MIRROR, MIRROR, ON THE WALL, WHO'S THE HACKIEST OF THEM ALL?

Here are some excerpts from the Global Threats report pertaining to the cyber threat.

> We assess that computer network *exploitation* and *disruption* activities such as denial-of-service attacks will continue.
>
> [snip]
>
> … many countries are creating cyber defense institutions within their national security establishments. We estimate that several of these will likely be responsible for offensive cyber operations as well.
>
> [snip]
>
> Critical infrastructure, particularly the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems used in water management, oil and gas pipelines, electrical power distribution, and mass transit, provides an enticing target to malicious actors. Although newer architectures provide flexibility, functionality, and resilience, large

> segments of legacy architecture remain vulnerable to attack, which might cause significant economic or human impact.

It’s as if the intelligence community called up NSA and CyberCommand, asked what they had been working on, and then “assessed” that those targets presented threats going forward.

And while I expect that China commits what would be judged the largest number of hacks (in part because much of the information we steal right from the communication backbone they would have to hack to get), the inclusion of SCADA in the list of vulnerabilities is particularly rich, considering we are believed to have pioneered that kind of attack with StuxNet.

Again, I’m not denying these other entities hack (the unclassified version of the report left off Israel and France, as unclassified versions tend to do). Just that we continue to exhibit no awareness that some part of this threat amounts to our genie blowing back in our face.