UNDER KEITH ALEXANDER'S GUARD, AMERICA CAN BE PLUNDERED LIKE A COLONY

Admittedly, Keith Alexander made things very easy on himself in this article on "Defending America in Cyberspace" by not mentioning the way DOD (or our ally, Israel) let StuxNet go free, not only exposing the attack on Iran, but also providing a map and code that others can use on us.

That reckless mistake and its potential consequences remains unmentioned, however, in the piece in which Alexander claims that his team has found and is implementing the magic formula for defending the country in cyberspace.

> We have learned through two decades of trial and error that operationalizing our cyberdefenses by linking them to intelligence and information-assurance capabilities is not only the best but also the only viable response to growing threats.

We know how to defend the country, Alexander says. It involves creating security holes, then using them to find out who will attack us, all while living on the network and watching what private citizens are also doing.

But then Alexander utterly contradicts the claim that his team has found the successful formula by describing the sheer scale of successful attacks against the US, suggesting it rivals the plunder of the Mongols and the colonies (though curiously, not slavery).

> Three times over the previous millennium, military revolutions allowed

> forces to conquer huge territories and
> forcibly transfer riches from losers to
> winners (namely, in the Mongol conquests
> of China, Russia and Baghdad; the
> Spanish conquests of the Americas; and
> the European empires in the nineteenth
> century). Remote cyberexploitation now
> facilitates the systematic pillaging of
> a rival state without military conquest
> and the ruin of the losing power. We
> have seen a staggering list of
> intrusions into major corporations in
> our communications, financial,
> information-technology, defense and
> natural-resource sectors. The
> intellectual property exfiltrated to
> date can be counted in the tens to
> hundreds of thousands of terabytes. We
> are witnessing another great shift of
> wealth by means of cybertheft, and this
> blunts our technological and innovative
> edge. Yet we can neither prevent major
> attacks nor stop wholesale theft of
> intellectual capital because we rely on
> architecture built for availability,
> functionality and ease of use—with
> security bolted on as an afterthought.

This repeats a claim he and others have made
repeatedly, though after having been proven
wrong about past claims about the scale of
financial wealth transfer, he seems to have
shifted to measuring the plunder that has
occurred on his watch in terabytes, not dollars.
Our country — which he has served in a key
defense role for 8 years — has been plundered
like a colony (I don't buy this, mind you — I
find the analogy downright offensive. But it is
the argument he's making).

In much of the rest of his paper, Alexander
explains his future plans, which we should
follow, he tells us, because he has been so
successful that our country has been plundered
like a colony.

I wonder. Might the most sane response to this

paper be to, at a minimum, question what success looks like? At a minimum, might we discuss publicly some alternatives? And if being plundered like a colony is not our goal, perhaps we should consider whether what Alexander presents as the "only viable response" really is?