

## Election fever?

---

30<sup>th</sup> October 2020

**Once again, the US election is to be fought between the two least-liked candidates in history and, once again, legitimacy concerns are swirling. President Trump has, without any evidence or provocation, declared the very practice of mail-in ballots to be ‘fraudulent’ and has openly stated that he is only likely to recognise the contest as legitimate... if he wins it. However, what is arguably lost in the slanging match between Trump and Biden is the return of a central theme from 2016: that Russia (and others) looking to interfere and possibly manipulate the result. And arguably if the election of the leader of the free world is not free, how can we ever trust anything again?**



The rap sheet against the Russians in 2016 was extensive, even if it was not undeniably proven: enacting a hack against the Clinton team’s servers, targeting of Democratic databases and promotion of knowingly false social media material. This time, the song remains the same, with the NCSC putting forth the view that the Russians are attempting to ‘denigrate’ Biden and his campaign through amplification of derogatory social media stories and attempted control of the public narrative. It is also understood that a communications firm working with his team was the target of an attempted Russian breach, although no data was taken: something which is ultimately immaterial if the potential exists for the hackers to just try again until, in the maxim of cybersecurity, they get lucky once.

As if it were needed (and it was not), October 2020 has also seen the announcement that six Russian intelligence officers were being charged with a series of cyberattacks that targeted the Olympics (from which all Russian-flagged athletes were banned), the upcoming French presidential election, and American businesses and vital infrastructure. Although the Trump-Biden contest was not included in the deposition, the six men charged, and their unit, are believed to have been involved in the Democratic hack of 2016 (one officer in particular was charged by Robert Mueller’s report) and the general picture painted of the Russian state’s capacity for deep-rooted, highly damaging intrusions is once again confirmed. Few serious Kremlinologists believe that Russia is not attempting in some way to smooth the way for Trump to be re-elected, and whether this be at local level of tapping into the networks of local parties and affiliations, or more nationally through campaigns of disinformation and attempted vote manipulation, madness like “QAnon” has already proven that at times, people do not need much convincing.

In the interests of 'balance' it must be pointed out that China is considered to be broadly pivoting towards Biden. US National Security Advisor Robert O'Brien claimed back in August that China was 'the most active' of the foreign nations looking to destabilise the election, although whether his refusal to elaborate was down to genuine security concerns or fear that they would do so in favour of Biden, is unclear. There is precedent in China's alleged hacking of the Obama and McCain campaigns back in 2008; but this time around, the action the country has taken, or is willing to take, is considered to be defensive towards China's own position rather than being more aggressive. It may be that even China has decided that a further four years of Donald Trump is too much for the world to bear...

Meanwhile Iran is an unknown quantity: largely focusing on domestic issues, it nevertheless suits the Iranian agenda to paint any incumbent of the White House as incompetent and weak and so may have a hand in propaganda and disinformation disseminated regarding both candidates. Notably, it is understood to be responsible for sending threatening emails to Democratic-registered voters, under the cover of the "Proud Boys" far-right agitation group in an attempt to stir further controversy and discord in the run-up to the election. This sort of involvement, even if on a relatively minor scale, could not only swing a particular vote but also act towards the normalisation of this election-tampering practice.

Ultimately all of the above might be considered immaterial when the President himself has not committed to a peaceful transfer of power and has been sowing the seeds for months that will enable his support base to refuse to recognise a result that goes against him. Foreign interference may be growing and becoming normalised, but given all of the disinformation and feverish insanity whipped up by the Trumpian base in recent months, should it be a surprise that the entire process is open to ridicule and compromise? November 3 might be the first indication of whether America has woken up to the delusions of the past half-decade, but given that an academic study of Gothenburg University's V-Dem Institute has found that the Republican Party (or the Trump-infused extreme wing of it) is at its most illiberal ever recorded, this is a malaise which does not look to have a cure anytime soon.

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

**To find out more or to arrange a meeting to discuss your business needs, please...**  
**email the team at [info@kcsgroup.com](mailto:info@kcsgroup.com) or call (00 44) 2072451191**

---