Advancing System of Systems Dynamics (SoSD) in the Cyber Intelligence (CYBINT) domain

Adam D.M. Svendsen, PhD

Copenhagen Institute for Futures Studies (CIFS/IFF), Denmark
asv@cifs.dk and adam@asgonline.co.uk

Following on from previous, more generally-ranging research relating to System of Systems Dynamics (SoSD) being better mobilised and then exploited or harnessed with regard to contemporary defence (including military) and security (including law enforcement/policing) intelligence work, this paper offers a more specifically-focused response to contemporary Cyber Intelligence (CYBINT) challenges.[1]

In its content, this paper further develops frameworks and related analytical concepts intended for advancing practical SoSD thinking in the more specialised domain of CYBINT, particularly as that work unfolds in globalised circumstances. Adopting the approach of building on currently deployed System of Systems Analysis (SoSA) methodologies - for instance, the use of PMESII (in NATO), PESTLE (in EUROPOL), STEEP (in business/commercial/private sector companies), HSCB and DIME (in the US Military), etc. - this paper aims to further advance a joined-up comprehensive systems-based approach towards the problems encountered in the broadly encompassing domain of cyber and CYBINT work.

The frameworks and closely associated analytical concepts advanced throughout this paper are designed to help a wide-range of defence, security and intelligence practitioners with their subsequent System of Systems Engineering (SoSE) efforts. This is however their CYBINT work might be precisely configured/calibrated/scaled, including spatially and/or temporally, together with taking into account those last entities' nexuses in the areas where they fuse. Interest includes: (i) assisting defence, security and intelligence practitioners and decision-makers in better realising successful conditions of 'mission accomplishment', such as through increasing the transformation of events and developments more in their favour; and (ii) helping to better enable those participants listed above to improve their capture of defence, security and intelligence enterprise-relevant characteristics found in the operational-to-battlespaces engaged, wherever they may occur both physically across the world or more virtually in cyberspace.

Essentially, the SoSD involved in the complex CYBINT-related contexts confronted seek to be better observed and then recorded, such as including those SoSDs experienced and encountered in environments where multiple situations of 'complex co-existence plurality' prevail as conditions. The overall aim of what is communicated both in and by this paper is for providing tools and their linked toolboxes and toolsets for enabling the realising of greater - and indeed more refined - contextualisation potential relating to the CYBINT missions and their closely associated areas of endeavour beyond. This seeks to be accomplished both now and into variously ranging futures.

[1] See, for example, Adam D.M. Svendsen, 'Advancing "Defence-in-depth": Intelligence and Systems Dynamics', *Defense & Security Analysis* (2015); see also A.D.M. Svendsen, 'Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics', *Defence Studies* (forthcoming).

By way of background embedding, throughout this paper a focus is maintained on the sustained delivery of the conventional or commonly understood intelligence requirements of the '3Rs', which namely consists of 'getting the right intelligence/information, to the right person/people, at the right time'; as well as continuing to simultaneously better meet and consistently sustain over time in cyber enterprises (operations, missions, etc.) all of the highly-pressing customer/end-user intelligence delivery criteria of 'STARC', which relate to the familiar noteworthy requirements of 'Specificity, Timeliness, Accuracy, Relevance and Clarity' in the CYBINT work conveyed. These 'STARC' criteria are especially pressing requirements to realise during the contemporary 'Big Data' and 'Cyber' age, particularly where challenging areas - for example, 'attribution' in cyber contexts - exist and remain difficult for agencies to address.

In its conclusions, this paper brings to the table some overall suggestions which intend to have potential viable utility in CYBINT work, such as in the form of manifesting refined targeting and the improved calibration of intelligence collection assets (e.g. sensors). Especially, this is while a wide-range of practitioners (as outlined above) strive to navigate several multi-functional operations (MFOs), which range from 'war' to 'peace', and as they strive to cover the full-spectrum of diverse concerns, such as including: crisis management, peacekeeping and humanitarian operations, counter-insurgency (COIN), counter-terrorism (CT), counter-proliferation, and the countering of transnational organised crimes, and so forth. Simultaneously, this is while all of those above MFOs are occurring in and across both virtual (cyber) and the four physical domains of activity (sea, air, land, space) during an overall era of much uncertainty and globalised strategic risk (GSR).

Ultimately, in this paper, a fast, constantly looping, feedback process of 'context appreciation' (for 'situational awareness') and 'solution fashioning' (for 'response calibration/configuration') is found to remain enduringly important in the CYBINT domain. That process is worthy of reiteration, including in relation to areas such as networked (network-centric) warfare. Generally, grander strategic, architectural and event and development shaping approaches - including needing ever greater structural and cultural efforts - emerge as especially pressing to be adopted. Particularly, this is for the purposes of generating more agile and positive-leaning, advantageous possibilities and opportunities into the future in both CYBINT work and in the domains of interconnected activity that extend beyond.