Systems Thinking for a Secure Digital World

William D. Miller, Innovative Decisions, Inc.

Abstract. The practice of cyber security appears to be predominantly a game of Whac-A-Mole, and the moles are winning! Systems are designed and deployed with security such as it is, grafted on, and the standard response to adversarial attacks is to continually patch the IT and burden humans with process and passwords. We must learn to think systemically to seek advantage, or at least maintain parity over adversarial threats, as our infrastructure becomes more complexly integrated.

Introduction

The stage is set by thriving communities of adversaries who seek all possible means to harm cyber systems and potentially to the infrastructure with which they are integrated. The functions currently performed by cyber security should thwart these adversaries but are too often add-ons rather than inherently designed into the cyber systems. A short history of systems thinking and its relevance to thwarting the threat is established. Then specific actions are identified to achieve the vision of a secure digital world, after the fact.

Cops and Robbers in the Digital Age

Adversarial attacks to compromise cyber systems can be broadly categorized as hacks, social engineering, insider jobs and stupid stuff:

- Hacks include malware, e.g. viruses and worms.
- Social engineering includes phishing schemes to trick individuals into divulging private information that can then be exploited. Social engineering can also be used to gain personal knowledge of individuals and to guess passwords.
- Insider jobs occur when adversaries have trusted access to at least some parts of cyber systems and violate the trust they have been granted.
- Stupid stuff occurs when individuals do not take proper care of information systems and/or personal information. Adversaries are the proactive ones that seek to compromise cyber systems and have the advantage to discover and exploit vulnerabilities on Internet time.

Security Engineering, Such as It [1]

Cyber security tends to have a technology focus and provides a defensive, static, security environment versus the dynamic behavior of its adversaries. The behavior of defensive oriented cyber security is asymmetrical, which gives the adversaries the "first move" advantage that must then be detected, identified, and protected against. The result is patch, upon patch, upon patch in response to adversarial attacks. Cyber security behaves as an evolutionary system, not a purpose-designed system.

A Short History of Systems Thinking

"Systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static 'snapshots.'"
– Peter Senge, 1990 [2].

The most popular definition of systems thinking is arguably defined by Peter Senge, who traces its roots to the feedback concepts of cybernetics and servo-mechanisms. Senge gives substantial credit to Jay Forrester's early work beginning in the mid-1950s in system dynamics. Forrester's stock-flow-feedback structure modeling of General Electric appliance manufacturing plants revealed that the observed three-year employment cycle of hiring and layoffs was attributable to the internal structure of the firm and not to the external forces of the business cycle [3].

A key lesson is that answers and solutions to observed phenomena may be non-intuitive without analysis. Stocks define the states of the system, and the variables defining the changes in states are the flows. The stock-flow-feedback metaphor models n^{th} order difference/differential equations that describe the behavior of a system [4]. Nouns represent stocks whereas verbs represent flows. Stocks send out signals representing information about the state of the system to the rest of the system. Stocks have the following characteristics: memory, ability to change the time shape of flows, decouple flows, and create delays.

Forrester's work bloomed into the System Dynamics Society and The System Dynamics in Education Project at MIT, now The Creative Learning Exchange, championing system dynamics and systems thinking in K-12 education. System dynamics has been applied to business management, sustainability studies, policy analysis and design. The Club of Rome embraced system dynamics in its 1972 report, The Limits to Growth. The methodology also supports agent-based modeling. This author applied systems dynamics in the late 1970s to understanding the cost impact of reported but unfound troubles in the telephone network. This provided the basis to justify a cost-effective system to improve the detection and repair of such troubles.

Figure 1. A simple stock and flow model of inventory.

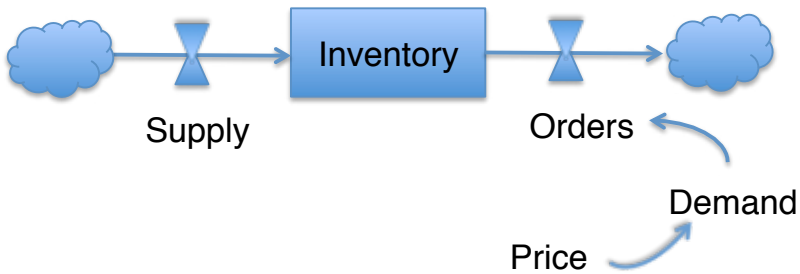
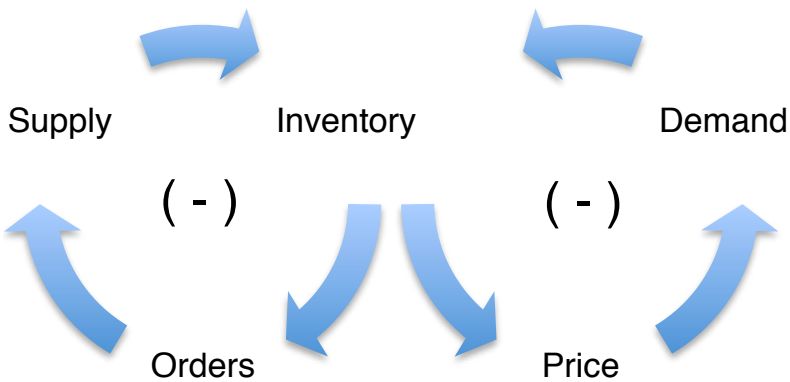


Figure 2: Business inventory causal loop.



Within DoD, CDR Brett Pierson developed a system dynamics model of the FM 3-24 COIN Manual [5]. There are several popular system dynamics software programs available. A simple inventory stock and flow model is shown in Figure 1.

Published in 1980, a classic document of systems is, "Systems 1: An Introduction to Systems Thinking" by Draper Kauffman and precedes Senge's book by a decade [6]. Kauffman's intent was to translate the ideas of systems and systems thinking, which is full of technical jargon and mathematics. He wanted non-expert educators to be able to teach the concepts to K-12 students.

Kauffman defines systems, the concept of feedback and introduces causal loop diagrams to model their behavior. Figure 2 is an example of a causal loop diagram describing the relationship of a business' inventory to price, demand, orders and supplies.

These causal loops are the precursor to modeling the stocks and flows. Kauffman provides a simple taxonomy of systems and their properties, as well as complex system characteristics and problems as shown in Table 1.

Several of the effects that Kauffman identifies are highly relevant to cyber security:

- Systems cope with problems by reacting to warnings.
- The obvious solution often makes things worse.
- Solving one problem almost always creates others.

The soft systems methodology in, "Systems Thinking, Systems Practice" by Peter Checkland was first published in 1981 and has been republished several times [7]. Checkland acknowledges systems engineers' contributions to the mature understanding of hard systems and then identifies the problems extending those paradigms to the unstructured problems of soft systems. Checkland lays out an action research program that led to the holistic methodology for soft systems, especially human activity systems, such as the British Rail System. He uses causal diagrams that are more free form than the formal causal loops introduced earlier.

Derek Hitchins, a contemporary of Checkland, integrates systems engineering and systems thinking in, "Systems Engineering: A 21st Century Systems Methodology" in 2007, with extensive use of causal loops and system dynamics applied to complex systems [8]. Hitchins focuses on defense capabilities, illustrating concepts in the case study of the World War II Battle of Britain Command and Control System.

Peter Senge popularized systems thinking in, "The Fifth Discipline: The Art & Practice of The Learning Organization" in 1990. Subsequent to its publication, Senge co-authored a series of field books applied to a variety of domains. The Fifth Discipline is systems thinking and completes the four disciplines of personal mastery mental models, shared vision and team learning. Senge's laws of the Fifth Discipline and causal loop system archetypes are shown in Table 2. The archetypes are naturally recurring patterns in systems and are represented by formal causal loop diagrams.

John Boardman and Brian Sauser integrated the concepts of causal loop diagrams, soft systems methodology and social network theory with the introduction of the system diagram, or systemigram, conceptual model [9] The systemigram provides a systemic visualization of system complexity and enables the elucidation of the key attributes of emergence, hierarchy and boundary of complex systems. The application of systems thinking is illustrated by the relevant systemigram example in Figure 3 from the Systems Security Engineering roadmap report published by the Systems Engineering Research Center (SERC), a University-Affiliated Research Center of the DoD [10].

Application of Systems Thinking for a Secure Digital World

The International Council on Systems Engineering's "INSIGHT" publication devoted its July 2011 issue to a special feature on "Systems of Systems and Self Organizing Security." The feature specified that:

"Resilient system strategies may be a more manageable way to counter the asymmetry of attack and defense. In recognition that systems will have vulnerabilities that adversaries will attack, and that system design needs mechanisms to weather successful attack and remain viable, engineers are now placing a new strategic priority on system resiliency. Survivability through resilient design is not a new concept, but still remains largely a research activity."

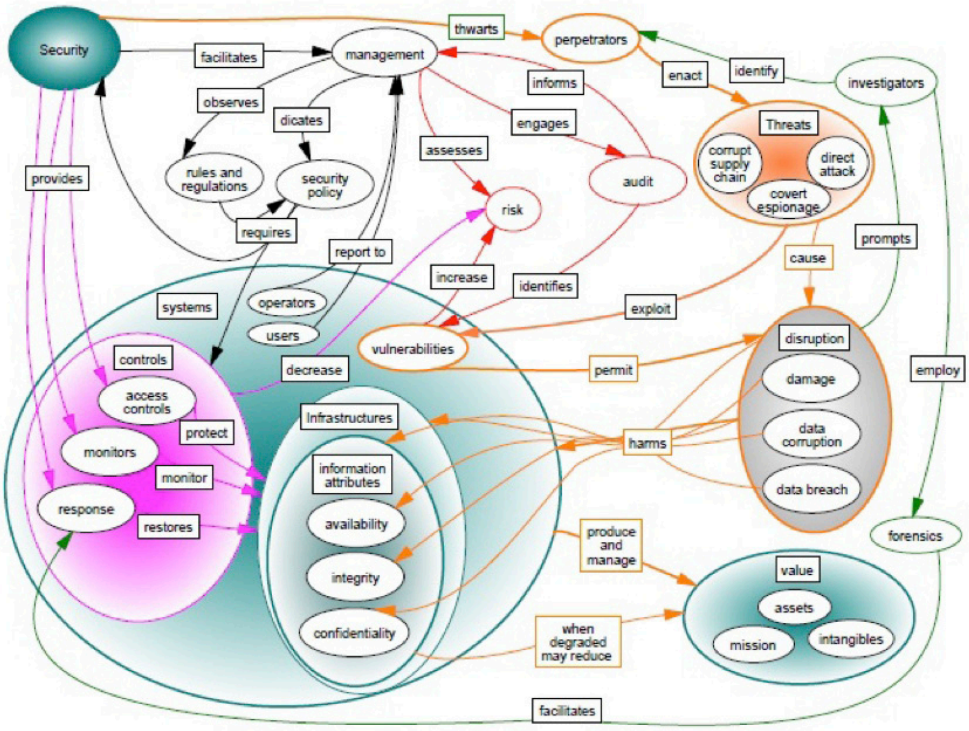
Table 1. Kauffman's system types and properties, as well as complex system characteristics and problems.

System Types	System Properties	Complex System Characteristics	Complex System Problems
Mechanical Human/ Mechanical Biological Ecological Social	Stability Limitations Loose Systems Reaction Times Anticipation Hidden Systems	Self-Stabilizing Goal-Seeking Program-Following Self-Reprogramming Anticipation Environment Modifying Self-Replicating Self-Maintaining/Repairing Self-Reorganizing Self-Programming	Tragedy of the Commons Cost of Information Distortion of Feedback Loss of Predictability

Table 2. Senge's laws of the Fifth Discipline and system archetypes.

Laws of the Fifth Discipline	System Archetypes
1. Today's problems come from yesterday's solutions	Balancing Process with Delay
2. The harder you push, the harder the system pushes back	Limits to Growth
3. Behavior grows better before it grows worse	Shifting the Burden
4. The easy way usually leads back in	
5. The cure can be worse than the disease	Eroding Goals
6. Faster is slower	
7. Cause and effect are not closely related in time and space	Escalation
8. Small changes can produce big results – but the areas of highest leverage are often the least obvious	Success to the Successful
	Tragedy of the Commons
9. You can have your cake and it it too – but not at once	Fixes that Fail
10. Dividing an elephant in half does not produce two elephants	Growth and Underinvestment
11. There is no blame	

Figure 3. SERC systems security systemigram (used by permission).



From the systems thinking perspective, the imperative is that cyber security learning loops must be fastest where the stakes are highest, as when systems become high-value targets under attack by determined, intelligent adversaries. Another systems thinking imperative is that people are part of the system, and therefore the human condition, with all its attributes including social systems and social engineering, must be part of the design formulation for cyber security.

Within DoD, the INCOSE "INSIGHT" article goes on to explain:

"Security has focused on keeping critical technology and information from getting out. However, as DoD systems have come to depend on commercial technology and components that are increasingly sourced through complex global supply chains, a new security emphasis is emerging: keeping malicious or compromised system elements or components from getting in."

The SERC Systems Security Engineering Final Technical Report establishes a research roadmap for DoD, with its executive summary summarizing insights from systems thinking:

"The U.S. needs dramatic improvements in systems security. Current defensive strategies, based principally on strengthening system peripheries, inspections, and similar bolt-on techniques add tremendously to cost and do not respond effectively to the growing sophistication of attacks. Systems cannot be assumed to have static boundaries, static user communities, or even a static set of services."

The report goes on to emphasize the application "of scientific and engineering principles to identify security vulnerabilities and minimize or contain the risks associated with these vulnerabilities." The SERC report is available at <http://www.sercuarc.org>.

Two additional works that address cyber security from a systems thinking perspective are "Enterprise Security for the Executive: Setting the Tone from the Top" by Jennifer L. Bayuk [11] and "Cyber Attacks: Protecting National Infrastructure" by Edward G. Amoroso [12]. Bayuk addresses security leadership and Amoroso proposes a comprehensive national infrastructure protection methodology. The reader is encouraged to become involved in INCOSE working groups and the cyber security professional society organizations.

Homeland Security

The Department of Homeland Security, Office of Cybersecurity and Communications, is seeking dynamic individuals to fill several positions in the areas of software assurance, information technology, network engineering, telecommunications, electrical engineering, program management and analysis, budget and finance, research and development, and public affairs.

To learn more about the DHS Office of Cybersecurity and Communications, go to www.dhs.gov/cybercareers. To find out how to apply for a vacant position, please go to USAJOBS at www.usajobs.gov or visit us at www.DHS.gov; follow the link Find Career Opportunities, and then select Cybersecurity under Featured Mission Areas.

Summary

This paper lays out the context of adversarial threats to cyber systems and taking a systems thinking approach to cyber security in the digital world. Past and current practices of patching vulnerabilities as they are discovered leave the initiative to the adversaries and do not solve the underlying structural problems that exist. Systems thinking addresses the wholeness and interrelated, dynamic behavior of this domain. To quote President Abraham Lincoln, "We must think anew, and act anew." Significant research remains to be accomplished, both theoretical and applied.

Acknowledgements

The author gratefully acknowledges the work of the INCOSE Model-Based Systems Engineering Initiative and the following INCOSE Working Groups for their contributions applying systems thinking to cyber security and infrastructure security: 1) Security Engineering, 2) Systems Science, 3) Resilient Systems, 4) Complex Systems, 5) Autonomous Systems Test, 6) Anti-Terrorism International, and 7) Human Systems Integration. The author also gratefully acknowledges the contributions of the Systems Engineering Research Center investigators who established a systems security engineering roadmap for the DoD. In particular, Dr. Jennifer Bayuk, a colleague at the Stevens Institute of Technology, School of Systems and Enterprises, established the Systems Security Engineering graduate program at the school, was a major contributor in both INCOSE and SERC initiatives, and has been an exceptional mentor in relating security engineering to systems engineering for the author.

ABOUT THE AUTHOR

William D. Miller is executive principal analyst with Innovative Decisions, Inc. and adjunct faculty at the School of Systems and Enterprises, Stevens Institute of Technology. Miller is the deputy technical director of the International Council on Systems Engineering (INCOSE), a nonprofit membership organization that promotes international collaboration in systems engineering practice, education and research. He specializes in systems engineering of government and commercial communications systems and services, working at companies including Bell Labs and AT&T.

Innovative Decisions, Inc.
1945 Old Gallows Road
Suite 207
Vienna, VA 22182
Phone: 908-759-7110
Fax: 703-854-1132
E-mail: wmiller@innovativedecisions.com

REFERENCES

1. Dove, Rick and Bayuk, Jennifer, editors. "Special Feature: Systems of Systems and Self-Organizing Security, 14.2 INCOSE INSIGHT (July 2011).
2. Senge, Peter M. The Fifth Discipline: The Art & Practice of The Learning Organization. New York: Currency Doubleday, 1990.
3. Radzicki, Michael J. and Taylor, Robert A. "Origin of System Dynamics: Jay W. Forrester and the History of System Dynamics." 2008.
4. Forrester, Jay W. Industrial Dynamics. Cambridge MA: MIT Press, 1961.
5. Brett Pierson, Brett. "A System Dynamics model of the FM 3-24 COIN Manual." Warfighting Analysis Division J8/WAD, accessed at <http://www.mors.org/UserFiles/file/meetings/07ic/Pierson.pdf on 4/5/2012>.
6. Kauffman, Jr., Draper L. Systems One: An Introduction to Systems Thinking. Future Systems, Inc., 1980. (Originally The Human Environment: An Introduction to Environmental Systems, developed under a grant to the Office of Environmental Education, Office of Education, Department of Health, Education, and Welfare.)
7. Checkland, Peter. Systems Thinking, Systems Practice. Chichester, England: Wiley, 1993.
8. Hitchins, Derek K. Systems Engineering: A 21st Century Systems Methodology. Chichester, England: Wiley, 2007.
9. Boardman, John and Sauser, Brian. Systems Thinking: Coping with 21st Century Problems. New York: CRC Press, 2008.
10. Bayuk, Jennifer, et al. "Systems Security Engineering Final Technical Report." SERC-2010-TR-005, Systems Engineering Research Center, August 22, 2010.
11. Bayuk, Jennifer L. Enterprise Security for the Executive: Setting the Tone from the Top. Santa Barbara, California: Praeger, 2010.
12. Amoroo, Edward G. Cyber Attacks: Protecting National Infrastructure. New York: Elsevier, 2011.