Advancing Intelligence Engineering
Operating Beyond the Conventional

by Adam D.M. Svendsen

Resumé

Artikeln presenterar och vidareutvecklar konceptet "Intelligence Engineering" (IE). Författaren konstaterar att IE-ramverket, presenterat under rubriken "Bridgehead Methodology" , är relevant för riskanalys, riskhantering, samt för uthållighet. Artikeln argumenterar också för att arbetet med IE är viktigt för att förstå sammanhang samt generera framtagandet av lösningar. Det övergripande syftet med IE är bättre förståelse samt bättre hantering av komplex ovisshet.

THIS ARTICLE INTRODUCES and further advances the concept of "*Intelligence Engineering*" (IE).[1] It contends that the presented IE framework (also known as the "Bridgehead Methodology", named after the author's research, education/training & consulting enterprise and venture, the Bridgehead Institute), is relevant for several key reasons – notably, for the functional purposes of: firstly, conducting successful risk analysis and assessment/estimate work; secondly, for assisting with risk management activities; and, thirdly, for helping to facilitate resilience.[2]

The article further argues that this IE work is done for much-needed sophisticated: (a) "context appreciation" (analysis and assessment – G/J2 Intelligence) and deeper-to-wider understanding/knowledge-related work; and then (b) improved "solution-fashioning" (engineering and building/synthesis – G/J3 Operations/Training) event and development shaping and transformation tasks.[3]

The overarching aim of IE is for, firstly, better understanding, and then, secondly, addressing complex uncertainty, experienced both now and readily anticipated in the future. For example, uncertainty occurs both in and across the full-spectrum range of operational – to battlespaces from "war" -to- "peace", as well as more strategically.[4]

Throughout the conduct of IE work, there is a strong focus on positioning. This 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 feature substantially.[5]

IE: Value

When presented in terms of its "value", IE boasts many instantly recognisable operational, and up to and including strategic, "ways", "means", and "ends".[6] 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.[7]

When thinking with regard to the conduct of 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 over adversaries and rivals.[8]

IE: Approach

At its most distilled, IE offers several tools, toolboxes and toolsets. This is represented, for instance, by the harnessing of increasingly familiar "System of Systems" or "Federation of Systems" (SoS) concepts.[9]

Perhaps more helpfully, offering advantage, IE also guides which SoS-based tools, toolboxes and toolsets are the best to select and apply. Indeed, this 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.[10]

Adopting sheer marketing perspectives, IE having several tools, toolboxes and toolsets embedded within its overarching approach demonstrates much. What can be communicated most readily 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 "war"-to-"peace", as characterised earlier (see above).[11]

Breaking down IE

To again summarise, the IE "toolbox" consists of five "toolsets" offering a series of "tools". Each "toolset" is representative of a "bite-sized" IE process "step". In turn, each "step" can be progressed linearly in a "building" manner. Overall, the IE process is arranged as a (semi-) structured analytical framework for risk, offering both intelligence analysis and more advanced intelligence engineering (IE) inputs.[12]

The different, five IE process "steps" drawn upon 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 – relating to Political, Military, Economic, Social, Informational/Intelligence, and Infrastructural factors – as used, for example, in the North Atlantic Treaty Organisation (NATO); (3) the different "system variables/attributes" involved and (4) the "levels" of experience and hence analysis-to-engineering to consider; and (5) the fashioning of "signifier node(s)" for helping make decisions and for generating "where next?" responses.[13] Several defence and security endeavors to enterprises gain broadly.

Conclusions

Through its arrangement as introduced and advanced throughout this article, IE effectively captures and then addresses the complexity of the "multi-everything" nature of operational-to-strategic environments.[14] 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."[15] 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 find and fill the "gaps" and/or mitigate so-called "missing dimensions", as well as helps to "join/connect-the-dots" in and across all domains of operational-to-strategic activity that span from Human to Sea, Air, Land, Space and Cyber(space).[16]

Furthermore, the IE tools and frameworks presented throughout this article, help us move across information and 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.[17]

As the following list demonstrates, this intelligence up and across to knowledge work is useful for a catalogue of tasks, extending from: operational-to-strategic early warning; over-the-horizon insights; better keeping "ahead of the curve of events and developments"; distinguishing (weak-strong) "signals" from (overall/background) "noise"; maintaining the "edge" and "initiative"; and for better filtering, targeting, prioritisation, and so forth.[18]

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 (more explicit IE engineering input) for most advantageous opportunities and possibilities.

Arguably, IE responds equally well to its 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?[19] 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."[20] Ultimately, through mechanisms such as IE, contemporary defence and security efforts can be viably improved to better operate beyond the boundaries of the conventional. Difference is generated and advanced.

The author is an intelligence and defence strategist, educator, researcher, and consultant.

Notes

1. For more detailed insights into "Intelligence Engineering", see as discussed throughout the book, Svendsen, Adam D.M.: *Intelligence Engineering: Operating Beyond the Conventional*, Rowman & Littlefield / Security & Professional Intelligence Education Series – SPIES, New York 2017.

2. Ibid., p. 25.

3. See also Svendsen Adam D.M.: "Advancing "defence-in-depth": Intelligence and systems dynamics", *Defense & Security Analysis*, 31, 1 2015, pp. 58-73 and Svendsen, Adam D.M.: "Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics", *Defence Studies*, 15, 2 2015, pp. 105–23.

4. See as discussed throughout, *inter alia*, Eriksson, Gunilla and Pettersson, Ulrica (eds.): *Special Operations from a Small*

State Perspective: Future Security Challenges, Springer, London 2017 and Kwa, Chong Guan: "Postmodern Intelligence: Strategic Warning and Crisis Management", chapter in Baudet, Floribert; Braat, Eleni; van Woensel, Jeoffroy and Wever, Aad (eds.): *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law,* Springer, London 2017, pp. 97-118; see also Svendsen, Adam D.M.: "Brexit: an agent of "disruptive change" for UK and European intelligence?", *Journal of Intelligence History*, 16, 2 2017, pp.108-111; Svendsen, Adam 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,* 2017-11-08.

5. Op. cit., Svendsen, Adam D.M., see note 1, esp. p. 25, p. 74 and p. 87.

6. As highlighted in Reveron, Derek S. and Cook, James L.: "From national to theater: Developing strategy", *Joint Forces Quarterly – JFQ,* 70 2013, pp. 113-20.

7. See, especially, op. cit., Svendsen, Adam D.M., see note 1, p. 21, pp. 61-62, pp. 72-73.

8. As articulated in, e.g., Svendsen, Adam D.M.: *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem*, Palgrave Macmillan, Basingstoke, UK 2012, p. 17.

9. For more SoS background insights, see via op. cit., Svendsen, Adam D.M., see note 1, p. 144, col.1; see also the use of PMESII in Ainsworth, Mary Beth: "Embracing analytics: A path forward for the intelligence community", *SAS Voices blog,* 2017-09-15.

10. Op. cit., Svendsen, Adam D.M., see note 1, p. 85 and p. 104.

11. See also as discussed in Svendsen, Adam 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. See as summarised in "Figure 4.6. Overview/ Summary", as published in op. cit., Svendsen,
Adam D.M., see note 1, at the bottom of p. 91.

13. These different steps are detailed throughout Chapters 3 and 4 of *Ibid.*

14. "Figure 3.2 – Geospatially Oriented Aspects of the Information Domain of the Operating Environment", published in Larson, Eric V. et al.: *Assessing Irregular Warfare: A framework for Intelligence Analysis,* RAND, 2008, p. 25.

15. Segell, Glen: "Book review: *International intelligence cooperation and accountability*", *Political Studies Review*, 10, 3 2012, pp. 410-11; Op. cit., Svendsen, Adam D.M., see note 1, p. 3 and p. 66.

16. 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 op. cit., Svendsen, Adam D.M., see note 1, p. 136, col. 2.

17. Op. cit., Svendsen, Adam D.M., see note 1, p. 73, pp. 92-93; see also Svendsen, Adam D.M.: "Discovering "unknown-unknowns" & beyond", *Conference paper presented at the 33rd International Symposium on Military Operational Research*, Royal Holloway, University of London, July 2016.

18. See, e.g., as discussed in Svendsen, Adam D.M. and Kruse, Martin: "Foresight and the Future of Crime: Advancing Environmental Scanning Approaches", chapter in Larsen, Henrik Legind; Blanco, José María; Pastor Pastor, Raquel and Yager, Ronald R. (eds.): *Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime,* Springer, London 2017; Op. cit., Svendsen, Adam D.M., see note 1, pp. 92-94.

19. See, e.g., Hillebrand, Claudia and Hughes, R. Gerald: "The Quest for a Theory of Intelligence", ch. 1 in Dover, Robert; Dylan, Huw and Goodman, Michael (eds.): *The Palgrave Handbook of Security, Risk and Intelligence,* Springer, London 2017, pp. 1-24.

20. Op. cit., Svendsen, Adam D.M., see note 1, p. 106.