Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Subcommittee Cybersecurity, Infrastructure Protection, and Security Technologies

Joint Hearing: "Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management."

10:00 a.m. - 311 Cannon House Office Building

We all know that cyber security is a matter of national, economic, and societal importance. Present-day attacks on the nation's computer systems do not simply damage an isolated machine or disrupt a single enterprise system, but current attacks target infrastructure that is integral to the economy, national defense, and daily life.

Computer networks have joined food, water, transportation, and energy as critical resources for the functioning of the national economy. When one of these key cyber infrastructure systems is attacked, the same consequences exist for a natural disaster or terrorist attack.

National or local resources must be deployed. Decisions are made to determine where to deploy resources. The question is who makes these decisions? The data required to make and monitor the decisions, and the location of available knowledge to drive them may sometimes be unknown, unavailable, or both.

Indeed, computer networks are the "central nervous system" of our national infrastructure, and the backbone of emergency management is a robust cyber infrastructure. These systems enable emergency management agencies to implement comprehensive approaches to natural disasters, terrorist attacks, and law enforcement issues.

Mr. Payne has introduced a bill, the ***Smart Grid Study Act*** that will give a fuller picture of the smart grid's role and our reliance on it, especially during an event where emergency management response is the key to our resilience. I'm glad to see the strong support that the National Electrical Manufacturers have given this bill, and I especially look forward to their testimony today.

There is a general lack of understanding about how to describe and assess the complex and dynamic nature of emergency management tasks in relation to cyber security concerns. And there are many issues involving knowledge integration and how it helps managers improve emergency management task performance. Ever since the first computer virus hit the Internet, it has been apparent that attacks can spread rapidly.

Just as society has benefited from the nearly infinite connections of devices and people through the U.S. cyber infrastructure, so have malicious parties with the intent of taking advantage of this connectivity to launch destructive attacks.

We must find a way to develop tools that we can use to improve Emergency Management successes through effectively handling cyber complexity, cyber knowledge, and cyber integration at the ground level for our first responders.