THE PREFERRED ANTI-OBAMA RUSSIAN HACK STORY REMAINS SILENT ON SHADOW BROKERS

Michael Isikoff and David Corn are fluffing their upcoming book on the Russian tampering with the 2016 election. This installment covers the same ground, and the same arguments, and has the same weaknesses that this WaPo article did: It describes how urgent but closely held the CIA tips were (without considering whether the close hold on the intelligence led the IC to make incorrect conclusions about the attack). It describes efforts to make a public statement that got drowned out by the Pussy Grabber and Podesta releases. It airs the disappointment of those who thought Obama should have launched a more aggressive response.

Perhaps the biggest addition to the WaPo version is that this one includes more discussion of Obama's thoughts on cyber proliferation, with the acknowledgement that the US would be more vulnerable than Russia in an escalating cyber confrontation.

> Michael Daniel and Celeste Wallander, the National Security Council's top Russia analyst, were convinced the United States needed to strike back hard against the Russians and make it clear that Moscow had crossed a red line. Words alone wouldn't do the trick; there had to be consequences. "I wanted to send a signal that we would not tolerate disruptions to our electoral process," Daniel recalled. His basic argument: "The Russians are going to push as hard as they can until we start pushing back."
>
> Daniel and Wallander began drafting options for more aggressive responses

> beyond anything the Obama administration or the US government had ever before contemplated in response to a cyberattack. One proposal was to unleash the NSA to mount a series of far-reaching cyberattacks: to dismantle the Guccifer 2.0 and DCLeaks websites that had been leaking the emails and memos stolen from Democratic targets, to bombard Russian news sites with a wave of automated traffic in a denial-of-service attack that would shut the news sites down, and to launch an attack on the Russian intelligence agencies themselves, seeking to disrupt their command and control modes.
>
> [snip]
>
> One idea Daniel proposed was unusual: The United States and NATO should publicly announce a giant "cyber exercise" against a mythical Eurasian country, demonstrating that Western nations had it within their power to shut down Russia's entire civil infrastructure and cripple its economy.
>
> [snip]
>
> The principals did discuss cyber responses. The prospect of hitting back with cyber caused trepidation within the deputies and principals meetings. The United States was telling Russia this sort of meddling was unacceptable. If Washington engaged in the same type of covert combat, some of the principals believed, Washington's demand would mean nothing, and there could be an escalation in cyber warfare. There were concerns that the United States would have more to lose in all-out cyberwar.
>
> "If we got into a tit-for-tat on cyber with the Russians, it would not be to our advantage," a participant later remarked. "They could do more to damage

> us in a cyber war or have a greater impact." In one of the meetings, Clapper said he was worried that Russia might respond with cyberattacks against America's critical infrastructure—and possibly shut down the electrical grid.
>
> [snip]
>
> Asked at a post-summit news conference about Russia's hacking of the election, the president spoke in generalities—and insisted the United States did not want a blowup over the issue. "We've had problems with cyber intrusions from Russia in the past, from other counties in the past," he said. "Our goal is not to suddenly in the cyber arena duplicate a cycle escalation that we saw when it comes to other arms races in the past, but rather to start instituting some norms so that everybody's acting responsibly."

The most dramatic part of the piece quotes an angry Susan Rice telling her top Russian expert to stand down some time after August 21.

> One day in late August, national security adviser Susan Rice called Daniel into her office and demanded he cease and desist from working on the cyber options he was developing. "Don't get ahead of us," she warned him. The White House was not prepared to endorse any of these ideas. Daniel and his team in the White House cyber response group were given strict orders: "Stand down." She told Daniel to "knock it off," he recalled.
>
> Daniel walked back to his office. "That was one pissed-off national security adviser," he told one of his aides.

But like the WaPo article before it, and in spite of the greater attentiveness to the

specific dates involved, the Isikoff/Corn piece makes not one mention of the Shadow Brokers part of the operation, which first launched just as NSC's Russian experts were dreaming up huge cyber-assaults on Russia.

On August 13, Shadow Brokers released its first post, releasing files that had compromised US firewall providers and including a message that – while appearing to be an attack on American Elites and tacitly invoking Hillary – emphasizes how vulnerable the US would be if its own cybertools were deployed against it.

> We want make sure Wealthy Elite recognizes the danger cyber weapons, this message, our auction, poses to their wealth and control. Let us spell out for Elites. Your wealth and control depends on electronic data. You see what "Equation Group" can do. You see what cryptolockers and stuxnet can do. You see free files we give for free. You see attacks on banks and SWIFT in news. Maybe there is Equation Group version of cryptolocker+stuxnet for banks and financial systems? If Equation Group lose control of cyber weapons, who else lose or find cyber weapons? If electronic data go bye bye where leave Wealthy Elites?

Sure, it's possible the IC didn't know right away that this was a Russian op (though Isikoff and Corn claim, dubiously and in contradiction to James Clapper's November 17, 2016 testimony, that the IC had already IDed all the cut-outs Russia was using on the Guccifer 2.0 and DC Leaks operations). Though certainly the possibility was publicly discussed right away. By December, I was able to map out how it seemed the perpetrators were holding the NSA hostage to any retaliation attempts. Nice little NSA you've got here; it'd be a shame if anything happened to it. After the inauguration, Shadow Brokers took a break, until responding to Trump's Syria strike by complaining that he was abandoning

those who had gotten him elected.

> Respectfully, what the fuck are you doing? TheShadowBrokers voted for you. TheShadowBrokers supports you. TheShadowBrokers is losing faith in you. Mr. Trump helping theshadowbrokers, helping you. Is appearing you are abandoning “your base”, “the movement”, and the peoples who getting you elected.

That was followed by a release of tools that would soon lead to billion dollar attacks using repurposed NSA tools.

As recently as February, the NSA and CIA were still trying to figure out what Russia (and the stories do appear to confirm the IC believed this was Russia) had obtained.

I mean, it’s all well and good to complain that Obama asked the NSC to stand down from its plans to launch massive cyberattacks as a warning to Putin. But you might, first, consider whether that decision happened at a time when the US was facing far greater uncertainty about our own vulnerabilities on that front.