Backgrounder

Published by The Heritage Foundation

No. 2261
April 16, 2009

Complex Systems Analysis—A Necessary Tool for Homeland Security

James Jay Carafano, Ph.D., and Richard Weitz, Ph.D.

As President Barack Obama rightly noted in one of his first directives, his "highest priority is to keep the American people safe."[1] Addressing homeland security challenges effectively requires understanding them. Many of the threats the United States faces, and many of the means available to counter them, are embedded in webs of complex systems that surround everyday life—from the transportation networks that move goods and people to the electrical grids that power the nation.

Understanding how complex systems perform is a vital component of homeland security. The responsibilities of the Department of Homeland Security (DHS) include making the complex systems that support the country more resilient in the face of natural or man-made disasters; preventing terrorist exploitation of the systems that support society; and advancing security measures in a manner that encourages healthy and stable global systems—which promote economic growth and protect individual liberties. In order to address the myriad challenges in managing complex systems, DHS requires centers of excellence proficient in complex systems analysis, as well as a more direct method of translating analysis into effective recommendations and policies.

Understanding Complex Systems

A system is "any set of regularly interacting factors and activities that has definable boundaries and that produces measurable outputs."[2] The complexity of a system is determined by the number and diversity of

Talking Points

- Many of the threats the United States faces, and many of the means available to counter them, are embedded in webs of complex systems that surround everyday life—from the transportation networks that move goods and people to the electrical grids that power the nation.
- The responsibilities of the Department of Homeland Security include making the complex systems that support the country more resilient to natural or man-made disasters and preventing terrorist exploitation of these systems.
- Complex systems are extremely difficult to analyze, so understanding how they function, predicting their behavior, or determining the optimum means for changing their performance represents a unique challenge.
- Countering threats to complex systems requires a comprehensive, multidisciplinary, and multi-layered approach. The Department of Homeland Security must become a national leader in developing and exploiting means of complex systems analysis and using that analysis to inform its policies and programs.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/bg2261.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

interacting components. When systems become overly complex, their behavior cannot be easily predicted by traditional methods of analysis: breaking a system into its component parts and analyzing elements in detail.[3]

In a complex system, elements are so interconnected and their relationship so multifaceted that their properties cannot be properly understood without assessing their interrelationship with each other as well as their relationship with the wider system and its environment.[4] Financial systems offer a case in point. It is often difficult, for instance, to appreciate the value of an individual stock just by knowing its current price. On the other hand, when the price of the stock is understood in relation to the performance of the larger system (for example, the market—whether the average price of stocks on the exchange are on a positive trend, a bull market, or on a negative trend, a bear market), the value of the stock takes on a more significant meaning. In short, in a complex systems analysis, assessing individual properties often requires mapping them according to their place in the overall system.

Additionally, a complex system can exhibit properties that cannot be understood by examining the system's individual components. Complex systems exhibit patterns, outcomes, and properties not present in any of their individual elements. Analysts often describe the performance of large complex systems as "nonlinear," meaning that how the system functions cannot necessarily be derived just from understanding the sum of the behavior of the many parts that compose the system.[5] Financial markets again offer an example. Analysts can study all kinds of information on the components of a market, from the monetary exchange rates to interest charges, yet cannot accurately predict whether future markets will be bullish or bearish.

Since complex systems are so much more difficult to analyze, understanding how they work, predicting their behavior, or determining the optimum means for changing their performance presents a unique challenge. When the performance of systems affects the security of the nation, the task can be particularly daunting.

Complex Systems and National Security

Most national security problems faced by policymakers today involve attempting to understand, predict, or affect the behavior of complex systems from border and immigration security to financial markets to transnational terrorist organizations. Yet, policymakers rarely fully comprehend the impact of their decisions on the behavior of these systems. Rather than dealing with systems as a whole, contemporary decision makers tend to concentrate their choices on discrete activities that are easier to identify and understand. There is a problem with that approach: The more complex and disorganized the system, the more unpredictable effects the discrete, uninformed, intuitive decisions of policymakers may have on specific outcomes.

Failing to understand how discrete decisions have an impact on the system as a whole can produce unintended and counterproductive consequences. In the aftermath of Hurricane Katrina, for example, emergency officials barred all but authorized emergency responders from entering New Orleans. As a result, fuel handlers who had not been credentialed by state officials could not make necessary deliveries to generator-powered emergency centers. Without gas or fresh batteries, the centers lost

1. The White House, Presidential Study Directive 1, February 23, 2009, p. 1, at *http://www.hsdl.org/hslog/?q=node/4718* (April 10, 2009).
2. Richard L. Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington, D.C.: National Defense University Press, 2006), p. 218.
3. L. A. N. Amaral and J. M. Ottino, "Complex Networks: Augmenting the Framework for the Study of Complex Systems," *The European Physical Journal B*, May 14, 2004, at *http://amaral.northwestern.edu/Publications/Papers/Amaral-2004-Eur.Phys.J.B-38-147.pdf* (April 13, 2009).
4. Yaneer Bar-Yam, "Multiscale Representation Phase I," New England Complex Systems Institute, August 1, 2001, at *http://www.necsi.edu/projects/yaneer/SSG_NECSI_1_CROP.pdf* (April 13, 2009).
5. "The Study of Complex Systems," Center for the Study of Complex Systems, The University of Michigan, at *http://www.cscs.umich.edu/old/complexity.html* (April 11, 2009).

power and became inoperable. Since officials failed to understand how the entire system worked, they fixed one problem, preventing unnecessary convergence at the disaster scene, and created another—disabling key command and control nodes.

System analysis for homeland security involves not only protecting and using the systems that support American society, but also gaining knowledge on how to attack the complex systems of America's adversaries. Some terrorist groups, for instance, have demonstrated tremendous capacity for adaptation. According to a report by the Homeland Security Advisory Council, a terrorist group can be "proactive, innovative, well-networked, flexible, patient, young, [and] technologically savvy, and learns and adapts continuously based upon both successful and failed operations around the globe."[6] Some terrorist groups may not only be best understood as complex systems; battling them may also require understanding how these groups exploit other complex systems such as the Internet.[7] Therefore, it is clear that the ability to effectively analyze complex systems has utility both for safeguarding against threats as well as mitigating or defeating potential or existing dangers.

Mastering Complex Systems

Describing complex systems—how they work, what they produce—and then applying various planning methods and choice models to determine how the systems' performance can be changed is the task of complex systems analysis. Until recently, researchers have approached complex systems by means of traditional analysis—breaking them down into their smaller constituent parts and analyzing these in detail. Cell biologists studied organisms in terms of how their component cell systems interact. Similarly, engineers tried to understand how a vehicle operates by taking apart all its individual components, analyzing their properties, and reassembling the vehicle in a slightly altered way to observe the effects on its performance.

The problems inherent in trying to analyze complex systems that have many units and variables were initially ascribed to a lack of information required to model or analyze the system. The working assumption was that, as data collection and processing techniques continued to improve, researchers would be able to develop superior models for predicting their properties. But contemporary research has demonstrated that these methods remain deficient because they still offer oversimplified descriptions of system behavior. Simply adding more data to the study of a complex system may not be enough. In contrast, complex systems analysis tries to bridge the gap between knowledge and understanding—of analysis and synthesis—by exposing and studying interrelationships rather than simply relying on linear chains of cause and effect.[8]

Complex systems have been studied in the natural world for the past two decades. Ecologists have applied this type of analysis to the life sciences using mathematical models to help understand what drives large fluctuations in wildlife populations, and have used computer models to establish the properties of small-scale systems to identify emergent properties of molecules within cells.[9] Often the complexity of the system of interest requires employing a multidisciplinary approach that combines insights from several scientific fields.

During the past decade, exploiting advances in mathematics and computer simulations, analysts have employed complex systems analysis extensively to human behavior in physical, economic, and social systems.[10]

6. Homeland Security Advisory Council, "Report of the Future of Terrorism Task Force," U.S. Department of Homeland Security, January 2007, at *http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf* (April 13, 2009).
7. James Jay Carafano and Richard Weitz, "Combating Enemies Online: State-Sponsored and Terrorist Use of the Internet," Heritage Foundation *Backgrounder* No.2105, February 8, 2008, at *http://www.heritage.org/Research/NationalSecurity/bg2105.cfm*.
8. Richard Gallagher and Tim Appenzeller, "Beyond Reductionism," *Science*, Vol. 284, No. 5411 (April 2, 1999), p. 79, at *http://www.sciencemag.org/cgi/content/short/284/5411/79* (April 13, 2009).
9. *Ibid.*
10. David R. Garvey, "Applications of Distributed, Networked Architectures to Port Security," Alidade Incorporated, at *http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/168.pdf* (April 13, 2009).

In order to gain an appreciation of the dynamics of a complex system, analysts often use a model composed of "stock" and "flow" diagrams. A "stock" represents an entity (for example, money) accumulated over time. Stocks change through "flows." A flow is a change in stock over time (for example, deposits and withdrawals from a bank account). The relationships between stocks and flows in a complex system are often depicted graphically through a network of "nodes" and "links" that portray how entities in the system are connected.[11]

Homeland Security and Systems Analysis

Used properly, complex systems analysis can help counter this limitation by alerting policymakers to unexpected outcomes of interactions between discrete parts of a system, thereby allowing them to anticipate and hedge against potential future national security threats. In addition, complex systems analysis should help counter the natural tendency of policymakers to dwell on their daily inbox rather than consider deeper, more comprehensive issues.

Among the many tasks suited to complex systems analysis could be helping the Department of Homeland Security identify and protect the nation's critical infrastructure and key resources (CIKR). America's critical infrastructures include those national economic sectors that involve transportation, oil and gas, water, electricity, emergency services, government, telecommunications, and banking. Each of these infrastructures is related to all others, and each plays a role in the success and the security of the United States. Homeland Security Presidential Directive 7 (HSPD-7), issued in December 2003, assigns the Secretary of Homeland Security responsibility for coordinating national efforts to strengthen the protection of the U.S. CIKR.[12]

DHS attempts to address these threats and vulnerabilities by establishing priorities, goals, and requirements for CIKR protection and then working with diverse public- and private-sector partners to implement them. Through the federal grants, the National Infrastructure Protection Plan, and other measures, DHS supports such activities as hardening facilities against attack, enhancing resiliency, developing active and passive countermeasures, and bolstering cyber security. Strengthening CIKR protection helps to deter attacks against these assets and minimizes the adverse effects of any disruption in their operation.

Complex systems analysis can help predict what might happen if an attack or natural disaster disrupted a critical infrastructure, especially its possible effects on other CIKR sectors that are part of the same system. Through modeling, scenarios, and other analytic tools employing complex systems analysis, DHS policymakers can consider optimal protection, response, and consequence-management strategies.

Some efforts have been made to apply complex systems to homeland security issues. The Pacific Northwest Partnership for Regional Infrastructure Security has held a series of exercises called "Blue Cascades" that examines all the interdependencies of a regional-wide failure of the electrical grid.

Indeed, the analysis of electric-power grids provides insightful illustrations of how such processes might manifest themselves. Each power line and each generator has a region in which it can generally operate safely. For reasons of economics, operators tend to run them close to their maximum safety margin rather than leave more capacity unused. If the power load exceeds the margin, the line can collapse. The power flow then redistributes itself throughout the network, sometimes along preplanned routes, sometimes more randomly. If this surge disables other lines, cascading failures can occur, leading to large power outages.[13]

In the northeastern blackout of August 14, 2003, a minor incident—the loss of a few power lines in

11. *Ibid.*
12. Office of the White House Press Secretary, "Homeland Security Presidential Directive/Hspd-7," December 17, 2003, Section 12, at *http://www.globalsecurity.org/security/library/policy/national/hspd-7.htm* (April 13, 2009).
13. Sara Robinson, "The Power Grid as Complex System," Society for Industrial and Applied Mathematics, December 1, 2003, at *http://www.siam.org/news/news.php?id=377* (April 13, 2009).

Ohio that came into contact with some trees—quickly cascaded into a massive power outage due to these compounding effects, as the loss of these power lines led to heavy loading on parallel lines, which soon collapsed and dragged down other connected lines with them. In turn, the failure of the power grid resulted in disruptions in interconnected transportation, communications, and other related networks since railways, airlines, gas stations, and oil refineries also suspended operations. Phone lines were overwhelmed due to the high volume of calls, while many radio and television stations went off the air. In the end, the cascading crisis disrupted commercial and daily activities in a large part of eastern Canada and the northeastern United States. The aggregate losses from the outage are difficult to calculate, but probably approached ten billion dollars despite its lasting only a single day.[14]

Complex systems analysis warns that misguided efforts to mitigate certain risks associated with small power failures can increase the risk of large cascading failures. The risks of blackout are interdependent. Cascading failures begin when one component fails and then power is redistributed within the system to other components, forcing them operate at higher loads. Once this load reaches a certain point (criticality), that component is more prone to failure. If it fails, the load will again be redistributed to a smaller number of adjacent components, which must then accept an even higher load, increasing the likelihood they will fail as well as the likelihood of cascading failure in which the entire power system collapses. In this light, if done incorrectly, suppressing small blackouts can put the larger system at risk of failure.[15]

Disaster Loops

In matters of homeland security, understanding complex systems is particularly critical since many of the complex systems are dependent on one another. Disrupting one could have a cascading effect on others. Cyber disruption and power failures could interact in a malicious feedback loop because physical and cyber infrastructure has become an integrated complex system vulnerable to single points of failure. A computer attack could disrupt the electric power grid, which in turn would cause many computers to shut down as soon as they exhausted any emergency backup power. Similarly, a malicious programming command that exploited a dam's control system in order to disable its operation could prevent it from generating electricity and providing water for irrigation or prevent the flooding of vulnerable communities and transportation nodes. The combined reduction in power supplies and computer power would weaken the ability of first responders to cope with the emergency. The power reduction would also severely disrupt the functioning of other critical interrelated infrastructure systems, such as the communications and transportation sectors.

Failures in complex systems have been likened to forest fires. In a forest, the more sparsely populated it is, the less likely it is that a small fire, localized in a cluster of isolated trees, would spread to the rest of the forest. But if the forest is filled with several connected clusters of trees, a small fire at one end of the forest is more likely to eventually consume the rest of the forest. What begins as a relatively insignificant failure can, quickly and without warning, cascade into a widespread disaster that affects several types of infrastructures and multiple jurisdictional boundaries.

Putting Complex Systems Analysis to Work

Countering threats to complex systems requires a comprehensive, multidisciplinary, and multi-layered approach. In order to do its job right, the Department of Homeland Security must become a national leader in developing and exploiting means of complex systems analysis and using that analysis to inform its policies and programs. Developing that capability must begin with deepening the knowledge and expertise within the national homeland security enterprise:

14. The Electricity Consumers Resource Council, "The Economic Impacts of the August 2003 Blackout," February 9, 2004, pp. 1–3, at *http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf* (April 13, 2009).
15. Ian Dobson, Benjamin A. Carreras, Vickie E. Lynch, and David E. Newman, "Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-Organization," Bulk Power System Dynamics and Control, Vol. VI (August 22–27, 2004), at *http://www.ornl.gov/sci/fed/Theory/publication/pub2004/dobsonIREP04.pdf* (April 13, 2009).

- **The Department of Homeland Security should develop Complex Systems Analysis Centers of Excellence.** The Department directs three Federally Funded Research and Development Centers (FFRDCs)—the Homeland Security Institute (HSI), the Homeland Security Systems Engineering and Development Institute (SEDI), and the National Biodefense Analysis and Countermeasures Center (NBACC). HSI focuses on policy development, decision making, analysis of alternative approaches, and evaluation of new ideas. SEDI provides systems-engineering expertise and acquisition strategy advice, while NBACC focuses on developing means to combat bioterrorism. Each center should be required to develop expertise in complex systems analysis and together form a consortium to serve as DHS's center of excellence on complex systems analysis.
- **DHS should collaborate with Homeland Security Centers of Excellence.** Universities chosen by the DHS's Directorate for Science and Technology through a competitive selection process participate in the Homeland Security Centers of Excellence program. The university centers bring together leading experts and researchers to conduct multidisciplinary research and education on a range of homeland security challenges from natural disasters to border security. The Science and Technology Directorate should ensure that the research agendas of these institutions advance DHS's understanding and application of complex systems analysis.
- **DHS should address complex systems analysis during the Quadrennial Homeland Security Review (QHSR).** Congress mandated the QHSR to address future challenges to the Department of Homeland Security.[16] The QHSR should establish the requirement for developing a homeland security master plan for institutionalizing multidisciplinary analysis, including expertise in complex systems analysis in the national homeland security enterprise.
- **DHS should integrate complex systems analysis into a net assessment office.** Net assessment, a widely used tool within the intelligence community, complements and contributes to complex systems analysis. Net assessment is based on the understanding that all national security challenges are a series of actions and counteractions between competitors.[17] The purpose of examining these actions and counteractions is to assess how these competitions could develop in the future. The Department of Homeland Security has considered establishing an Office of Net Assessment within its policy and planning directorate. This office should include developing expertise in employing complex systems analysis to develop policy recommendations.
- **DHS should add complex systems analysis to the Homeland Security Professional Development Program.**[18] Homeland security needs the foundation of a professional development system that will provide the cadre of leaders required to meet the demands of the 21st century. This foundation must include education, training assignments, and accreditation tools that can help develop professionals for homeland security and other critical interagency national security activities. Developing expertise in critical systems and multidisciplinary analysis should be a core component of any professional development curriculum. The government should have a "brick and mortar" homeland security university dedicated to teaching these and other essential national security management, leadership, and decision-making skills.

16. Jena Baker McNeill, "The Quadrennial Homeland Security Review: A Vital Tool for the Obama Administration," Heritage Foundation *Backgrounder* No. 2215, December 12, 2008, at *http://www.heritage.org/Research/HomelandSecurity/bg2215.cfm*.
17. James Jay Carafano, Frank J. Cilluffo, Richard Weitz, and Jan Lane, "Stopping Surprise Attacks: Thinking Smarter About Homeland Security," Heritage Foundation *Backgrounder* No. 2026, April 23, 2007, at *http://www.heritage.org/Research/HomelandDefense/bg2026.cfm* (April 13, 2009).
18. James Jay Carafano, "Missing Pieces in Homeland Security: Interagency Education, Assignments, and Professional Accreditation," Heritage Foundation *Executive Memorandum* No.1013, October 16, 2006, at *http://www.heritage.org/Research/HomelandSecurity/em1013.cfm.*

Conclusion

The Department of Homeland Security requires a robust capacity to conduct complex systems analysis and apply this knowledge to the policies and programs that will keep the nation safe in the 21st century. Taking the right steps now will make the department and the national security enterprise over which it has stewardship the right tools to face current and future threats.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. Richard Weitz, Ph.D., is Senior Fellow and Director of the Center for Political-Military Analysis at the Hudson Institute.