Resolved: Discussions, strategies and efforts towards coordinated defense 'at scale' have limited efficacy should we fail to recognize that 'at scale' requires responses occur in cyber relevant time as well as responses consist of unambiguous and universally understood information models.

We consider the following engineering principles to be consistent with achieving coordinated defense at scale:

- Separation of Concerns:
- Standards based Interfaces:
- All designs and implementations are public knowledge (an extension of Kerckhoff's principle).

Background and Motivation: Cyber systems are subject to a global threat from adversaries that are increasingly dynamic and operate at machine speed. Modern cyber defense products tend to operate in isolation and often statically configured. The use of statically configured point defenses against a global attack surface is not tenable. Future defense systems must be coordinated defenses and timely.

Creating coordinated cyber defense systems in the absence of standards is impractical. The integration of a suite of monolithic products may result in redundant cyber defense functions, incompatible functions and capability gaps. The functional blocks within a given product may be tightly coupled with other functions and the may not be directly accessible by way of an API. Typically, integration efforts are expensive, require customized interfaces, and if tightly coupled, difficult to maintain or modernize.

OpenC2: The Open Command and Control (OpenC2) effort is a technical committee within the OASIS International Standards Body. The purpose of OpenC2 is to define a standardized language for machine to machine exchange of command and control messages for cyber defense.

OpenC2 Scope, Assumptions and Principles: A high-level decomposition of the functional blocks within a cyber-defense system is roughly analogous to an OODA loop.

OpenC2 will address the acting portion of cyber defense by focusing on the creation of specification that enable unambiguous machine-to-machine communications and assumes the other functional blocks are in place. These assumptions permit OpenC2 to define a simple and low overhead language that is agnostic of any particular transport protocol or information assurance implementation.

OpenC2 makes three key assumptions with respect to cyber-attacks and defense. In the context of cyber defense, the high-level action that defenders take has been stable for years (such as block, deny, redirect). Similarly, what we are acting on has also been consistent for quite some time (such as malicious files, compromised

users, compromised devices, and unauthorized users). The area of active research, development and innovation takes place in the cyber defense products, example; virus scanners have evolved from static signature based to sophisticated Bayesian classifiers and machine learning.

OpenC2 Strategy: OpenC2 will produce a 'Language Specification' that defines the actions (what we are doing) and targets (what we are acting on). The Language Specification defines the syntax of the language and the means to extend the language. The language specification is consistent with the first two assumptions.

OpenC2 will create a suite of 'Actuator Profile' specifications. In the context of OpenC2, an actuator is the entity that executes the command. The purpose of the actuator profile is to identify the appropriate actions and targets that are applicable or make sense in the context of a particular cyber defense function. A suite of Actuator Profile specifications allows vendors to focus on what is relevant to their product, accommodates new technologies and functions while minimizing the need to revise the language specification. This is consistent with the third assumption.

OpenC2 will create a suite of 'Implementation' specifications. By design, OpenC2's scope is limited to the 'acting' portion of cyber defense however, a command and control system requires an assured message fabric and the components of the cyber defense system must be on a standard transport infrastructure in order to interoperate. A given implementation specification will leverage pre-existing standards and protocols to provide transport, key management, information assurance, audit, logging and other external dependencies. By design, OpenC2 is agnostic of the transport layer. This will permit cyber-ecosystems to select the optimal message fabric for their particular requirements and still utilize OpenC2.

End State, OpenC2 Enabled Enterprise:

Ultimately, this suite of documents will enable the mission owner to acquire an OpenC2 enabled enterprise that can be tailored for a particular cyber ecosystem.

The Language Specification will define the semantics of the language and at a high level will capture the breadth of cyber defense technologies.

Actuator profiles will refine the language in the context of particular cyber defense functions. The Actuator profiles will specify to vendor community how to ensure that their products are OpenC2 compliant. Similarly, the actuator profiles will provide a means for the system integrators to determine what a particular product does so that meaningful comparisons are possible.

The Implementation Specifications will document how a system integrator can achieve interoperability of cyber defense functions and address matters that are critical to the success of a command and control system, but beyond the scope of 'response'.