Curry J. and Blanks L. (2018) Dezinformatsiya and the Art of Information Warfare

ITNOW, Vol 60 (3) 1 September 34–35, https://doi.org/10.1093/itnow/bwy070

Dezinformatsiya and the Art of Information Warfare

Russian use of cyber power to meddle in elections is well-known, but its effectiveness is less clear. However, in any discussion of this topic it should be noted that the Russians themselves deny the allegations and blame Western governments for this 'fake news'. It should also be noted that is not alone in this space. For example, it estimated that up to eighteen countries saw foreign influence having a significant impact on the outcome of their elections in 2016 alone.

Dezinformatsiya

Before analysing Russian efforts to destabilise recent elections, it is essential to understand the art of "dezinformatsiya". These are the methods used to influence and alter Western perception; cyber-power is just a new tool for their campaigns. The use of dezinformatsiya stems from the Soviet Era, when the GPU (the predecessor to the KGB) suggested: "the establishment of a special disinformation office to conduct active intelligence". This office played an integral role in both domestic and foreign affairs during the early twentieth century, often using disinformation tactics. *Active measures* have developed well beyond the use of lies and fake information as originally used by the GPU. Some of these measures included:

- Forgery: Altered or concocted documents which are designed to trick the media, political officials, and intended to sway public opinion. They often only have to be believable for a short period of time to make an impact.

- Fake-news: Planting stories into the media which are beneficial to Russia or Russian interests. The most successful examples are where the 'news' was published in pro-Russian outlets with the hope that Western media will the recirculate the information therefore legitimising it.

- Front Organisations: Unaffiliated groups who are secretly pro-Russia. Potentially, they could even unwittingly support the Soviet ideology and agenda.

- Human Assets: This includes a broad spectrum of people: from spies, to people who are just willing to help, perhaps even be paid legitimately to produce output favourable to Russia.

The U.S Presidential Election (2016)

The aim of the alleged Russian campaign was to damage the reputation of Hilary Clinton and bolster support for rival candidates such as Donald Trump. Clinton was seen as an 'anti-Russian hawk', who if elected, would make things difficult for Russia. In the summer of 2016, the America public were faced with choice between a reality TV business man and an established politician from Washington. Neither was that popular.

There was a continual succession of hacking attempts on the accounts of those associated with the both sides of the campaign, including their families, but nearly all the embarrassing leaks were from Clinton's campaign. Even more worrying was the concerted hacking of election officials accounts, those who were responsible for the actually counting, but there is no evidence that this was used to influence the counting on the day.

In addition to the above there were two very successful attacks. The first was on Hilary Clinton and how she achieved the Democratic Party nomination. A WordPress page posted by *Guccifer2.0* started to dump embarrassing emails and memoranda hacked from the Democratic National Committee systems. This showed the latter were determined to appoint Clinton over her more moderate rival and they did not put Clinton or the nomination committee in a flattering light. Wikileaks, a source that delights in embarrassing America, posted even more leaked information. It did not take security researchers long to identify that a phishing attack had compromised the National Committee's network and could be traced back to *Fancy Bear* and *Cozy Bear*, two powerful Russian hacking groups with close links to the Russian government.

The second very successful attack was the familiar issue of senior managers using personal devices for work. Prior to Clinton being made Secretary of State in 2009, she was using a Blackberry for her emails and this was linked to a private server in her home. This was very convenient, easy to use and for a private citizen, Blackberry has a reputation for being secure. The problem was she carried on using the Blackberry, as she was familiar with it, rather than the allocated computer in her government office. Her emails included content that was classified and should not have been sent outside the US government network. The story of whether she had committed a crime, by sending government emails via a private email account, and whether the emails had been hacked, damaged her election campaign.

Looking back from 2018, most researchers agree that cyber security was at the heart of Hilary Clinton losing.

The Brexit Vote (2016)

Attempts by Russia to sway preference for Britain leaving the EU have received far less publicity than that of the U.S election. The campaign to disrupt the EU referendum included some of the tactics that Russia used in the U.S election; the key difference was in the UK social media was the primary tool. In a recent study by Bastos and Mercea titled *The Brexit Botnet and User-Generated Hyper-Partisan News*, they found that over thirteen thousand Twitter accounts linked to Russia were posting large amounts of pro-Brexit content.

One such example of a prolific Russian Botnet was that of the twitter account *SouthLoneStar* who garnered widespread media attention after the terror attacks outside of Westminster. Although this event took place after the referendum results, analysis of the account showed tweets dating back over the past few years; often participating in political discussions with a pro-leave stance. Such botnets were carefully designed to fuel discussion with a right-wing agenda, where the account seemed to be spreading anti-immigration feuds.

Use of these tactics over social media was not confined to the Twitter platform, however, with reports of compromised content on Facebook and Google. Despite numerous reports of Russian 'Troll Factories', it is hard for most people to imagine entire office blocks full of people working on concerted efforts to spread 'fake news'. Although the effect of these 'trolls' is still being researched,

if you accept the idea that social media influence people's opinions, then you accept that foriegn 'trolls' played a role in the Brexit vote.

General Lessons

There are many lessons from the experience of the US Presidential election and the BREXIT Referendum. One is that disinformation spread through the channels of social media is a threat to the democratic system. To counter this, more transparency is needed from the likes of Facebook and Google on the data that they collect and share. Governments need to actively countering 'fake news', but without interfering with the right to free speech, even those saying the outrageous.

The second lesson for business is the same techniques of *dezinformatsiya* that have been used to influence elections can be targeted at an individual business. What business would not be damaged by a well-coordinated and timed brand reputation type attack? It is an interesting scenario to add to your list of cyber wargames; one where a company is faced by a determined effort by a red team, who want to remove your business from a contract bidding process. They do this not by traditional hacking, but just using information warfare. Of course, a cyber wargame is only a game and reality is always different, but a game on this topic for a few hours will help give the leaders of your business the mental agility to cope if faced by a real world brand reputation attack.

Further Reading

Bastos, M. T. and Mercea, D. (2017) *The Brexit Botnet and User-Generated Hyperpartisan News*. http://openaccess.city.ac.uk/18143/

House of Commons Library (2017) *Russian interference in UK politics and society*. http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2017-0255

Office of the Director of National Intelligence (2017) *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. https://www.dni.gov/files/documents/ICA_2017_01.pdf