I CON THE RECORD ADMITS ALL THIS SPYING ALSO SERVES COUNTERINTELLIGENCE

James Clapper has a statement up at I Con the Record trying to dismiss any concerns that the US is using the same kind of technologies as China uses against its people to crack Tor.

As per usual, Clapper complains that the stories don't paint the Intelligence Community in the light they'd like to be described.

In particular, he complains that — notwithstanding the Guardian's publication of NSA's graphic suggesting every Tor communication hides a bearded terrorist — the stories haven't emphasized the "very naughty" targets of this spying.

> However, the articles fail to make clear that the Intelligence Community's interest in online anonymity services and other online communication and networking tools is based on the undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies.

But that complaint comes with a new admission,

one that has been all but unmentioned since when, on June 10, Clapper's most impressive PRISM success story pertained to cybersecurity. For the first time in quite a while, Clapper today acknowledged NSA uses this not only for counterterrorism and other foreign targets, but also counterintelligence.

> The articles fail to mention that the Intelligence Community is only interested in communication related to valid foreign intelligence and counterintelligence purposes and that we operate within a strict legal framework that prohibits accessing information related to the innocent online activities of US citizens.
>
> Within our lawful mission to collect foreign intelligence to protect the United States, we use every intelligence tool available to understand the intent of our foreign adversaries so that we can disrupt their plans and prevent them from bringing harm to innocent Americans. [my emphasis]

The admission is important not just because Clapper and Keith Alexander have consistently been trying to hide the cybersecurity application of this. But because it makes clear that NSA requires no foreign nexus to target Tor communications.

Which they couldn't well require in any case, since the design of Tor ensures the government can't know whether an encrypted message is a domestic or foreign communication.

Of course, once you include counterintelligence (and threats to property) as a valid excuse to keep encrypted communications indefinitely and even to compromise people's computers (see slide 16), particularly in an environment where leaks of even unclassified information are treated as spying, then the distinction between "citizens" and "targets" crumbles.