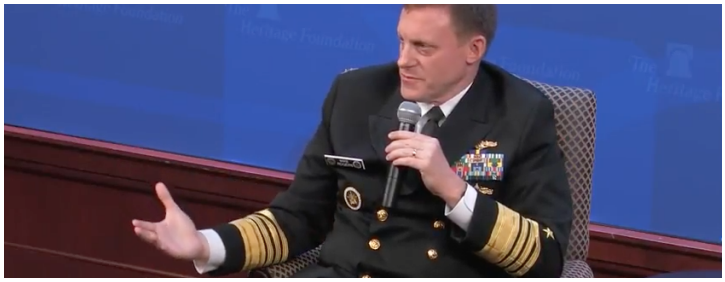
IN DISCUSSION OF UNMASKING ADMIRAL ROGERS GETS CLOSER TO ADMITTING TYPES OF SECTION 702 CYBERSECURITY USE



Last Friday, Director of National Intelligence Dan Coats, Director of NSA Mike Rogers, and FBI Director Christopher Wray did an event at Heritage Foundation explaining why we need Section 702 and pretending that we need it without reasonable reforms. I attended Wray's talk — and even got my question on cybersecurity asked, which he largely dodged (I'll have more about two troubling things Wray said later). But I missed Rogers' talk and am just now catching up on it.

In it, he describes a use of Section 702 that goes further than NSA usually does to describe how the authority is used in cybersecurity.

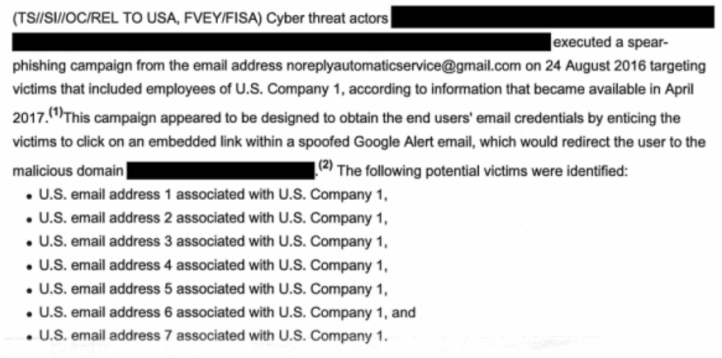
> So what are some examples where we'll unmask? Companies. Cybersecurity. So we'll report that US company 1 was hacked by the following country, here's how they got in, here's where they are, here's what they're doing. Part of our responsibility on the US government side is the duty to warn. So how do you warn US company 1 if you don't even know who US company 1 is? So one of the reasons we do unmasking is, so for example we can take protective to ensure this

> information is provided to the appropriate individuals.

What Rogers describes is an active hack, by a nation-state (which suggests that rule may not have changed since the 2015 report based off 2012 Snowden documents that said NSA could only use 702 against nation-state hackers). The description is not necessarily limited to emails, the type of data NSA likes to pretend it collects in upstream (though it could involve phishing). And the description even includes what is going on at the victim company.

Rogers explains that the NSA would unmask that information so as to be able to warn the victim — something that (via the FBI) happened with the DNC, but something which didn't happen with a number of other election related hacks.

Of course, Reality Winner is facing prison for having made this clear. The FISA-derived report she is accused of leaking shows how the masking works in practice.



(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted] executed a spear-phishing campaign from the email address noreplyautomaticservice@gmail.com on 24 August 2016 targeting victims that included employees of U.S. Company 1, according to information that became available in April 2017.(1) This campaign appeared to be designed to obtain the end users' email credentials by enticing the victims to click on an embedded link within a spoofed Google Alert email, which would redirect the user to the malicious domain [redacted].(2) The following potential victims were identified:

- U.S. email address 1 associated with U.S. Company 1,
- U.S. email address 2 associated with U.S. Company 1,
- U.S. email address 3 associated with U.S. Company 1,
- U.S. email address 4 associated with U.S. Company 1,
- U.S. email address 5 associated with U.S. Company 1,
- U.S. email address 6 associated with U.S. Company 1, and
- U.S. email address 7 associated with U.S. Company 1.

In the case of VR Systems, the targeted company described, it's not entirely clear whether NSA (though FBI) warned them directly or simply warned the states that used it. But warnings, complete with their name, were issued. And then leaked to the press, presumably by people who aren't facing prison time.

In any case, this is a thin description of NSA's use of 702 on cybersecurity investigations. But more detail in unclassified public than has previously been released.