

U.S. election threat bigger than Russia

Russia, China and Iran are all seeking to influence the U.S. presidential election in November – with Kremlin-linked interference in 2016 regarded as a trial run, according to intelligence assessments



Yevgeny Prigozhin (above), close associate of President **Vladimir Putin**, operates St Petersburg-based **Internet Research Agency** (right) which targeted Democrats and African-American community to boycott 2016 election



■ **Phishin:** Attacks begin on fringes of campaign – think-tanks, academics and political consultants with weak

cybersecurity. Once inside, hacker sends emails with PDF files from “trusted” accounts to members at campaign headquarters.

When files are opened, network is infected

■ **Audio phishin:** Synthetic-audio software allows hacker to mimic voice of campaign official, to send voicemail messages



■ **Illegal ads:** Trolls steal identities of U.S. citizens to hide foreign origin of funds used to buy political ads. Facebook’s algorithms send ads to U.S. voters passionate about themes being pushed

LIKE
IF YOU BELIEVE



■ **Active Measures:** Trolls, with automated bots, create groups on social media organized around most divisive issues in U.S. life. Groups intensify lies and distrust

■ **Leaks:** Hackers steal presidential campaign emails and publish genuine emails along with fake, incriminating, emails to give them credibility



■ **Screen to street:** Social media pages convene demonstrations and counter-demonstrations in same place at same time

■ **Hack the vote:** Hackers flip digits in addresses on voter-registration database – voters’ photo IDs no longer match official records. Confusion and anger at polling stations stokes suspicion about integrity of vote

