KEITH ALEXANDER: ARMAGEDDON FOR THEE BUT NOT FOR ME

The other day, I noted how in an essay touting his cybersecurity approach, Keith Alexander claimed that approach had permitted the US to be plundered like a colony.

Hardly a selling point.

I want to return to Alexander's essay, but first, consider Bruce Schneier's conception of the Internet as an increasingly feudal society.

> I have previously characterized this model of computing as "feudal." Users pledge their allegiance to more powerful companies who, in turn, promise to protect them from both sysadmin duties and security threats. It's a metaphor that's rich in history and in fiction, and a model that's increasingly permeating computing today.
>
> Medieval feudalism was a hierarchical political system, with obligations in both directions. Lords offered protection, and vassals offered service. The lord-peasant relationship was similar, with a much greater power differential. It was a response to a dangerous world.
>
> Feudal security consolidates power in the hands of the few. Internet companies, like lords before them, act in their own self-interest. They use their relationship with us to increase their profits, sometimes at our expense. They act arbitrarily. They make mistakes. They're deliberately—and incidentally—changing social norms. Medieval feudalism gave the lords vast powers over the landless peasants; we're seeing the same thing on the Internet.

> [snip]
>
> Most people, though, are stuck in the middle. These are people who have don't have the technical ability to evade either the large governments and corporations, avoid the criminal and hacker groups who prey on us, or join any resistance or dissident movements. These are the people who accept default configuration options, arbitrary terms of service, NSA-installed back doors, and the occasional complete loss of their data. These are the people who get increasingly isolated as government and corporate power align. In the feudal world, these are the hapless peasants. And it's even worse when the feudal lords—or any powers—fight each other. As anyone watching *Game of Thrones* knows, peasants get trampled when powers fight: when Facebook, Google, Apple, and Amazon fight it out in the market; when the U.S., EU, China, and Russia fight it out in geopolitics; or when it's the U.S. vs. "the terrorists" or China vs. its dissidents.
>
> [snip]
>
> Without the protection of his own feudal lord, the peasant was subject to abuse both by criminals and other feudal lords. But both corporations and the government—and often the two in cahoots—are using their power to their own advantage, trampling on our rights in the process. And without the technical savvy to become Robin Hoods ourselves, we have no recourse but to submit to whatever the ruling institutional power wants.

Where we're headed, Schneier says, particularly in the face of cybercriminals whose power is vastly magnified through technology, is increased servitude to both private corporations

and governments, but that offers little protection when our pledged lords fight each other.

Now back to Alexander's pitch that his approach to cybersecurity is best.

We need to embrace it, General Alexander suggests, because of the threat of Armageddon, the possibility that malicious actors will carry out a systemic attack that will result in a kind of Armageddon.

> The features that allow all these infrastructure sectors to link together in cyberspace, however, also make them accessible to intruders from almost anywhere at a comparative minimum of cost and risk. The cyberdimension, therefore, adds an unprecedented degree of complexity and vulnerability to the task of defending ourselves against a modern-day "Armageddon" strategy.
>
> The century-old dream and nightmare of crippling a modern society by wrecking its infrastructure—or just by disturbing its synchronization of functions—is now a reality others are dreaming of employing against the United States. We do not know how effective such a strategy would be against the United States in practice, but glimpses of global financial panics in recent years should raise concern about even partial "success" for an adversary attempting such an attack. [my emphasis]

Frankly, Alexander's mention of the financial crash is a tell. He's right that the damage Wall Street did reveals how damage accelerates in this globalized world, the possibility of an Armageddon. But no one (well, except for me!) has ever suggested NSA use its considerable power to guard against similar bankster-caused systemic disruptions in the future. Until such time as we decide to use this considerable

surveillance power against banks – probably the most dangerous entities in the world right now – or admit that such surveillance really incurs too much cost even against such a grave threat, we simply are picking and choosing where and whom we want to surveil, and right now it's not the most dangerous threats we're surveilling.

Now consider how Alexander portrays USCYBERCOM to function in his vision of cyberdefense.

> The Pentagon is moving to reduce significantly the number of its networks and limit the points where those networks touch the Internet. Its new joint network—the JIE—is inherently more defensible than the fifteen thousand disparate enclaves that currently exist in the Department of Defense. USCYBERCOM is involved in efforts to leverage cloud-computing technology to dramatically increase the ability to safely and securely store and access data.
>
> [snip]

> We are developing a force capable of defending the nation in cyberspace, operating and defending Department of Defense information networks, and providing direct support to Unified Combatant Command plans and operations. These forces must be able to defend our national-security networks, providing a vital sanctuary from which we can operate even while under attack. Having such an assured capability will not only defend Department of Defense and national-security functions, but also help government and civilian networks by convincing adversaries that an "Armageddon" strategy will not succeed against America. [my emphasis]

Alexander describes pulling our defensive forces

substantially off of the public Internet where these malicious actors roam, building a sanctuary — a medieval fortress! — in which the defensive establishment will still be able to function in the event of Armageddon.

But consider the logic: that means the rest of us — who Alexander is demanding must sacrifice our privacy in the name of mutual defense — will be stuck outside the sanctuary, still at the mercy of those malicious actors.

This defensive plan will only work then, if the malicious actors are sufficiently deterred (and acting with sufficient consciousness and rationality, even given the likelihood of unintended consequences in a globalized system) by that "defensive" force holed up in the sanctuary to decide not to attack the world outside the sanctuary. If they're not, then we'll all still be exposed to Armageddon. The defensive establishment will survive to fight the malicious actors, but we may not.

That is, Alexander is describing that same feudal structure Schneier is, in which we're just peasants who must sacrifice for the common defense, without, however, being invited inside the sanctuary he intends to keep safe.

So to sum up what Alexander is offering: a system that has already resulted in plunder on a massive scale (though largely from those whose riches are measured digitally), and the promise that in case of Armageddon, his "defensive" troops will be safe in the sanctuary to fight back.