UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 16

A Case of Russian Disinformation to Exploit Fears about US Election Hacking

Helen Oliver **20 October 2020**

Executive summary

CCC COVID Briefing Papers are an ongoing series of short-form, open access reports aimed at academics, policymakers, and practitioners, which aim to provide an accessible summary of our ongoing research into the effects which the coronavirus pandemic (and government responses) are having on cybercrime.

In this report, we describe the journey through Twitter of a Russian newspaper article about hackers breaching US electoral data. Rather than a major breach, this was in fact a trivial collection of largely public data. Some English-speaking journalists reacted with alarm, though some corrected themselves once they understood the actual significance of the "hack". This paper gives an overview of the progression of media reactions to the article. The real story was not the hack, but the use of news reporting to stoke fears that President Trump is a "strongman" who will always succeed in subverting democratic processes in his favour.

Person, woman, man, superman, strongman

There have been reports that President Trump, on leaving hospital after COVID-19 treatment, considered opening his shirt to reveal a Superman shirt underneath. True or not, the story is consistent with established impressions of the President's media persona. In this narrative, projecting strength is psychologically necessary for him and he reserves his admiration for other world leaders to those who project the level of power he aspires to attain. One such leader is, famously, the Russian president, alleged instigator of what strategic expert Thomas Rid called "the biggest election hack in US History" – until 2016 at least.

Read all about it

At 01:00 BST on 1 September 2020, the Russian newspaper Kommersant published an article with the headline **"The hackers have turned to the State Department – American voters' data has appeared on the Russian darknet"**. Almost six hours later, at 06:56 BST, the first tweet (that I could find) of the article appeared, from a small unregarded Russian language account. At 07:00 BST the first English-language tweet of the article was published, by the more popular account of Matthew Luxmoore, the Moscow correpondent of Radio Free Europe/Radio Liberty. Luxmoore wrote that the hackers had "doxxed" millions of US residents, and picked out the Kommersant article's claim that one of the hackers had used "SQL Injection" to access allegedly vulnerable voter databases.

Look into my eyes

There are Russian information antics in this story, but not where Luxmoore was looking. The databases in question were electoral rolls, which are publicly purchasable for a small fee. A jargon phrase like "SQL injection" is just obscure enough that a non-technical reader might reasonably doubt their understanding of the supposed hack. This is precisely what happened with Luxmoore, who admitted that he was "not sure what to make of this". By alleging that a great and terrible hack had occurred, the article drew his attention

away from *which* data were "hacked" and onto the *way* they were hacked, successfully using the trivial technical aspects of the case to propagate uncertainty about the security of US electoral data. The article even briefly fooled Dmitri Alperovitch of CrowdStrike.

Even taking the context into account – Russia, where hacked data is bought and sold almost openly – this might as well be a story about a Russian hacker stealing a pack of chewing gum. Of course the nature of the stolen goods and the way they were accessed are more important than the monetary value. However, it's difficult to see why Russian hackers having this data is more alarming than American hackers having it, *once you know what the data actually is*.

The answer is right in front of you

There were a range of responses to Luxmoore's tweet, of which only one did not take it at face value (Figure 1); unfortunately for Anglosphere readers, this tweet was in Finnish.

Figure 1: *"In this way, among other things, a narrative about the unreliability of the election is constructed in support of Trump. Perhaps also the basis for legal action to challenge the election results in court. Michigan is also one of the most important electoral states in the election."*

By lunchtime, Meduza in English had reported on the story, though they added a correction prominently and promptly at the top of the page.

Shortly after 1pm, the user @pierrevaux tweeted a fact check after searching the "hacker" named in the article. Another user replied with this fact check to Carole Cadwalladr of the *Observer*, after her reaction to a report in the Moscow Times: *"This time we can see it happening in real time. And there's nothing we can do to stop it..."*

Five minutes later, the Michigan Department of State sent an explanation to Julia Ioffe of *GQ*, who had tweeted the Kommersant article with no fewer than three alarm emojis. The State Department warned the public about attempts to "hack their minds"; and Ioffe, like a number of her fellow journalists, deleted her tweet.

Conclusions

The Kommersant article appeared to be about Russian cybercrime, but it elicited anxious reactions among opposition voters who already feared for the integrity of the US election, effectively contributing to the strongman con, an effect which was propagated through quick reactions on social media. In fact, many people spotted the misinformation and corrected themselves and others; the voice of reason can also be amplified by social media.

At the Cambridge Cybercrime Centre we make our research data available to other academics, sometimes before we have looked at it ourselves! Researchers can be provided access to our 'CrimeBB' dataset of (26 and counting) underground cybercrime forums, our extensive collections of chat channel data, and our new collections of forums relating to online right-wing extremism and radicalisation. We can also share email spam and sensor data related to DDoS and IoT malware. All these collections are regularly updated and can be rapidly provided under licence – for full details see: `https://cambridgecybercrime.uk`

The full set of CCC COVID Briefing Papers can be found at: `https://cambridgecybercrime.uk/COVID`