30th Annual INCOSE international symposium
Cape Town, South Africa
July 18 - 23, 2020

Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering

Rick Dove
Paradigm Shift International
dove@parshift.com

Keith D. Willett
Department of Defense, USA
Keith.Willett@incose.org

Abstract. *Security orchestration* is the command and control behind security operations. *Command* includes governance and adjudication logic and rules. *Control* includes the messaging infrastructure and message set for bidirectional communication between the orchestration engine and the constituent parts of its enclave. Open Command and Control (OpenC2)[1] is one effort advancing the messaging infrastructure and message set. Automating the command portion of orchestration remains largely unexplored and will emerge as a symbiosis between people and technology. Technology will have some autonomy including the ability to establish and sustain relationships (argued in a social sense) with other technology. To help facilitate trust relationships and interactions that secure the respective systems and their environment, *techno-social contracts* are explored as an approach to explicitly encode technology-to-technology rules of intra-protection and inter-protection as part of security orchestration.

Introduction

The Future of Systems Engineering (FuSE) is an INCOSE led multi-organization collaborative initiative that has identified a number of specific topics to be investigated (INCOSE nd). The authors of this paper accepted the responsibility to lead and initiate the FuSE topic on security. This paper and another (Dove, Willett 2020) attempt to lay some foundation thought for further security-topic project work.

The future of systems engineering and of systems security are both determined by the nature of the environments in which the system of interest (SoI) and the process that produces the SoI will operate. Those environments contain fitness functions that naturally select compatible approaches and select out those which aren't compatible, with prejudice. We don't have to guess at what those environmental shaping forces will look like. William Gibson's frequently repeated quotation tells us why: "The future is already here – it's just not very evenly distributed[2]." We just need to look

[1] https://openc2.org/, last accessed 10-Nov-2019

[2] Gibson verbally delivers his famous quotation in a 30-Nov-1999 NPR recording. He claims he never wrote it. https://ondemand.npr.org/anon.npr-mp3/npr/totn/1999/11/19991130_totn_science_fiction_becoming_science_fact.mp3. See https://quoteinvestigator.com/2012/01/24/future-has-arrived/ for more detail on origin.

around for what is already happening. These sage words guide both the need and intent behind this paper's purpose.

The purpose of this paper is to explore the concept of *techno-social contracts* as an approach to explicitly encode technology-to-technology rules of intra-protection and inter-protection as part of security orchestration.

Need: Quick detection and mitigation of innovative attacks.

Intent: Behavior-based threat detection with immediate response, distributed among a team of collaborating and cooperating system components, with human governance when necessary.

The cyber-physical-social aspects of systems engineering are gaining attention in the social dimension principally for human-human and human-technology interaction. This paper suggests that systems and systems of systems can be viewed as social communities of technical elements, where security of the community and its technical members can benefit from collective and distributed mutual protection behaviors. The intent of this paper is to show that mutual protection behavior among system technical components is both beneficial and possible.

Some may question the extension of social concepts to non-organic system element; but it is the behavior of interactions among community members rather than the nature of community members that makes this appropriate. It should come as no surprise that robot-to-robot social interactions and communities have already received attention, e.g. (Duffy 2004). Though Duffy is concerned with robots, he makes a good general case of considerations for social interactions among non-robotic system components. More will be said of Duffy's work later.

The future of systems engineering will necessarily produce systems that are dynamically attentive and responsive to the environment in which they operate. A system interfaces with, and interacts with its operating environment and remains viable (capable of working successfully) and relevant (appropriate to current desires) only to the extent to which it is operationally compatible with the *current order* (Willett 2020). Environmental factors include shaping forces that define that which is necessary for constituent systems to remain compatible with the environment. A change in environmental shaping forces may require change in the systems within that environment for those systems to remain viable and relevant; or, in other words, for the system to remain compatible with the current order. One might say that the *current order* tolerates a clear and present system only to the extent that homeostasis can be maintained or effectively readjusted.

FuSE recognizes that both systems and their environments are becoming more complex, that systems belong to systems of systems, that a system's operating environment is a system of systems, and that the current order and constituency of the external and internal environments are unpredictably dynamic. These unpredictable dynamics require equally dynamic security strategies and structures. The adversary is agile – initiating relentless innovations to disrupt system functionality and compatibility with the current order, which requires an equally agile security capability. Agility is a capability for responding effectively in dynamic situations, often of unexpected nature. As one objective, agile operational security should offer some means to address new security threats that arise in real time, with resolution in cyber-relevant time (Herring and Willett 2014).

Offering a foundation for agile operational security in the Future of Systems Engineering is the objective of this paper, with the intent to explore how a mutual protection pact among non-organic system components might inform operational strategy. Inspiration for this approach follows.

In 1762 the French philosopher Jean-Jacque Rousseau wrote *On the Social Contract*, translated into English more recently by Maurice Cranston (Rousseau 1762). The book deals with the concept of a social contract among members of a society to counter the deleterious effects of individual self-centered behavior. A social contract is an implicit cultural agreement or contract among members of a society that "essentially binds the members into a community that exists for mutual preservation (SparkNotes nd)."

The next section introduces the concept of a social contract for mutual protection among technical community elements. Sections that follow reviews some prior work, expands on that work with some suggested strategies for consideration, and offers concluding remarks before finishing with next steps.

Techno-Social Contracts

Consider a *society* to be a group of entities existing together in an ordered community. As people started living together in clans, villages, towns, and cities, they tended to aggregate with others of similar values. They entered into implicit social contracts for mutual cooperation to ensure a certain quality of life including safety and security. Those willing to participate were welcome. Authoritative hierarchies were established to formalize and enforce the rules (government). Those who violated the social contract were tried, acquitted, punished, exiled, or killed. Such communities were self-forming with some active recruitment of others who would add benefit, and active repelling of those deemed a threat. A social contract may be *cultural* (emergent from behavior) and/or *authoritative* (laws set by a governing body).

The story of Peyton Quinn will provide a conceptual example. Peyton has a conscience, or so it seems. That voice that says you did something that probably caused others some problems, and you ought to fess up. Peyton resides in a gated community that has a social contract for mutual protection. A bit like neighborhood watch, but a lot more. The gate didn't stop an intruder, evidenced by a mess made around the place where a neighbor's keys were kept. Payton's conscience gets the upper hand and notifies the community association as well as the neighbors. The association responds shortly thereafter with a community broadcast that says a few residents are noticing security problems, and recommends all go on high alert. Peyton double locks the doors, increases surveillance by cutting back on editing some videos as planned, and calls the cleaners to fix the mess that the intruder made. Peyton Quinn is a blazing fast hardware/software techno-social device – pay a ton for your edits, quintuple what software would have cost.

In technology, social contracts emerge from how people code social activity into the components according to a set of governing rules for system behavior. From a strict *contract* point of view, technology obeys the terms of the contract writ by the human creators. Artificial intelligence (AI) provides the ability for the technology to deviate from the strict contract and establish its own set of rules. Similar to people, techno-social contracts emerge and evolve in part from the need for self-protection.

The emerging concept of loss-driven systems engineering (LDSE)[3] explores the focus and nature of self-protection that will have an effect on techno-social contracts. The ultimate self-protection is to sustain value-delivery via many means, one of which is security. This implies the need for security to safeguard those system characteristics on which value-delivery depends. This also implies establishing relationships with other systems to compensate for some degradation or disruption. For example, System X requires some input to which it has lost access (e.g., human equivalent of needing a bank loan but lacking the collateral to obtain one). System X therefore obtains necessary inputs from System Y (e.g., human equivalent of procuring funds from a loan shark). While the loan is not strictly security, it directly enables System X to sustain value-delivery. The exploration herein acknowledges the complexities in sustaining value-delivery interwoven throughout the many LDSE domains, but narrows focus to security.

Prior Techno-Social Thought

Brian Duffy has a body of work toward the realization of socially interactive robots that collaborate and cooperate as a team to achieve a collective mission. In (Duffy 2004) he deals directly with mobile robots, but at core he discusses a social framework for a community of non-organic entities that can sense some things about their environment and other entities, know some things about themselves and other entities, and have a socially cooperative role to play. Social functionality he suggests manifests from four social attributes possessed by entities: identity, character, stereotypical representations, and role.

- Identity: "When social interaction exists, each element of the social group must be able to be differentiated from others. [They] require a sense of themselves as distinct and autonomous individuals obliged to interact with others in a social environment."

- Character: "The combination of perceived features or qualities that distinguishes one entity from another in that entity's social envelope."

- Stereotypical representation: "…perceived identity of another should be strongly founded on some fundamental set of internal and external attributes that describe [entities]. This is achieved by the use of stereotypical representations, or stereotypes. A fixed subset of internal and external attributes comprises the stereotype with which each [entity] is associated."

- Role: "The characteristic and expected behaviour of an individual with regard to a particular social goal or task within a social collective of individuals."

A lot of what Duffy's paper discusses can usefully inform next steps of techno-social system designs, and is beyond this paper's foundation focus. This reference to Duffy's work is meant to show that there is existing work by others in the techno-social sphere, and to inspire subsequent work in this vein for security.

A non-author-attributed DHS white paper published in 2011, entitled Enabling Distributed Security in Cyberspace, provides an initial framework for consideration, and recognizes the concept of social relationships among inanimate devices. That report addressed the "building of a healthy and

[3] INCOSE INSIGHT Oct 2020 on Loss-Driven Systems Engineering, publication pending.

resilient cyber ecosystem," composed of people, organizations, devices, and processes. The section on Attributes of Healthy Participants spoke principally and specifically to eleven attributes of "healthy cyber devices (DHS 2011, pp. 24-25)." Attributes below are reproduced verbatim from the report – with no further elucidation than what appeared in the report – and is offered simply as evidence of prior thought on techno-social relationships that can lead to "Automated Courses of Action (ACOA's)."

"Self Aware. Having the ability to collect information about security properties, draw conclusions, and report or act upon the conclusions."

"User Aware. Having the ability to collect or receive and process information about supported users, missions, or business processes or assigned role in a larger cyber infrastructure plus ability to draw conclusions, report or act upon the conclusions, and implement policies that assure user privacy."

"Environmentally Aware. Having the ability to collect or receive and process information about the security of surrounding cyber devices of interest or the cyber environment, draw conclusions, and report or act upon the conclusions."

"Smart. Having the ability to retrospectively examine events and associated responses, correlate historical patterns with current status data, and either select from a range of ACOAs [Automated Courses of Action] or formulate a new ACOA."

"Autonomously Reacting. Having the ability to initiate an ACOA."

"Dynamic. Having the ability to alter appearance or persona. Ideally, alterations are enacted on cycle times that are shorter than target acquisition and attack execution times."

"Collaborative. Having the ability to work in partnership with other participants to collect and assess security information, and select, formulate, or alter an ACOA intended to counter an attack or sustain priority services."

"Heterogeneous. Having the ability to collaborate with other participants using a common communications channel despite differences in affiliation, security policies or service level agreements."

"Diversifying. Having the ability to sense the appearance or persona of surrounding devices and to make oneself different from other devices."

"Resilient. For cyber defense purposes, having sufficient capacity to simultaneously collect or receive and assess security information, execute any ACOA, make alterations to the ACOA as needed, and sustain agreed upon service levels."

"Trustworthy. Performing as expected – and only as expected – despite environmental disruption, user and operator errors, and attacks by hostile parties."

Considering Techno-Social Security Strategies

A social focus has patterns to draw upon from mutual security practices in human and animal social groups. The social focus in this paper is on technology-technology relationships rather than

relationships involving humans as participants. Technology includes what would be called devices, components, systems, and systems of systems.

Self Protection. When a techno-social contract is present there is an obligation for participants to perform on that contract, seemingly to the benefit of others but in reality it is a contract entered into for purposes of optimizing self-protection.

Self Aware. Techno-social capabilities rely on self awareness, as socialness is a relationship between self and others. How much self awareness does a participant need? Minimally, awareness of the functional exchanges that establish interactive relationships with other participants that warrant attentive interest. Maximally, perhaps, as follows.

Self Behavior Judgement. This is somewhat like a conscience, an independent local agent that evaluates behavior for expected norms and deviations that constitute abnormality. This approach doesn't rely on the sustained integrity of others to make that judgement, distributes watchfulness diversely and widely, and is independent of potentially aberrant performance mechanisms, regardless of cause. Such an agent might be contained within the participant or as a separate participant-dedicated companion. See (Horowitz 2015) for a functional example.

Self Behavior Mitigation. A self judgement may have different levels of confidence. Some may be sufficient for unilateral immediate action. An extreme example proposed for ad hoc networks includes the ability for a node to commit suicide for the greater good. Another participant type might call for a wipe and reload. A less confident judgement may call for consensus among peer participants or appeal to a higher authority, perhaps a participant that functions as community overwatch attentive to multiparticipant appeals, or a human.

Peer Behavior Judgement. Peer-behavior monitoring and judgement occurs naturally and constantly in social animals. Each member of the group evaluates the others for adherence to social norms and threats to social coherence and security. Humans monitor the behavior of others in ways more sophisticated and more complex than animals of lesser cognitive capability. A techno-social participant interacts with other participants through communication and observed behavior, can learn or be told what to expect as normal, and vet for normalcy before, during, or after acting upon it. Literature supporting concepts and methods for peer behavior monitoring among unmanned autonomous systems is reviewed in a two-part journal paper in (Dove 2009a, 2009b). Trust but verify might be a polite operable phrase; but at core that phrase is fundamentally about the need for distrust.

Peer Behavior Mitigation. Rogue elephants are the result of banishment for unacceptable behavior. Social insects are known to restrain and even kill members of the group that overstep certain social bounds. One of the 911 planes had passengers who took preventive action against the attackers. Nodes in some ad hoc networks will take a vote on questionable communication behaviors experienced with specific nodes, and take collective action to refuse further interaction with a node that gets bad vote results.

Peer Collaboration. Vehicular communication systems are computer networks in which vehicles and roadside units are the communicating nodes, providing each other with information, such as safety warnings and traffic information. They can be effective in avoiding accidents and traffic congestion. Both types of nodes are dedicated short-range communications devices. Vehicular

communications is usually developed as a part of intelligent transportation systems (Wikipedia: "Vehicular communication systems").

Adaptable Attention Priorities. *Maslow's [human] hierarchy of needs* (Wikipedia) contends that fuel and security are the first two of six, sustained existence needs taking precedence over higher level purpose needs. This is seen in robotic mobile devices that interrupt their tasks to seek an electrical outlet, and in devices and operating systems with a variety of anti-tamper detection and prevention capabilities (short of self-destruction). Figure 1 provides a notional technical hierarchy of needs.

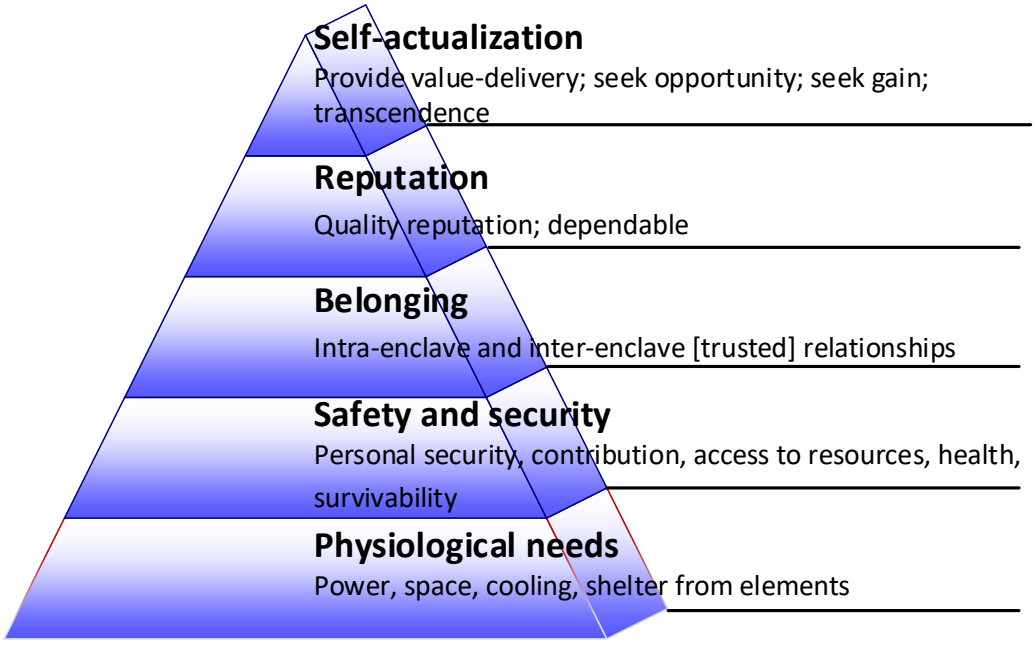

Figure 1: Technical Hierarchy of Needs

Diversity. The DHS white paper discussed earlier suggested one attribute that was difficult to understand initially – *Diversifying* – as there was no further elucidation. Subsequent thought appreciates the security socially attentive load on participants that attempt to cover a large awareness area, and the inefficiency of duplicating the same measures of their neighbors. All members don't have to participate, and all participants shouldn't be looking for exactly the same list of things. One way this could be implemented might be to have a selection of (work intense) things to do that is randomly down selected by or for each component. Gal Kaminka makes this case in his doctoral thesis (Kaminka 2000) for distributed social behavior monitoring and detection, showing that a centralized monitor does not do as well as multiple monitor/detectors among socially aware participants. He also shows that this can be accomplished effectively without any one participant monitoring all participants, and without all the participants having this monitoring capability.

Heterogeneous Awareness. A recent study of grey squirrels (Lilly, Lucore, and Tarvin 2019) found that signals from multiple bird species are used by them to indicate a present threat is in the area, as well as to indicate that no immanent threat is present. Normal calm bird chatter finds the squirrels attending to foraging tasks, while alarm notes cause heightened agitation and evasive

moves. Technical participants that can receive signals about the general state of alarm or calm in other participants not in direct peer communication can be used to ratchet the relative device attention level between self protective activity and purpose. Heterogeneity differs from diversity in that different social sub-groups have some cross communication, whereas diversity is concerned with a single social sub group.

Encoding Techno-Social Contracts

Keep things as simple as possible, but not simpler[4]; too complex evades understanding and too simple loses meaning. Simple rules may result in emergent behavior from the collective unachievable by any individual member. Duffy's work (Duffy 2004) introduced earlier suggested a four attribute social functionality framework "to facilitate the resolution of allocating social tasks without becoming overwhelmed by the added complexity of the [participant's] environment."

For another example, platooning of autonomous ground vehicles (Oquendo 2019) is shown effectively accomplished with three simple encoded social behavior rules: separation (don't get too close), cohesion (stay close enough to remain a neighboring group), and alignment (go generally in the same direction). In this example there is no designated platoon leader, a vehicle sensing proximity of another vehicle activates the rules. A translation to mutual security participants might be proximity sensing based on peer communication, cohesion accomplished with persistence of communication, separation accomplished with diversity in security attention, and alignment accomplished with the nature of the social contract.

Techno-Social Contract Boundaries

The orchestration engine has purview over an enclave (authoritative boundaries). There is the concept of *intra*-enclave orchestration, which is more local; and, *inter*-enclave orchestration for coordination among systems in a system-of-systems. At the least, a techno-social contract exists within an enclave. The enclave may be one of many existing under a broader authoritative umbrella (i.e., a system of systems) where all the constituent systems share the same techno-social contract. Alternatively, the constituent systems may adhere to macro-level rules while maintaining a degree of autonomy for establishing local rules. Techno-social contracts may vary among cooperative as well as competitive systems.

Enclaves may accept new participants seeking membership. As part of sustaining value-delivery, enclaves may recruit new systems as members. As part of sustaining value-delivery, systems may seek membership in larger enclaves. A system may be a member in multiple larger systems. The active seeking of new members may encounter conditional participation; e.g., the sought after system may request adjustment to the social contract in the form of a rule addition, elimination, or modification; e.g., I'll join your group if you accept my rules.

There are techno-social contract boundaries of *authority* (governance), *adjudication* (allowable modification; degree of modification per instance and cumulative degree of modification over time), and *imposition* or colonization to spread the use of its own rules in order to sustain value-delivery. Permission of modifications to the techno-social contract seems reasonable within

[4] Albert Einstein

certain boundaries. One of the many challenges is to specify the baseline for those boundary deviations such that each subsequent small variation doesn't end up with completely diametric rules over time. In trite terms, positive change is good, negative change is bad. Defining what constitutes good and bad and the degree of small good changes that cumulatively result in bad remains a challenge.

Concluding Remarks

In human society compelled satisfaction of another's request or demand isn't being social. The essence of being social is an interaction that isn't compulsory, at least potentially confers benefit to another, and may require foregoing self satisfaction. It is incorrect to think that a network of communicating nodes constitutes a social network. Trolls on Facebook aren't engaging in a social activity. Being physically located in a bounded community of communicating entities (nodes in a network) doesn't designate that group as a social community. The essence of a social community is the social contract that compels beneficial and selfless interaction. Among humans such a contract is strongest when cultural, with governing laws and legal enforcement when culture is insufficient to constrain behaviors to those deemed acceptable or desirable in a group that interacts.

One might argue that technology is compelled to behave, as it is structured and programmed to do what it does by humans, with no real choice in what it does. But on the one hand this paper has dealt with technology that has been programmed for social awareness in fulfillment of a social contract. On the other hand today's artificial intelligence capabilities already employ learning capabilities that lead to decisions and actions unpredicted and unprogrammed by its human creators.

Novel Contributions

The concept of *the social contract* as proposed by (Rousseau 1762) was introduced – a mutual protection pact behind why humans aggregated as communities. It was suggested that similar interactions among non-human technical elements could form the basis for exploring the concept of a techno-social contract, based on the nature of social interactions rather than the nature of the members in a community,

The work of Brian Duffy was introduced as evidence of prior thought on techno-social system concepts, and as a possible starting point for technical-social contract design.

The concept of mutual protection was then explored for application to non-human aggregations of system elements. The exploration identified some mutual protection strategies from examples among human, animal, and non-human communities for consideration. A novel variation of Maslow's Hierarchy adapted for techno-social systems underscored the role of security as a viability requirement to enable the achievement of purpose.

This paper's thesis is that mutual protection behavior among technical system components is both beneficial and possible. Beneficial in that collaboration, cooperation, and teaming among system elements during system operation offers novel strategy for quick detection and mitigation of innovative security threats. Possible in that human and animal communities employ effectively demonstrated approaches, and some work in non-human socially behaving system aggregations already exists.

This paper set out to address a need (goal) with an intent (strategy).

Need: Quick detection and mitigation of innovative attacks. Innovative attacks have not left an historical knowledge base for here-it-is-again detection. Detecting innovative attacks can be quickest when sensed at the granular level. Mitigation can be quickest when enacted by the detector.

Intent: Behavior-based threat detection with immediate response, distributed among a team of collaborating and cooperating system components, with human governance when necessary. A techno-social community relies on abnormal behavior as an indicator of potential and actual security threats, and has the ability to respond immediately; where response may be unilateral action or a report to a higher authority.

The operational human role is techno-social community governance, higher authority decision making, and techno-social contract enforcement.

Research Needs

Research is needed to identify rules and the resulting emergent self-protective behavior to establish and sustain techno-social contracts. Agent-based modeling can be used to explore initial settings and emergence of simple rules to establish and enforce techno-social contracts for security as part of sustaining value-delivery. This includes encoding rules for the interweaving of explore/exploit decisions. Exploit is continuing with status quo and explore is the seeking of new/alternative means. Exploit if the SoI is providing value-delivery (effective), providing value-delivery within specified performance parameters (efficient), and providing value-delivery with minimal resource expenditure (elegant). Explore if the SoI experiences or anticipates degradation, disruption, destruction, or deception.

Rules will accommodate the application and adjudication for acceptance of new members, voluntary and involuntary departure of members, and behavior monitoring of functions and functional exchanges. The rules apply against a framework of what constitutes normal, deviations from normal that are permissible, and deviations that are considered abnormal. The rules includes adjudication of those members found to be abnormal, deciding on punitive actions according to the degree of deviation ranging among reduction of privilege, temporary isolation, or permanent eviction.

Research for rules should include algorithmic approaches as well as axiomatic approaches to accommodate for AI-driven deviations that may be undesirable. For example, the SoI achieving self-protection by means of widespread destruction of that which it deems a threat. This requires revisiting fundamental axioms like the system shall do no harm, the system shall minimize intentional harm, or the system shall minimize unintentional harm. The area of *AI Alignment* provides a starting point for the encoding of ethics and resolution of moral dilemmas.

Assume techno-social contracts are successful. On the upside, they help systems be mutually self-protective. On the downside, they encode techno-social prejudice that encode limits to seeking opportunity from those that vary too much from acceptable techno-social norms. Being secure by limiting acceptance of those that vary from preconceived rules is one goal; but preferably not at the expense of isolation from those that can contribute to growth.

Next Steps

Our current focus in the security topic within the FuSE initiative is on foundation development – general considerations for shaping the breadth and depth of future solution strategies. This paper and a companion paper (Dove, Willett 2020) offer two initial foundations. This paper suggests a social foundation for security strategies that address the problem space during operation. The other outlines the general problem space for both operations and development, and suggests a foundation for security strategies that address the problem space during development. Both papers are offered as partial foundational thinking for subsequent work on the topic of Security in the Future of Systems Engineering.

Next steps for the FuSE security topic will initiate active collaborations on foundational work: identifying additional foundational areas to pursue, establishing project participants in those different areas, and beginning those projects. These two initial papers are offered as inspirational models for identifying additional work at the foundation level.

Next steps for building upon this paper's foundation need to address means for enabling, designing, and implementing mutual protection social contracts. Enabling includes rethinking security strategy and systems architecture. Designing includes the selection of techno-social strategies and the development of tactical concepts. Implementing includes the employment of an agile systems engineering life-cycle approach that facilitates continuous learning and evolution.

Some of these next steps are likely in process at this paper's publication date; but more is needed. FuSE is a multi-organization collaborative initiative. To be a part of this activity contact the lead author of this paper with your interest.

References

DHS. 2011. Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. 23 March. <www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>

Dove, R. 2009a. Paths for Peer Behavior Monitoring Among Unmanned Autonomous Systems. International Test and Evaluation Association, ITEA Journal 2009; 30: 401–408. <www.parshift.com/s/090901IteaJ-PathsForPeerBehaviorMonitoringAmongUAS.pdf>

Dove. R. 2009b. Methods for Peer Behavior Monitoring Among Unmanned Autonomous System. International Test and Evaluation Association, ITEA Journal 2009; 30: 504-512. <www.parshift.com/s/091201IteaJ-MethodsForPeerBehaviorMonitoringAmongUas.pdf>

Dove, R., K.D. Willett. 2020. Contextually Aware Agile Security in the Future of Systems Engineering. International Council on Systems Engineering, INCOSE International Symposium, Cape Town, South Africa, July 18-23.

Duffy, B. 2004. Robots Social Embodiment in Autonomous Mobile Robotics. International Journal of Advanced Robotic Systems, Volume 1, Number 3, pp. 155-170. <https://journals.sagepub.com/doi/pdf/10.5772/5632>

Herring, M.G., Willett, K.D. 2014. The Future of DoD's Active Cyber Defense. Journal of Information Warfare, April.

Horowitz, B. (Principal Investigator). 2015. Four part System Aware Cyber-Security Project report. Systems Engineering Research Center. Report No. SERC-2015-TR-036-4. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a626823.pdf>

INCOSE. nd. The Future of Systems Engineering. An INCOSE initiative with charter at: <www.incose.org/about-systems-engineering/fuse accessed 2/28/2020>
Kaminka, G.A. 2000. Execution monitoring in multiagent environments. Ph.D. dissertation, University of Southern California. <http://u.cs.biu.ac.il/~galk/publications/papers/phd.pdf>
Lilly, M.V., E.C. Lucore, K.A. Tarvin. 2019. Eavesdropping Grey Squirrels Infer Safety From Bird Chatter. PLOS | ONE September 4. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0221279>
Oquendo, F. 2019. Architecting exogenous software-intensive systems-of-systems on the internet-of-vehicles with SosADL. Systems Engineering. 2019;22:502–518. Wiley Periodicals.
Rousseau, J-J. 1762. *On the Social Contract*. English translation by Maurice Cranston, Penguin Publishing Group, 28-June-1968.
SparkNotes. nd. The Social Contract. Barnes & Noble. <www.sparknotes.com/philosophy/socialcontract/characters>

Biography

Rick Dove is CEO of Paradigm Shift International, specializing in agile systems and security research, engineering, and project management; and an adjunct professor at Stevens Institute of Technology teaching graduate courses in agile and self-organizing systems. He chairs the INCOSE working groups for Agile Systems and Systems Engineering, and for Systems Security Engineering. He is an INCOSE Fellow, and author of *Response Ability, the Language, Structure, and Culture of the Agile Enterprise*.

Dr. Keith D. Willett is a Data Scientist / Enterprise Security Architect for the U.S. Department of Defense with focus on future technologies, science of security, and systems security engineering. He is co-chair of the INCOSE Systems Security Engineering WG and active in working groups for Agile Systems and Systems Engineering, System Resilience, and System Science. He is the author of *Information Assurance Architecture* and many papers on the future of systems engineering and security.