# Chapter 29
# Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP)

**John S. Hurley**

*College of Information and Cyberspace (CIC), JPME and Cyber-L Department, National Defense University, iCollege, Washington, DC, USA & Information, Communications, Technology and Acquisition Department, National Defense University, Washington, DC, USA*

## ABSTRACT

*In this paper, we examine the benefits of a more quantifiable way to make decisions that enable senior leaders to better manage disruption of and attacks on the critical infrastructure. Most of the decisions have been made using intuition and in some cases unrelated experiences and have not particularly worked to the benefit of the sectors' performance and stability. Much of this is due to the history of the logic control systems and networks that were fairly isolated and much better protected. Attempts to reduce costs and secure many of the benefits of IP-based environments have unfortunately now also introduced some of the vulnerabilities indicative of IP-based systems into the logic environments. Senior leaders have not been used to these new 'hybrid' information technology/operational technology (IT/OT) environments which though creating new opportunities also introduce new challenges. The unique nature of the critical infrastructure in which it is over 80%-owned by the private sector, often regulated by the federal government, and serves the interests and demands of the public, creates a non-trivial challenge at many different levels. More trust and cooperation between the three elements of society is surely a desired interest by the key stakeholders, but there are many concerns in terms of over-regulation, costs, and loss of intellectual property that have consistently sustained a level of discomfort between the three communities in terms of the priorities and self-serving interests of each other. The challenges of the low asymmetry entry and attribution within the cyber domain have raised the profile of many actors who would not even have previously registered in the 'noise' on a trouble or problem scale. Now, the ability to determine those responsible, as well as, almost any actor having the ability to present a challenge to the environment have changed many of the dynamics in terms of how senior leaders must now oper-*

DOI: 10.4018/978-1-7998-2466-4.ch029

*ate and manage the appropriate systems and networks. Hence, for obvious reasons, senior leaders are much more cautious in their approach to decision making because of the potential consequences. This is especially true because cyber assets, though so valuable can be also so vulnerable. In this study, we will discuss a method that moves decision from a less arbitrary to a more data-centric, quantifiable approach that drives leadership to better and quicker decisions.*

## INTRODUCTION

General Martin Dempsey, 18th Chairman of the Joint Chiefs of Staff, noted that the global security environment was the most unpredictable he had seen in his 40 years of service. In the 2015 National Military Strategy, it spoke of a significant increase in global disorder—a world now filled with multiple security challenges from traditional state actors and transregional networks of sub-state groups (National Military Strategy, 2015). Advancements in computing over the past five or six decades have transformed our society from one in which we have seen lives changed through access, innovation, and convenience. We see end-to-end connectivity around the globe; devices that look increasingly less like traditional computing devices, e.g., laptops, desktops, and even personal digital assistants (PDAs); and a world that has become strikingly more intertwined and interdependent.

Much of General Dempsey's view is shared by many, including some organizations, such as the Organization of American States (OAS). Adam Blackwell, Secretary for Multidimensional Security, OAS, noted that 'the Internet has reduced through connectivity the size and separation of the world'. The incorporation of information and computing technologies into devices that no longer resemble traditional computing devices such as laptops, desktops, and personal digital assistants (PDAs) reflecting the Internet of Everything has dramatically altered today's landscape, including:

- Changed significantly how information is shared
- Revolutionized business processes
- Changed the way countries and critical infrastructure are operated (Report on Cybersecurity and Critical Infrastructure in the Americas, 2015)

The pervasiveness of computing within our lives has changed the services and capabilities we expect to be available to us. The role of the critical infrastructure in meeting many of the service needs that we demand has not fully been appreciated in terms of its relevance to the quality of life that we have learned to embrace and demand. The critical infrastructure provides 'critical' services and products that drive and support society, serving as the backbone of a nation's economy, security, and health. In the United States, the critical infrastructure sectors (all 16 of them) consist of the assets, systems, and networks (physical or virtual) considered vital to the nation's interests and survival (Homeland Security, 2015).

Senior leaders are very reluctant to make multi-million-dollar decisions on the investments within cyberspace largely because of the enormous risk and potential uncertainty of the outcomes of their decisions. This is understandable given that investments that do not pan out and the information assets for which they are intended can be serious impediments to career growth and longevity. Often, the decisions are being driven by 'gut' reactions void of valuable data that could be an essential asset in better determining outcomes. To be very clear, there certainly are no guarantees that decisions will be perfect on any account nor outcomes that can be expected with 100% certainty. However, we look forward to