

A widespread cyberattack was launched on July 4, 2009 and disabled the websites of several US government agencies, including the Department of Transportation (DOT). The sophistication, speed, and anonymity of the attacks prompted the Department of Homeland Security and the DOT of Inspector to investigate the application security and intrusion protection measures, which revealed numerous vulnerabilities. Because our national security is heavily dependent upon information technology and the information infrastructure, the increasing quantity and complexity of such attacks is raising serious concerns about the safety of some of our nation's most sensitive data and critical infrastructure. As the July 4 attack (subsequently labeled as the “Independence Day”) attack revealed, cybersecurity represents a serious challenge to our nation’s sensitive military and federal cyberinfrastructure. As the White House Spokesman Nick Shapiro stated on July 9: “We see attacks on federal networks every day.”¹

According to experts, 166,908 PCs from 74 countries were used in attacks on federal websites on July 4, 2009.² Commands were routed through eight control servers, tied into a master server location in United Kingdom that was controlled from Russia and China. The organization and sophistication of the attack offers a glimpse into the growing maturity of the attackers as well as their techniques and objectives. It is evident that this attack was not launched by an individual hacker, but instead from a highly-organized team of professionals located in different countries. Contrary to another expert, quoted in Washington Times to say that the Independence Day attack “was so primitive it could be compared to a modern air force

¹ “U.S. government sites among those hit by cyberattack”, *CNN*, July 8, 2009. Available at: <http://edition.cnn.com/2009/TECH/07/08/government.hacking/index.html>

² “UK, not North Korea, source of DDOS attacks, researcher says”, *PC World*, July 14, 2009. Available at: http://www.pcworld.idg.com.au/article/311070/uk_north_korea_source_ddos_attacks_researcher_says

using hot-air balloons instead of planes to attack a foe”,³ the objectives of the attacks were not necessarily to cause a “Denial of Service”, an incident in which a user or organization is deprived of the services of a resource they would normally expect to have, but could have been used to gather classified data pertaining to electric grid systems, water/sewerage infrastructure, and vital transportation networks. This infrastructure is so vital to the United States national security that their incapacitation or destruction would have a debilitating effect on our national security.

According to a recent research study by Secure Computing Research, which surveyed 199 international security experts, “more than half of these experts believed that most critical infrastructure continues to be vulnerable to cyberattack. Further, a majority of respondents said that major attacks have already begun or are likely to occur in the next 12 months.”⁴ Although the US Government has already taken many measures to address the risk of cybersecurity, it remains an extraordinary difficult task that requires a coordinated effort from the entire federal government, state and local governments, the private sector, and ultimately, individuals themselves. As the May 2009 White House Cyberspace policy review concluded, “The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.”⁵

³ “July 4th Attack Called Very Minor”, *The Washington Times*, July 16, 2009. Available at: <http://www.washingtontimes.com/news/2009/jul/16/july-4-cyberattack-called-very-minor/>

⁴ “Critical infrastructure is not prepared for cyber attacks”, November 18, 2008 <http://www.net-security.org/secworld.php?id=6727>

⁵ “Cyberspace Policy Review”, White House, May 29, 2009. Available at: <http://www.whitehouse.gov/asset.aspx?AssetId=1906>

The White House review offered numerous steps and potential solutions to addressing the crisis, and we should strive to implement each one of these complex steps and recommendations. In my view, however, we should begin with simple, logical steps, by pursuing three objectives in order that can strengthen our nation's cybersecurity at all levels:

1) **Identifying and assessing** security risks for the entire network, software application, and other critical systems. The results of a thorough risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

2) **Selecting controls:** once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. The selection of these security controls would be dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, as well as federal and state regulations.

3) **Mandating a Cyber Security Response Plan** for each entity, including a comprehensive framework for the management of cybersecurity incidents. The plan should provide structure and mechanisms, plan of action, as well as assigning defined roles and responsibilities of response team members.

Moreover, private companies have long played a leading role in effectively preventing cybercrimes. Therefore, it is absolutely essential that the US government develop a partnership with the private sector -- not only facilitate the exchange about best practices and intelligence, but also to develop additional strategies to confront such attacks, to increase awareness, to launch training, and to design appropriate recovery operations. As the July 4 attacks demonstrated, we must no longer remain vulnerable in the face of this menacing threat to our national security.

I hereby give my authorization, permission and consent to the Lint Center, for National Security Studies, Inc. to use, disclose, release and/or publish my name, photo and any or all other information which I have provided. Additionally, I give specific release of my Essay for publishing on the website of the Lint Center, for National Security Studies, Inc.



A handwritten signature in black ink, appearing to read "J. Almont", is written over a horizontal dashed line.