Chapter 6
Cybersecurity Requires a Clear Systems Engineering Approach as a Basis for Its Cyberstrategy

Dr. Raymond J. Curts
George Mason University, USA

Dr. Douglas E. Campbell
Syneca Research Group, USA

ABSTRACT

Systems engineering is the branch of engineering concerned with the development of large and complex systems, where a system is understood to be an assembly or combination of interrelated elements or parts working together toward a common objective. Past experience has shown that formal systems engineering methodologies have not always been successfully applied to large and complex cybersecurity systems. These complex systems have become commonplace when applying cyberstrategies in cybersecurity operations. The ability to build, operate and maintain such systems is crucial to the effectiveness of cybersecurity operations. Most importantly, a cyberstrategy program must surround these systems on a global scale across multiple inter-related platforms. In this chapter, the authors demonstrate why a systems engineering approach is best suited for large and complex information systems used in cybersecurity, as well as the overall cyberstrategies that must also reside over these systems.

INTRODUCTION

Without robust systems engineering methodologies, the realization of complex information systems involving numerous interacting components would be prohibitively expensive, prone to failure and involve timescales unacceptable in today’s cybersecurity industry. By following appropriate, best practice methodologies, highly integrated and complex cybersecurity information systems can be built to interact securely on a global scale. The purpose of this chapter is to build an understanding of systems engineering processes as they apply to a large and complex information system within a cybersecurity environment. By the end of this chapter, the reader should have an appreciation for the environment within which
Cybersecurity Requires a Clear Systems Engineering Approach as a Basis for Its Cyberstrategy

systems engineering occurs; understand the management skills needed to facilitate the development of complex information systems and the cyberstrategies needed in such an environment; and have a clear appreciation of systems engineering as applied to cybersecurity information operations.

It is the intention of the authors to present this chapter along the usual systems engineering lines including some discussion of the basic concepts of system engineering, cybersecurity, interoperability, life cycle support, cyberstrategy operational considerations, and automated tools that can assist with various processes along the way.

BASIC CONCEPTS OF SYSTEMS ENGINEERING, CYBERSECURITY, AND INTEROPERABILITY

Systems Engineering. Systems Engineering is defined as an interdisciplinary process that ensures that the customer’s needs are satisfied throughout a system’s iterative life cycle (see Figure 1). When the system under consideration is something manufactured, like a computer, then its system life cycle usually has seven phases: (1) requirements development, (2) concept development, (3) full-scale engineering design and development, (4) manufacturing and deployment, (5) system integration and test, (6) operation, maintenance and modification, and (7) retirement, disposal or replacement. The system life cycle is different for different industries, products and customers (Chapman, Bahill and Wymore, 1992; Wymore, 1993; Kerzner, 1995; Shishko, 1995). However, even when a system life cycle is defined within the manufacturing process, the authors still question why requirements development comes before concept development (Figure 1). Concept development is the high-level process of determining and understanding customer needs. Without understanding what the customer wants in the first place, it becomes very difficult to discover system requirements. With apologies to Chapman, Bahill, Wymore, Kerzner, Shishko and other developers of the systems engineering process, there still remains a good argument as to why concept development should come first. Some authors refer to phase 2 as preli-
