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

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Field hearing on "Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime."

10:00 a.m., Paul Peck Alumni Center, Drexel University
3142 Market Street, Philadelphia, Pennsylvania

Today's hearing will focus on Cyber Crime and our Nation's response to it. Modern criminals increasingly rely on the Internet and advanced technologies to spread their criminal operations. I think everyone would agree that Internet technology has now emerged as a key factor for the vast majority of organized crime activity.

For instance, criminals can leverage the properties of the Internet to carry out traditional street crimes such as distributing illicit drugs and sex trafficking.

But what we are hear to talk about today, is how criminals exploit the digital world to assist crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft.

As we will hear today, the FBI considers high-tech crimes to be the most significant crimes confronting the United States as a Nation, and we, on this Subcommittee, have shown an increasing interest in guaranteeing the federal government has the tools and capabilities to combat modern day crime—particularly those with cyber components—while safeguarding privacy rights.

Today's cyber criminals make their crimes more profitable by choosing specialties, and creating cyber networks of colleagues. These types of criminals can victimize individuals and organizations alike.

They are generally motivated by self interest and profit, but cybercrimes can have public health and national security consequences, especially when cyber crimes are directed towards critical infrastructure, such as our hospitals, water systems, government entities, or our nation's financial systems.

U.S. officials face the challenging task of identifying the perpetrators of malicious cyber incidents in which victim and criminal can be far removed from one another.

The person or persons behind an incident can range from lone actors to expansive criminal networks or even nation states. This challenge of attribution is further compounded by the anonymity afforded by the digital realm.

It can sometimes be difficult to determine the actor's motivation—is the criminal driven by greed or glory in the form of recognition among fellow criminals in the cyber world? Or does the criminal have broader ideological motives?

Finding the answers to these questions is key to distinguishing between cybercrimes and other cyber

threats such as cyber attacks, cyber espionage, and cyber warfare.

Relevant distinctions exist between these various malicious activities in the cyber domain, just as lines have been drawn between the their real world counterparts, and today's hearing will help us understand those distinctions.

In July 2011, the Obama Administration released the *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*. This strategy provides the federal government's first broad conceptualization of "trans-national organized crime," highlighting it as a national security concern.

It highlights 10 primary threat categories posed by trans-national organized cyber crime:

- penetration of state institutions,
- corruption, and threats to governance;
- threats to the economy,
- threats to U.S. competitiveness, and strategic markets;
- the nexus between criminals, terrorists, and insurgents;
- expansion of drug trafficking;
- human smuggling; trafficking in persons;
- weapons trafficking;
- intellectual property theft; and finally,
- cybercrime.

The President's strategy outlines key actions to counter the range of threats posed; by building international capacity, cooperation, and partnerships, and taking shared responsibility to identify what actions federal, state, and local entities can take to protect against the threat and impact of trans-national cyber crime.

We are here today to discuss complex prosecutorial and investigative problems that face law enforcement officials and companies when dealing with cybercrime, and I look forward to their testimony.