeavour occurring both in and/or overlapping with the more specific intelligence context—spanning both human intelligence (HUMINT) and technical intelligence (TECHINT) realms…*

In turn, the intelligence context:

> *[S]ignificantly involves the collection and processing (analysis) of information that is particularly of military and/or political value, and which especially (and purposefully) relates to international relations, defence, and national (extending to global, via regional) security (threats, encompassing at their most broad, the full-spectrum of issues-problems-hazards-up-to-risks confronted). The last of these efforts frequently also involves secret (covert and/or clandestine), and often (although not exclusively—as private and sub-/non-state actor contributions are also included) state activity conducted by specialized 'intelligence' institutions (or organisations) to understand or influence entities.*[2]

In its main, this article contends that the 'IE framework' that is introduced and advanced here is relevant for several key reasons. Notably, these reasons include such as for the *functional purposes* of: first, conducting successful risk analysis and assessment/estimate work; to, second, for assisting with risk management activities; and for, third, helping to facilitate resilience in overall defence and security-related contexts (however those contexts are precisely conceived in all of their detail).[3]

This article further argues that IE work is done for much-needed sophisticated: (a) 'context appreciation' and deeper-to-wider understanding/ knowledge-related work (namely, recognised analysis and assessment/ estimation - e.g. G/J2 Intelligence - activities); and then (b) improved 'solution-fashioning', relating to event and development shaping and transformation tasks (acknowledged as engineering and building/synthesis - e.g. G/J3 Operations/Training - efforts).[4]

---

[2] *Ibid*, pp.19-20.
[3] *Ibid.*, p.25.
[4] See also A.D.M. Svendsen, 'Advancing "defence-in-depth": Intelligence and systems dynamics', *Defense & Security Analysis*, 31, 1 (2015), pp.58–73, and A.D.M. Svendsen, 'Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics', *Defence Studies*, 15, 2 (2015), pp.105–23.

Ultimately, the overarching aim of IE is for, firstly, fostering better understanding, and then, secondly, for addressing *complex uncertainty* - a condition that is experienced both now at present and that is readily anticipated to persist in the future. For example, this is as that uncertainty occurs both in and across the full-spectrum range of various operational- to battlespaces from 'war'-to-'peace', as well as more strategically when it exists in a greater overarching manner.[5]

Throughout the conduct of Intelligence Engineering work, there is a strong focus on what can be best termed as 'positioning' and/or 'posturing'. Adoptions of these stances can be summarised, for instance, as better getting 'ahead of' event and development 'curves' as they unfold temporally, at times rapidly. Both *a priori* (before/ahead) and *post facto* (after/behind) concerns and considerations therefore feature substantially - closely relating to situations, events and developments both encountered and experienced (reactively), and/or perhaps even about to be encountered or experienced through their anticipation (more proactively).[6]

The Intelligence Engineering (Ie) Approach

At its most distilled, Intelligence Engineering offers its practitioners, followers and implementers several tools, toolboxes and toolsets they can readily access for use. This approach is represented, for instance, by the harnessing of increasingly familiar 'System of Systems' or 'Federation of Systems' (SoS) concepts, such as represented by PMESII, which relates to Political, Military, Economic, Social, Informational/Intelligence, and Infrastructural indicators and factors - as already used for some years, for example, in the North Atlantic Treaty Organisation (NATO) and during the course of its analysis/assessment (estimation) work.[7]

---

[5] See, for example, as discussed throughout, *inter alia*, G. Eriksson and U. Pettersson (eds.), *Special Operations from a Small State Perspective: Future Security Challenges* (London: Springer, 2017) and C.G. Kwa, 'Postmodern Intelligence: Strategic Warning and Crisis Management', chapter in F. Baudet, E. Braat, J. van Woensel, A. Wever (eds.), *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law* (London: Springer, 2017), pp. 97-118; see also A.D.M. Svendsen, 'Brexit: an agent of "disruptive change" for UK and European intelligence?', *Journal of Intelligence History* (2017).

[6] Svendsen, *Intelligence Engineering*, esp. p.25, p.74 and p.87; see also A.D.M. Svendsen, 'Strategic Futures and Intelligence: The Head and Heart of "Hybrid Defense" Providing Tangible Meaning and Ways Forward', *Small Wars Journal - SWJ* (June 2017).

[7] For more SoS background insights, see via Svendsen, *Intelligence Engineering*, p.144, col.1; for the value of indicator approaches in intelligence analysis contexts, see also L. Madureira, 'Market and Competitor Analysis: Real Exercise', ch. 8 in W.J. Lahneman and R. Arcos (eds), *The Art of Intelligence* (NY: Rowman & Littlefield, 2014), p.133; R.H. Pherson and John Pyrik, *Analyst's Guide to Indicators* (US: Pherson Associates, LLC, 2017).

Perhaps more helpfully, offering advantage, IE also guides its users as to which SoS-based tools, toolboxes and toolsets (such as PMESII introduced above) are the best ones to select and apply. Indeed, this selection or choice consideration resonates whatever the context that might be precisely experienced and encountered (and however, in whichever circumstances), pointing to - at least a degree of - claimed 'multi-scaler' utility that belongs to the overall IE approach (pertaining to its use or help in a number or multitude of differing contexts).[8]

Adopting sheer marketing perspectives, Intelligence Engineering having several tools, toolboxes and toolsets embedded within its overarching approach demonstrates much to several different stakeholders from producers to consumers. What can be communicated most readily here in this article is the 'added value' in the form of 'unique selling points' (USPs) IE overall brings to multiple defence (including military) and security (including policing/law-enforcement) enterprises, such as those ranging across the 'war'-to-'peace' environments, as characterised earlier (see above), and including the high-profile, continuing contemporary fight against so-called Islamic State (IS) - also known as the Islamic State of Iraq and al-Sham or Syria (ISIS), the Islamic State of Iraq and the Levant (ISIL), and Da'esh.[9]

Breaking-Down Intelligence Engineering Into Its Components

To provide a comprehensive summary by way of its further introduction, the IE 'toolbox' consists of five 'toolsets', which each offer a series of 'tools'. Each 'toolset' is also representative of a digestible, 'bite-sized' IE process 'step'.

The different, five Intelligence Engineering process 'steps' drawn upon during the course of pursuing the overall IE approach, cover diverse areas, such as, *inter alia*: (1) 'focus/topic selection' for helping in targeting and with prioritisation tasks; (2) ascertaining which 'federation or system of systems dynamics' are chosen to employ or draw upon during analysis and assessment/estimate work when evaluating entities and/or situations, such as PMESII (see as outlined earlier); (3) the different 'system variables/ attributes' involved, and (4) the 'levels' of experience and hence analysis-to-

---

[8] Svendsen, *Intelligence Engineering*, p.85 and p.104; in a 'hybrid defense' context, see also Svendsen, 'Strategic Futures and Intelligence'.

[9] See, for example, as discussed in A.D.M. Svendsen, 'Developing international intelligence liaison against Islamic State: Approaching "one for all and all for one"?', *International Journal of Intelligence and CounterIntelligence*, 29, 2 (2016); see also 'UK launched cyber-attack on Islamic State', *BBC News* (12 April 2018).

engineering to consider; and (5) the fashioning of 'signifier node(s)' for helping make decisions and for generating 'where next?' responses.[10]

In turn, each IE process 'step' can then be progressed linearly, in sequence, from beginning to end in a highly 'building' and/or 'shaping' or 'framing' manner. Overall, the IE process is arranged as a (semi-)structured analytical framework for risk, offering a lens that provides both intelligence analysis and more advanced Intelligence Engineering inputs to wider processes, extending to the comprehensive evaluation of situations, events and developments, including surrounding their awareness and even steering.[11] Several defence and security endeavours to enterprises gain broadly.

IE Value

As demonstrated thus far, when presented in terms of its 'value', IE clearly boasts many instantly recognisable operational and up and across to strategic 'ways', 'means', and 'ends'.[12] To recap, in its entirety IE encompasses: firstly, intelligence-associated collection/gathering and analysis/assessment (estimate) work; to secondly, the further operationalised implementation of plans and intents generated by commanders and other high-level leaders and policy- to decision-makers.[13]

Several different stakeholders are involved. When thinking with regard to the conduct of many purposed multi-functional to special operations during an overall era of globalised strategic risk, several 'edges' naturally benefit from their 'extra sharpening' to gain advantage: for example, as can readily be acknowledged in competitive terms, such as acquiring and maintaining the initiative or 'upper-hand' over adversaries and rivals - see also, for example, in relation to the previously referenced case of the contemporary fight against so-called Islamic State in the Middle East and elsewhere across the World.[14]

---

[10] These different steps are detailed throughout Chapters 3 and 4 of *Ibid.*

[11] See as summarized in 'Figure 4.6. Overview/Summary', as published in Svendsen, *Intelligence Engineering* at the bottom of p.91.

[12] As highlighted in D.S. Reveron and J.L. Cook, 'From national to theater: Developing strategy', *Joint Forces Quarterly - JFQ*, 70 (2013), pp.113-20.

[13] See, especially, Svendsen, *Intelligence Engineering*, p.21, pp.61-62, pp.72-73.

[14] For more on 'gaining-the-initiative' insights, see as articulated in, e.g., A.D.M. Svendsen, *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem* (Basingstoke, UK: Palgrave Macmillan, 2012), p.17; see also A.D.M. Svendsen, 'Intelligence, Surveillance and Reconnaissance' in D. Galbreath and J. Deni (eds), *The Routledge Handbook of Defence Studies* (London: Routledge, 2018), pp.275-6 and p.280.

Currently, Intelligence Engineering is representative of a very much continuing to evolve work-in-progress. Many parts continue to be worked out in the entirety of their details. IE should retain that status of remaining a 'work-in-progress'. This is in order to adequately maintain the sustained (extending to sustainable) delivery of its end-user (customer, client or consumer) STARC criteria, relating to being: Specific, Timely, Accurate, Relevant and Clear. IE overall considerably reflects the operational parameters that would naturally be expected with such a developing entity unfolding along the lines and in the directions as just characterised.[15]

Further insight is available. IE can also be regarded as being substantially strategic, classroom and workshop-orientated at present - for example, this present configuration is to encourage more 'off-line'-related modes of constructive *critical thinking*, such as 'outside', even 'beyond', 'the box', offsetting less-reflective and reflexive 'no time to think' push-and-pull pressures.[16]

Arguably, into the future, to further extend its current capabilities, the IE approach would benefit from greater automation and from better harnessing 'Big Data' to 'data intelligence' or DATINT inputs in its overall calibration to become even more instantly and operationally relevant. This is so that IE to all of its fusion potential can be used more effectively and efficiently in higher-tempo environments - for instance, relating to the improved collection and gathering to analysis and assessment of data in variously configured operational to battlespaces (whether they are multi-functional or special, see above).[17] Different 'intelligence cycles' involving a series of processes going from 'data' to 'information', 'information' to 'intelligence', and 'intelligence' to 'knowledge', similarly gain via Intelligence Engineering and its more explicit mobilisation.[18]

---

[15] For more on the STARC criteria, see Svendsen, *Intelligence Engineering*, p.143, col.2; see also A.D.M. Svendsen, '"Work-in-progress"? Revisiting the UK Serious and Organised Crime Strategy of 2013 and surveying UK efforts against transnational organised crime', *RUSI Strategic Hub for Organised Crime Research (SHOC) - The Informer blog* (8 November 2017).

[16] See also the different 'modes' or 'systems of thinking' as discussed throughout D. Kahneman, *Thinking, Fast and Slow* (London: Allen Lane, 2011); see also Svendsen, *The Professionalization of Intelligence Cooperation*, p.144; Svendsen, *Intelligence Engineering*, p.102.

[17] Again, see for example as advanced throughout, *ibid.* - including in relation to the so-called Islamic State (IS/ISIS/ISIL/Daesh) and cyber intelligence (CYBINT) mini-case study examples presented over pp.68-69; see also *ibid.*, p.74 and p.102; M.B. Ainsworth, 'Embracing analytics: A path forward for the intelligence community', *SAS Voices blog* (15 September 2017).

[18] Svendsen, *Intelligence Engineering*, p.39.

Conclusions

Through its arrangement as introduced and advanced throughout this article, Intelligence Engineering effectively captures and then addresses the complexity of the '*multi-everything*' nature of operational-to-strategic environments.[19] As already suggested, this is for the multi-functional purposes of (amongst other aims): 'M4IS2: multiagency, multinational, multidisciplinary, multi-domain information sharing and sense making'. Those activities also range across and involve the 'eight entities [of] commerce, academic, government, civil society, media, law enforcement, military and non-government/non-profit' organisations.[20] From these insights so configured, business and enterprise relevance becomes increasingly self-evident.

By pursuing its different steps with adequate due diligence across suitably defined timeframes and locations, IE work helps (1) find and fill the 'gaps' and/or mitigate so-called 'missing dimensions', (2) better address instances of so-called 'cognitive dissonance', as well as (3) helps to 'join/connect-the-dots' in and across all domains of operational-to-strategic activity that span from Human and Information to Sea, Air, Land, Space and Cyber(space).[21]

Furthermore, the Intelligence Engineering tools and frameworks extending to their related concepts as presented throughout this article, help us move across several knowledge domains, from: (i) merely exploiting KNOWN-KNOWNs ('what we know we know'); to (ii) exploring KNOWN-UNKNOWNs ('what we know we do not know'); to (iii) exposing UNKNOWN-KNOWNs ('what we do not know we know'); and to (iv) discovering (potential) UNKNOWN-UNKNOWNs ('what we do not know we do not know') areas.[22]

As the following list demonstrates, this intelligence up and across to knowledge work is useful for a further extensive catalogue of tasks, extending from: (a) operational-to-strategic early warning; (b) over-the-horizon insights; (c) better keeping 'ahead of the curve of events and developments'; (d) distinguishing (weak-strong) 'signals' from (overall/background) 'noise';

---

[19] 'Figure 3.2 - Geospatially Oriented Aspects of the Information Domain of the Operating Environment', published in E.V. Larson, *et al.*, *Assessing Irregular Warfare: A framework for Intelligence Analysis* (RAND, 2008), p.25.

[20] G. Segell, 'Book review: *International intelligence cooperation and accountability*', *Political Studies Review*, 10, 3 (2012), pp.410-11; Svendsen, *Intelligence Engineering*, p.3 and p.66.

[21] For a useful illustration, see the figure titled: 'Cross Domain Synergy: Campaign planners can understand the complex environment by considering each domain and its effects on others', as published in *PRISM*, no.3 (2016), p.16; see also, e.g., via Svendsen, *Intelligence Engineering*, p.136, col.2.

[22] Svendsen, *Intelligence* Engineering, p.73, pp.92-93; see also A.D.M. Svendsen, 'Discovering "unknown-unknowns" & beyond', *Conference paper presented at the 33rd International Symposium on Military Operational Research (ISMOR)*, Royal Holloway, University of London (July 2016).

(e) maintaining the 'edge' and 'initiative'; and (f) for better filtering, targeting, prioritisation, and so forth (again, *whatever* the precise context confronted).[23]

Offering assistance for answering the critical questions of 'So What?' and 'why does this matter?' or 'why should we care?', IE provides added value and USPs contributing towards, firstly, 'intelligence optimisation' tasks (IE analytical input), and then, secondly, 'best event and development transformation' such as through shaping and better situation to event and development awareness and framing to nudging and steering (involving more explicit IE engineering input). This last work is undertaken for the purposes of tailoring most advantageous opportunities and possibilities into the future. All-important *harm prevention* is simultaneously encouraged by these more conscientious activities and thereby improved.

Arguably, Intelligence Engineering responds equally well to critique. Perhaps in the remit of its ambition(s), IE even offers us at least beginning steps towards the 'holy grail' in (at least) Intelligence Studies of a 'grand(er) theory' of intelligence?[24] Granting not only greater intellectual potential that theoretical work can then be realised more practically in action through its greater application and harnessing, using IE as at least a guide for pathways ahead: 'Going forward, the intelligence theorist can learn much from the intelligence engineer, and vice versa.'[25] Ultimately, through mechanisms such as Intelligence Engineering and its extended implementation, contemporary defence and security efforts can be viably improved for better operating beyond the boundaries of the conventional. Difference is created.

* * *

ACKNOWLEDGEMENTS:

The author would like to thank Dr. Stephen Coulthart for his valuable feedback after the presentation of a draft of this article during a panel at the *Intelligence in the Knowledge Society (IKS) Conference 2017*, held in Bucharest, Romania (October 2017), as well as thank an anonymous reviewer for their helpful comments.

---

[23] See, e.g., as discussed in A.D.M. Svendsen and 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* (London: Springer, 2017); Svendsen, *Intelligence Engineering*, pp.92-94.

[24] See, e.g., C. Hillebrand and R.G. Hughes, 'The Quest for a Theory of Intelligence', ch. 1 in R. Dover, H. Dylan, M. Goodman (eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (London: Springer, 2017), pp.1-24.

[25] Svendsen, *Intelligence Engineering*, p.106.

References:

1. Ainsworth, M.B., 'Embracing analytics: A path forward for the intelligence community', *SAS Voices blog* (15 September 2017).

2. Eriksson, G., Pettersson, U., (eds.), *Special Operations from a Small State Perspective: Future Security Challenges* (London: Springer, 2017)

3. Hillebrand, C., Hughes, R.G., 'The Quest for a Theory of Intelligence', ch. 1 in R. Dover, H. Dylan, M. Goodman (eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (London: Springer, 2017), pp.1-24.

4. Kahneman, D., *Thinking, Fast and Slow* (London: Allen Lane, 2011); see also Svendsen, *The Professionalization of Intelligence Cooperation*, p.144;

5. Kwa, C.G., 'Postmodern Intelligence: Strategic Warning and Crisis Management', chapter in F. Baudet, E. Braat, J. van Woensel, A. Wever (eds.), *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law* (London: Springer, 2017), pp. 97-118;

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

7. Madureira, L., 'Market and Competitor Analysis: Real Exercise', ch. 8 in W.J. Lahneman and R. Arcos (eds), *The Art of Intelligence* (NY: Rowman & Littlefield, 2014), p.133;

8. Pherson, R.H., Pyrik, John, *Analyst's Guide to Indicators* (US: Pherson Associates, LLC, 2017).

9. Reveron, D.S., Cook, J.L., 'From national to theater: Developing strategy', *Joint Forces Quarterly - JFQ*, 70 (2013), pp.113-20.

10. Segell, G., 'Book review: *International intelligence cooperation and accountability*', *Political Studies Review*, 10, 3 (2012), pp.410-11;

11. Svendsen, A.D.M., 'Developing international intelligence liaison against Islamic State: Approaching "one for all and all for one"?', *International Journal of Intelligence and CounterIntelligence*, 29, 2 (2016);

12. Svendsen, A.D.M., *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem* (Basingstoke, UK: Palgrave Macmillan, 2012), p.17;

13. Svendsen, A.D.M., 'Intelligence, Surveillance and Reconnaissance' in D. Galbreath and J. Deni (eds), *The Routledge Handbook of Defence Studies* (London: Routledge, 2018), pp.275-6 and p.280.

14. Svendsen, A.D.M., "Work-in-progress"? Revisiting the UK Serious and Organised Crime Strategy of 2013 and surveying UK efforts against transnational organised crime', *RUSI Strategic Hub for Organised Crime Research (SHOC) - The Informer blog* (8 November 2017).

15. Svendsen, A.D.M., 'Discovering "unknown-unknowns" & beyond', *Conference paper presented at the 33rd International Symposium on Military Operational Research (ISMOR)*, Royal Holloway, University of London (July 2016).

16. Svendsen, A.D.M., Kruse, M., '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* (London: Springer, 2017);

17. Svendsen, A.D.M., (2017), *Intelligence Engineering: Operating Beyond the Conventional* (New York: Rowman & Littlefield / Security & Professional Intelligence Education Series - SPIES, 2017).

18. Svendsen, A.D.M., (2015), 'Advancing "defence-in-depth": Intelligence and systems dynamics', *Defense & Security Analysis*, 31, 1 (2015), pp.58–73.

19. Svendsen, A.D.M., (2015), 'Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics', *Defence Studies*, 15, 2 (2015), pp.105–23.

20. Svendsen, A.D.M., 'Brexit: an agent of "disruptive change" for UK and European intelligence?', *Journal of Intelligence History* (2017).

21. Svendsen, A.D.M., 'Strategic Futures and Intelligence: The Head and Heart of "Hybrid Defense" Providing Tangible Meaning and Ways Forward', *Small Wars Journal - SWJ* (June 2017).

22. 'UK launched cyber-attack on Islamic State', *BBC News* (12 April 2018).