IF AMAZON WEB SERVICES GOES DOWN, DO THE CLOUD SERVICES AWS PROVIDES THE INTELLIGENCE COMMUNITY TOO?

As you may have heard, Amazon has had a bad outage today, taking down many entities that rely on its cloud service.

Most of the coverage has focused on the private businesses that have been affected, from small businesses to larger ones (I suspect Office Max was broadly affected, because they were down today too), to media outlets.

I want to know if, when Amazon's Northern Virginia cloud services go down, whether the cloud services Amazon provides to the Intelligence Community goes down too. The IC cloud is supposed to be completely separate from AWS' commercial services. But if things are going haywire generally in Northern Virginia, those problems may extend to Amazon's (understood to be NoVA located) IC servers.

I raise that, in part, because of a point I made in these two posts about the new EO 12333 sharing rules Obama implemented in January. The data sharing envisioned can happen in one of three places: on NSA's own servers, on the recipient agency's own servers, or on the cloud.

> NSA may choose to make raw SIGINT available (i) through NSA's systems; (ii) through a shared IC or other Government capability, such as a cloud-based environment; or (iii) by

> transferring some or all of the information to the recipient IC element's information systems. Only information that can be afforded appropriate handling, storage, retention, and access protections by the recipient IC element will be made available.

Indeed, rolling out the IC cloud was a necessary technical precondition for this sharing process.

As I subsequently pointed out, one application for this expanded sharing was to make counterintelligence information — of the kind that would be central to the investigation into Russia's hack of the DNC and/or other influence peddling with Trump allies — more widely available (for example, to CIA and FBI).

> In the procedures, the conditions on page 7 and 8 under which an American can be spied on under EO 12333 are partially redacted. But the language on page 11 (and in some other parallel regulations) make it clear one purpose under which such surveillance would be acceptable, as in this passage.
>
> > Communications solely between U.S. persons inadvertently retrieved during the selection of foreign communications will be destroyed upon recognition, except:
> >
> > When the communication contains significant foreign intelligence or counterintelligence, the head of the recipient IC element may waive the destruction requirement and subsequently notify the DIRNSA and NSA's OGC;
>
> Under these procedures generally, communications between an American and a foreigner can be read. But

> communications between Americans must be destroyed except if there is significant foreign intelligence *or counterintelligence* focus. This EO 12333 sharing will be used not just to spy on foreigners, but also to identify counterintelligence threats (which would presumably include leaks but especially would focus on Americans serving as spies for foreign governments) within the US.
>
> Understand: On January 3, 2017, amid heated discussions of the Russian hack of the DNC and public reporting that at least four of Trump's close associates may have had inappropriate conversations with Russia, conversations that may be inaccessible under FISA's probable cause standard, Loretta Lynch signed an order permitting the bulk sharing of data to (in part) find counterintelligence threats in the US.
>
> This makes at least five years of information collected on Russian targets available, with few limits, to both the CIA and FBI. So long as the CIA or FBI were to tell DIRNSA or NSA's OGC they were doing so, they could even keep conversations *between Americans* identified "incidentally" in this data.

Certain state adversaries would have big incentives to destabilize AWS, just for shits, giggles, and the chaos it would cause. If they could get into Amazon private clients' servers, there would be plenty of data to make such an attack worthwhile.

But if such an attack also affected the IC cloud, that might be a different thing entirely.