# Chapter 12
# Cyber-Search and Cyber-Seizure:
## Policy Considerations of Cyber Operations and Fourth Amendment Implications

**Catherine B. Lotrionte**
*Georgetown University, USA*

## ABSTRACT

*This chapter discusses the nature of cyber threats against government and private computer systems, describing some steps the government has taken and the challenges involved in protecting those systems. The chapter argues that a national security approach for cyber security policy is the most promising option for preventing these cyber threats while operating within the domestic legal framework. After a review of the President's constitutional authorities to protect the nation from traditional threats, the chapter concludes that the President has some power to monitor Internet communications in transit within the United States when the communications threaten the welfare of the nation. The chapter recommends that this authority be augmented by Congressional action through legislation. The President's powers in cyber security, even given Congressional support, however, are still restrained by the protections the Fourth Amendment provides for traditional forms of communication and individual privacy. Although there is limited Fourth Amendment precedent in the area of cyber security, the well-established exceptions to the Fourth Amendment requirements, based on consent, special governmental needs and the reasonableness of the search or seizure, provide a legal basis for executive branch action to protect critical infrastructures and their computer systems. As the Courts have long held, these exceptions allow the government to conduct searches or seizures without being bound by all of the requirements of the Fourth Amendment. If the government develops its cyber security policy in line with these exceptions, this chapter argues the government can both protect critical computer systems and operate within Fourth Amendment doctrine that recognizes the legitimacy of privacy in electronic communications.*

DOI: 10.4018/978-1-61520-831-9.ch012

## INTRODUCTION

On Saturday, November 21, 2009 at approximately 4:00 pm, a radiation leak at the Three Mile Island nuclear power plant near Middletown, Pennsylvania resulted in the evacuation of over 100 employees. According to press reports, the leak occurred after a change in air pressure inside a building caused the release of irradiated particles within the piping of one of the generators (CNN, 2009). The air pressure change happened after the ventilation fans inside the building started. The immediate cause of the leak is still unknown. The spokesperson for Exelon, the private company that operates the plant, announced that the public was never at risk of exposure to radiation from the leak. In 1979, the same plant had a major accident. After that leak there was a halt in the building of any new nuclear plants in the United States. Currently, there are more than 100 nuclear power reactors in over 30 states within the United States. There are 30 different private companies that operate these plants and are responsible for their security.

The recent leak at Three Mile Island was real and potentially catastrophic. Imagine that the change in air pressure that occurred at the plant building was caused by a malfunction of the computer systems at the plant that controlled air pressure throughout the plant. Then imagine that the malfunction was the result of a malicious code sent via email to an employee at the plant. When the employee opened his email, the malware caused a chain of events that led to the failure of the systems that control the air pressure systems throughout the plant. Imagine that malware went undetected for weeks until it was triggered to cause the failure of the air pressure systems. Next imagine that the National Security Agency is monitoring incoming Internet traffic to the nuclear power plant at Three Mile Island. The NSA now believes that the individual (s) responsible for the recent attack on the plant's computer systems have sent another computer virus that will cause the plant safety mechanisms to fail. The NSA estimates that when the email reaches its targeted destination it will trigger a cascading series of events that will lead to a complete system failure of the plant's security controls, causing a meltdown of the reactors.

The exact extent of the possible damage will be unknown to those at the NSA analyzing the malicious code. In this case, though, they believe the second attack will be more dangerous because the perpetrators have learned about the plant's system vulnerabilities from their first attack. The NSA will continue to monitor incoming Internet traffic to the plant (blocking any emails that they detect to have malicious code in order to disrupt a much more catastrophic second attack). The NSA's computers open the emails in order to scan the contents to determine the presence of the malicious code. The NSA analysts will review some personally identifiable information (PII) in the emails, such as email addresses. The analysts, however, will not have access to any of the content of the emails. NSA computers will automatically scan the content of the emails in order to identify the presence of malicious code. If the malware is detected, the email will be blocked, preventing the malware from reaching the plant's computer systems, infecting the network and causing a catastrophic second attack. While the NSA will keep a copy of the email, no individual at NSA will review the content. In monitoring, scanning and blocking email communications in transit to the plant, has the NSA triggered the protection of the Fourth Amendment? Has the government conducted a search or seizure? And what, if any, Fourth Amendment requirements are relevant?

The answers to these questions depend on many factors, including whether automated monitoring of Internet traffic and email communications to the power plant constitutes a Fourth Amendment "search" (U.S. Constitution, 1791). If monitoring email content amounts to a search, then the government cannot monitor the email without a warrant or special circumstances. On the other