Iran Stole Marine One Specs ...Really?

9:20 PM PST, March 5, 2009

No, I don’t think so… it seems to be just the latest round of **‘media spin wars.’** Several reports of an alleged ‘security’ breach appeared during the past few days, actually hundreds of links based mostly on NBC’s [WPXI-TV] February 28th “scoop”, which really turn out to be unequivocal endorsements of the new direction that the Administration is pursuing. Because our military security and critical infrastructure needs more attention, I had also previously endorsed President Obama’s initiative to give increased emphasis to these security areas [see Hathaway and my previous blog comments about her].

By just sampling these articles that lie beneath those 'political headlines below, you can see just how poisonous they can be and how their negative effect can mushroom, particularly when you read some of the accompanying postings that they inspire:

- Blueprints and avionics leaked to Iran – Feb 28
- Iran Stole Marine One Specs – Feb 28
- Obama Helicopter security breached – Mar 1
- Obama’s Marine One Secrets in Iran – Mar 1
- Iran gets Marine One plans – Mar 1
- Iran leeches Obama's helo plans - Mar 2

The only thing that appears to be missing are statements from the RIAA and the MPAA, decrying the results of using file sharing programs as 'something that they’ve been warning this Nation about for years!'

A March 2nd AP report finally cleared the air by simply using facts to describe these unclassified events and offering a soul searching opportunity for those who were the earlier reporters. Source in Iran views chopper blueprints – Mar 2 Still unaddressed is the softness of our systems and the challenges that we face in balancing prosperity and security with an open Internet. Large parts of our critical information infrastructure are privately owned, which includes segments of our Defense systems and telecomm networks that need to be separately isolated and protected lest we jeopardize them. The time for sharing responsibility for the securing of cyberspace with the private sector is long overdue, as is the need for a fundamental rethinking of traditional Government's relationships.

An interesting example of an Internet security issue was seen during the Russian-Georgian hostilities of last July and how Internet resources were used. What I read about it sounded like we were involved as a Nation, whether we were or not is immaterial. Maybe the actions of the Atlanta-based ISP and the use of Google Blogger services were just the workings of American private enterprise at its best...
Or maybe not…

We all need to become smarter about cyberspace, recognizing the value and fragility of existing systems and the connectivity that we currently have and better craft them for future use and secure them for common good. But that is not the military's role and if our military strategies include the disruption of communications, spying, spoofing, infrastructure attacks or any similar acts of warfare, such words should never show up on page one of the paper or surface in public political discussions.

Also, on both the domestic and international fronts, traditional crimes of fraud, theft, blackmail, forgery and embezzlement in cyberspace still need to be addressed and this has to be done in an entirely separate camp, law enforcement. The annual cost of cyber crime is estimated to have exceeded one trillion dollars in 2008 worldwide. If these lines become blurred, then we will really have problems. It would be like having everyone talking about the Global War on Terror and the U.S. military's strategic plans in open forums. And just like Eric's grandmother would have said about discussing such topics, "That's not soup talk!"

Think Security; Not Spin! – Bob