RICHARD CLARKE ALSO SUGGESTS HACKING HAS MADE F-35 INEFFECTIVE

A number of people have pointed to this interview for Richard Clarke's suggestion that the US, not Israel, bears most of the responsibility for the StuxNet attack.

But I'm just as interested in his assessment that hacking threatens to undercut our ability to deploy our fanciest war toys.

> "I'm about to say something that people think is an exaggeration, but I think the evidence is pretty strong," he tells me. "Every major company in the United States has already been penetrated by China."
>
> "What?"
>
> "The British government actually said [something similar] about their own country. "
>
> Clarke claims, for instance, that the manufacturer of the F-35, our next-generation fighter bomber, has been penetrated and F-35 details stolen. And don't get him started on our supply chain of chips, routers and hardware we import from Chinese and other foreign suppliers and what may be implanted in them—"logic bombs," trapdoors and "Trojan horses," all ready to be activated on command so we won't know what hit us. Or what's already hitting us.
>
> "My greatest fear," Clarke says, "is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our

> research and development stolen by the Chinese. And we never really see the single event that makes us do something about it. That it's always just below our pain threshold. That company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars on R&D and that information goes free to China….After a while you can't compete."
>
> But Clarke's concerns reach beyond the cost of lost intellectual property. He foresees the loss of military power. Say there was another confrontation, such as the one in 1996 when President Clinton rushed two carrier battle fleets to the Taiwan Strait to warn China against an invasion of Taiwan. Clarke, who says there have been war games on precisely such a revived confrontation, now believes that we might be forced to give up playing such a role for fear that our carrier group defenses could be blinded and paralyzed by Chinese cyberintervention. [my emphasis]

The other day, I suggested that our inability to protect our defense and defense contractor networks means we're wasting billions on hacking-related rework.

That's not the only way our vulnerability to hacking will rot our national security supremacy. As Clarke notes, it will make all the defenses we build into our weapons systems less effective. All of which won't stop us from dumping the national treasure into already-compromised toys. It'll just make those toys more expensive.