ARE ESCAPED ZOO ANIMALS AUTONOMOUS?

Back when David Sanger revealed new details of how StuxNet broke free of Natanz, he used the metaphor of an escaped zoo animal actively unlocking its cage.

> In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.
>
> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. [my emphasis]

This zoo animal found the keys to its cage, broke free, spread to an engineer's computer, failed to recognize its new environment, and then began replicating itself all around the world.

That is, Sanger used the language of a cognizant being, acting as an agent to spread itself. That's not inapt. After all, viruses do spread themselves (though they don't actually go seek out keys to do so).

Which is why this detail, noted in Obama's other pre-Thanksgiving document dump, is so stunning. (h/t Trevor Timm)

> The Defense Department does not require developers of computer systems that launch cyber operations to implement the same safeguards required of traditional arms makers to prevent collateral damage.
>
> [snip]
>
> A directive, released Nov. 21, mandated that automated and semi-autonomous weaponry – such as guided munitions that independently select targets – must have human machine interfaces and "be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force." The mandate called for "rigorous hardware and software verification and validation" to ensure that engagements could be terminated if not completed in a designated time frame. The goal is to minimize "unintended engagements," the document states.
>
> The Pentagon is permitting less human control over systems that deploy malware, exploits and mitigation tools, highlighting Defense's focus on agile responses to computer threats. The document, signed by Deputy Secretary of Defense Ashton Carter, explicitly states that the directive "does not apply to autonomous or semi-autonomous cyberspace systems for cyberspace operations."

We have already lost control of one our semi-autonomous cyberspace operations. The potential danger from its "escape" could be tremendous.

And yet DOD specifically exempts similar operations in the future? So we can commit the same error again?