Opening Statement for Cyber Hearing
Congressman C.A. Dutch Ruppersberger
Tuesday, October 4, 2011

Good Morning.

Thank you for being here today.

I would like to welcome our three witnesses…. Retired General Michael Hayden, Art Coviello of RSA and Kevin Mandia of Mandiant. Thank you all for being here today.

I am pleased we are having an open hearing on cyber security.

I believe cyber security is an issue our country and the average person are not paying enough attention to.

The internet has made amazing strides over the last ten years.

Think of all of the things you can do now, but couldn't do then.

You can pay your phone bill or order a pizza from your I-phone.

If you get in a car accident and call 9-11 but don't know exactly where you are, emergency crews can locate you through the signal from your cell phone.

Our nation's networks power our computers, our cell phones, our Blackberries, and our I-pods.

They power the electrical grid that allows us to turn the lights on, the classified military and intelligence networks that protect the war-fighter on the battlefield and keep us safe here at home.

But the more we rely on our nation's networks to go about our everyday lives, the more vulnerable we become to an attack stopping us in our tracks.

Important websites, everything from the Department of Defense to Google to the Nasdaq, are being attacked every day… and it is only getting worse.

The Department of Defense logged 260 million hacking attempts in one year alone.

We've had critical defense files stolen in the past, including details about U.S. fighter jets, missile systems and unmanned drones.

In South Korea, close to 30 million people were unable to use their bank's ATMs or make online transactions because their bank was cyber attacked.

And what's worse, important financial data was lost – forever.

I fear this could happen here.

The threats are real. Our enemies are elusive and the stakes are high.

I believe we need a comprehensive cyber strategy to protect our country… and we need it now.

Military, government and business must work together to beef up our nation's cyber defenses.

The National Security Agency does a phenomenal job protecting the dot-mil domains.

The newly created "Cyber Command" leverages the massive brainpower of the NSA to ward off potential attacks.

The Department of Homeland Security is having a harder time defending the dot-govs and helping the private sector protect the dot-coms.

There isn't a "gold standard of protection"… that all government agencies and businesses must achieve to properly defend their networks from attacks.

And there aren't incentives such as tax credits for voluntary implementation of security tools.

We must harness NSA's expertise and share the critical information it collects about potential threats with all of our nation's networks.

We must have an active defense - where we are staying one step ahead of cyber attackers by being on the lookout for "malicious" code lurking in the shadows… ready to wreak havoc on our nation's networks.

This information must be shared in a way that ensures it does not quickly land in the hands of our adversaries and criminals… the people who hacked us in the first place.

DHS must act as a bridge between NSA and the private sector.

The Department of Homeland Security recently started a pilot program for sharing classified data about cyber attacks involving about 20 volunteer companies.

Already, it has stopped hundreds of attempted intrusions.

I believe this program could be a model for the nation.

The idea is to share malware with businesses and Internet Service Providers and say, "Hey, watch out for this."

Your average person using their I-phone, blackberry or cell phone has no idea how vulnerable we are to cyber attacks.

I believe we must launch a public awareness campaign when it comes to cybersecurity.

We need to encourage every computer user in this country to consistently download and install the manufacturers' recommended patches and updates.

Studies show 80% of all attacks can be prevented if this is done.

Security experts are amazed when they go in after the fact and clean up the mess… that simple security measures like patches and updates could have prevented the problem.

We also have to establish a specific procedure for where businesses can go for clean-up help.

And we need one person in charge – coordinating our efforts.

We need to give the Cyber Coordinator in the White House operational and budget authority to work across all agencies and have some real clout to make those important decisions.

He must have a direct line to the President and the power to get things done.

We must do all of this and guarantee civil liberties are protected.

The Army protects the land.

The Air Force protects our skies.

The Navy and the Marines protect our seas.

The Coast Guard protects our coasts.

The Cyber Coordinator must protect cyber space.

Congress must evaluate our existing laws… update them to achieve our goals… and work together as an organized team to get this done.

I understand this is a tall order, but I believe we must act quickly and effectively.

Our nation and our way of life depend on it.

I look forward to testimony from the witnesses here today as we work to achieve these important goals.

Thank you.

########