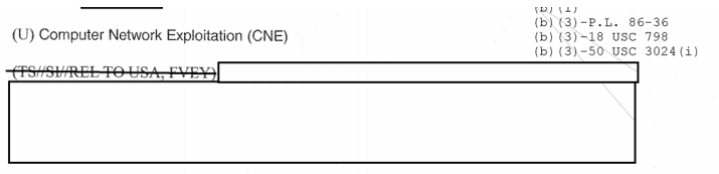
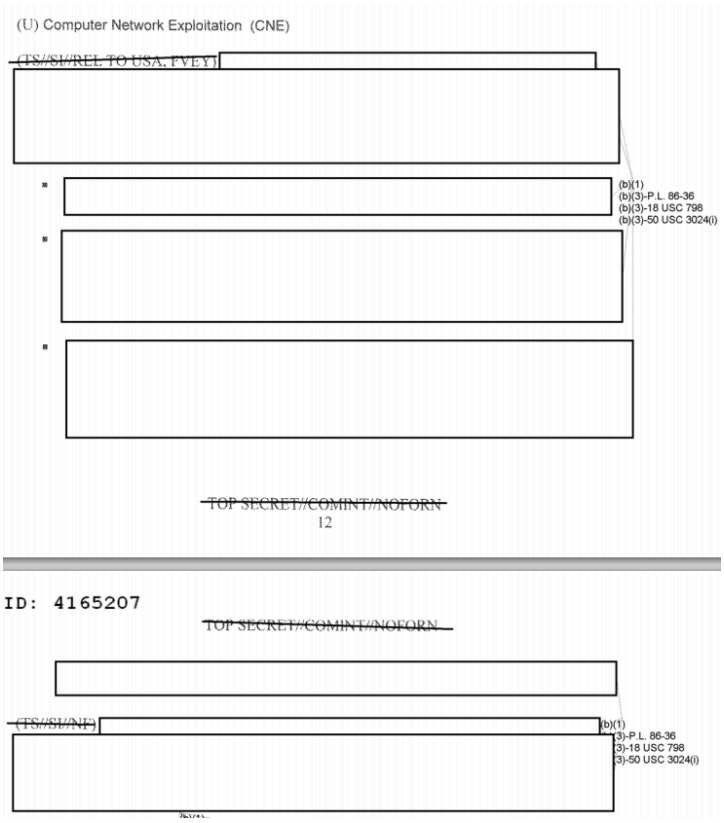
HACKING IN THE IOB REPORTS

If I'm not mistaken, this — in the Q3 2008 NSA Report to the Intelligence Oversight Board — is the first mention of Computer Network Exploitation in the reports.



As with almost every single reference to CNE — that is, hacking, or the use of malware to be able to spy on a target — this one is entirely redacted. (The sole exception is a targeted email that was detasked because the target entered the US, in the Q1 2009 report).

The number/complexity of incidents or details expand for some years, as with this in Q2 2009.



The entries invariably cite 18 USC 798 as a FOIA

exemption. They vary on whether they're FVEY (that is, permissibly shared with members of the Five Eyes) or NF (that is, not to be shared with any foreign government), though in later years the entries have much more frequently been NF — take that, Brits! And the entries appear under "Other," not EO 12333 (which is curious, given that hacking should be governed by EO 12333).

After that first, single-incident mention, CNE appears in each report until Q4 2011, after which it doesn't appear again (though there is an entirely redacted section that appears in all but the most recent report in the EO 12333 section).

I make these observations not because they tell us anything about what kind of hacking the NSA is doing (you can look to Snowden's documents for that). But to lay out several questions.

If — as claimed in Shane Harris' @War hacking is increasingly how we collect SIGINT — how is it regulated? Did NSA, does NSA still, consider it to be something other than EO 12333 collection? What counts as a violation when you're hacking to collect intelligence? To what degree is IOB overseeing the methods used, as opposed to just the actions that'd be violations regardless of the collection type (as detasking someone in the US would be)? And if CNE (hacking) has entirely disappeared from these reports, does that mean NSA has just cleaned up its act, or that it simply doesn't report on this anymore?

I get why these passages are entirely redacted. In part, NSA is sustaining the same myth it sustains when it doesn't admit StuxNet. It's pretending it is not engaging in the same hacking it sanctions North Korea for.

Only it is. Which raises real questions about what kind of oversight it gets.