

ERIC HOLDER CLAIMS RULE OF LAW EXISTS IN CYBERSPACE

Just days after asking Congress not to give the intelligence community a hard deadline to put a basic cybersecurity measure into place, the Obama Administration rolled out a cybersecurity strategy yesterday with great fanfare. The event itself seemed designed to bring as many Cabinet Secretaries into one place at one time—Hillary Clinton, Gary Locke, Janet Napolitano, and Eric Holder, along with DOD Deputy Secretary William Lynn and White House Cybersecurity Coordinator Howard Schmidt—to give the appearance of real cooperation on cyberspace issues.

The strategy itself is still mostly fluff, with paragraphs like this:

This future promises not just greater prosperity and more reliable networks, but enhanced international security and a more sustainable peace. In it, states act as responsible parties in cyberspace—whether configuring networks in ways that will spare others disruption, or inhibiting criminals from using the Internet to operate from safe havens. States know that networked infrastructure must be protected, and they take measures to secure it from disruption and sabotage. They continue to collaborate bilaterally, multilaterally, and internationally to bring more of the world into the information age and into the consensus of states that seek to preserve the Internet and its core characteristics.

And loaded paragraphs like this, in the section on military goals:

Recognize and adapt to the military's increasing need for reliable and secure

networks. We recognize that our armed forces increasingly depend on the networks that support them, and we will work to ensure that our military remains fully equipped to operate even in an environment where others might seek to disrupt its systems, or other infrastructure vital to national defense. Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so.

Lucky for DOD, there was no discussion of deadlines anywhere in the document, so they didn't have to admit their plan to "adapt to the military's increasing need for reliable and secure networks" was a long term project.

And then the strategy had a lot of language about norms, which places our cybersecurity strategy in the paradigm and language of international regime development from foreign relations (interestingly, Hillary started off the parade of Secretaries, further emphasizing this diplomatic approach).

But what struck me most about this dog and pony show, delivered on the day SCOTUS endorsed the executive branch's efforts to hide torture behind the invocation of state secrets, was Eric Holder's discussion about rule of law in cyberspace.

In recent months, the Justice Department has announced takedowns of significant criminal groups operating from Romania, Egypt, and elsewhere that had been victimizing American businesses and citizens – including children. We've also brought multiple criminal conspirators to justice for their roles in coordinated cybercrimes that, according to court documents, netted

nearly 1.5 million dollars from U.S. victims. And, just a few weeks ago, we announced an operation to disable an international criminal network that had infected more than two million computers worldwide with malicious software. Until we stepped in – with the help of industry and security experts, as well as key international partners – this malware was allowing criminals to capture bank account numbers, user names, and other sensitive and financial information online.

While we can all be encouraged by these and other successes, we cannot become complacent. As President Obama has repeatedly indicated – we must, and we will, take our global fight against cyber threats to the next level. The strategy that we are announcing today is an affirmation of that promise. It reinforces our nation's support for the Budapest Convention –and for efforts to establish the rule of law in cyberspace. It also reflects our ongoing commitment to prevent terrorists and other criminals from exploiting the Internet for operational planning or financing – or for the execution of attacks. [my emphasis]

We're going to build rule of law in cyberspace apparently. Sort of like an extraterrestrial colony to preserve a way of life that used to exist on Earth (or at least in the US), but no longer does.

So rest assured, if this cyberstrategy is successful, we can expect rule of law in cyberspace as compensation for the fact that the government has destroyed rule of law in meatspace.

Oh, on that note, there was no discussion of any investigation into how it was that a media outlet, Wikileaks, was attacked with a

sophisticated DDOS attack, ultimately damaging
free speech.