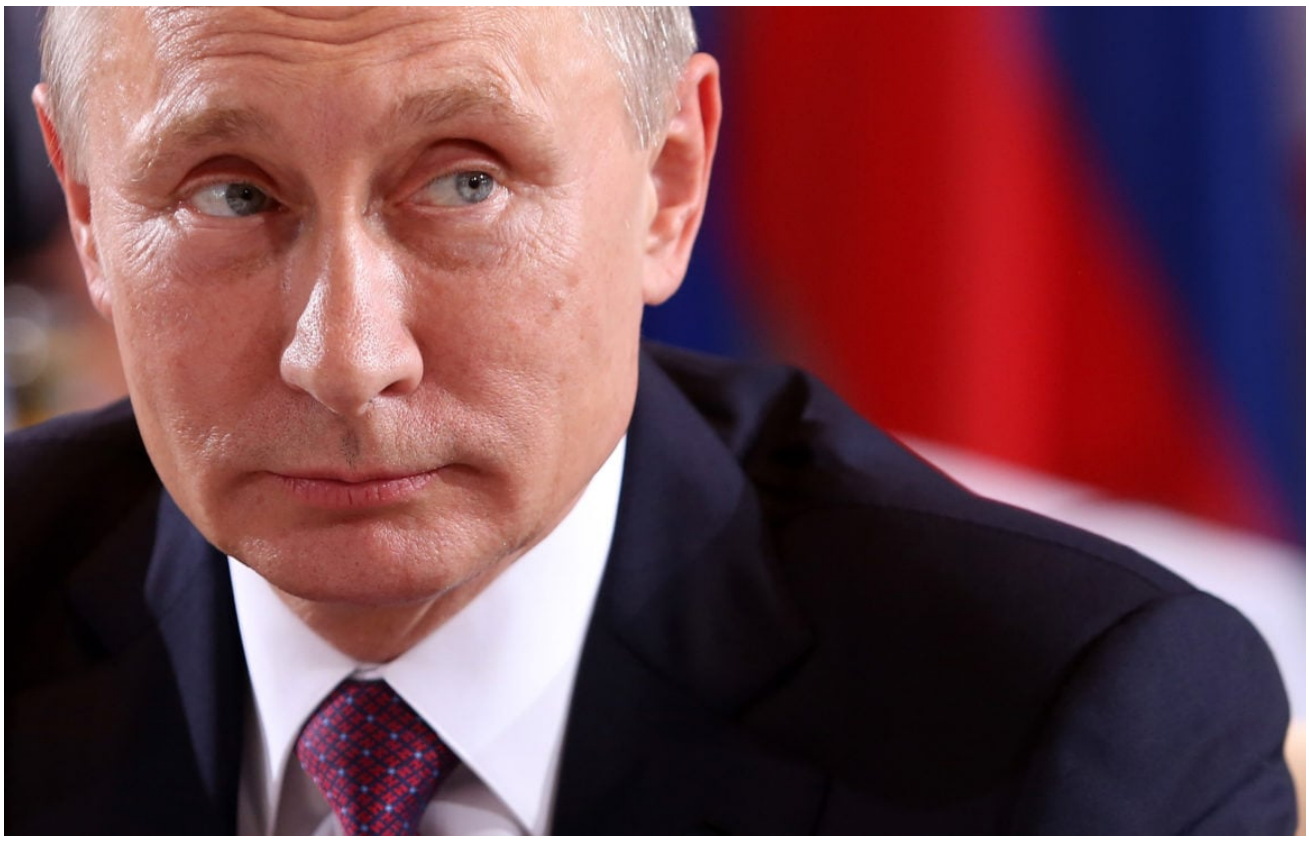
Russian Spying and the Virus

by Michael Curtis



I've got my eyes on you so best beware where you roam. I've set my spies on you so don't stray too far from home.

On July 17, 2020 authorities in the Kremlin issued a statement, "We have no information on who could have hacked pharmaceutical companies and research companies in Britain. Russia has nothing at all to do with those attempts." Other authorities were less ignorant and have made the issue clear, directing attention directly at "Russian spies," not simply as previously and merely implicitly at "state-backed hackers." Moreover, the UK statement accusing the Russians of spying is focused on a specific issue, the vaccine. The UK National Cyber Security Center issued a statement a day earlier that a Kremlin related group, acting as part of Russian intelligence, was attempting to steal research on Covid-19 vaccine development and testing, and that there was an ongoing cyber

campaign to steal intellectual property about a possible Covid-19 vaccine. Fortunately, there is no evidence to suggest that Russia has succeeded in obtaining key research information and has had only limited success in its spying.

Though Russian intelligence efforts may now have concentrated on the issue of the vaccine, new revelations have revealed Russian involvement," Russian actors," in unending intelligence and practical operations in Britain and other countries in recent years. Those "actors" attempted to disrupt the UK energy grid on the day of the 2017 parliamentary election, and leaked material, disinformation, during the UK 2019 national parliamentary campaign. The false information, including statements that the National Health Service was for sale, were used by the then leader of the Labour Party, Jeremy Corbyn ,during the campaign. A major effort of Russian hackers had also been to try to target the Foreign Office and the Porton Down lab of the Ministry of Defense in 2018.

Russia is fomenting discord between the UK and the U.S. In October 2019 it was responsible for leaking documents put on Reddit, suggesting that the UK was giving way on the trade deal with the U.S. by allowing chlorinated chicken from the U.S. to be sold in the UK. A month later, in November, a false 451 page document was issued alleging that National Health services would be changed as part of the U.S.-UK trade deal. The information was also disseminated via the social media platform Reddit.

It is abundantly clear that Russia, like China, has been active in trying to destabilize the U.S. and western democratic countries, and sow discord among them. Some examples are well known. During the 2016 U.S. presidential election, Russia targeted information in all 50 states, with misinformation on social media, and hacked campaign organizations. It also attempted to influence the French election in 2017, introduced false information about Norway politics in 2017, tried to discredit the World Anti-Doping

Agency, and OSCE, the Organization for Security and Cooperation in Europe.

Russia also interfered in other European affairs. In the politics of Moldovia, between Ukraine and Romania, it supported political candidates favorable to the East. Russia was linked to the failed coup in Montenegro in 2016 led by leaders of the opposition in that country and by Russian nationals. A number of Russians were charged with the attempted murder of three Bulgarians arms dealers by poisoning. Germany in 2015 exposed Russian responsibility for hacking their parliament.

Russia has mastered the art of disinformation. The Internal Research Agency the Russian military intelligence agency, Secondary Infektion, planted false stories, especially on social media before amplifying them on Facebook, and forged documents to sow conflict in western countries and engage in smear campaigns. The campaigns were widespread. The U.S. and NATO were aggressive powers. German Chancellor Angela Merkel is an alcoholic, Senator March Rubio has accused the UK of spying on the U.S., and of interfering in the 2018 election, the U.S. was trying to provoke an uprising in Azerbaijan. The U.S. was also responsible for creating a variety of diseases in Covid-19, Bill Clinton was in the pay of Saudi Arabia, former prime minister Theresa May, a World War I fighter pilot had shot down a European plane, French President Emmanuel Macron was the new hope of migrants in Europe, leaders of the anti-Brexit campaign in Britain were planning to assassinate Boris Johnson.

Perhaps for Westerners a crucial line was drawn by Russian activity in the UK, with the poisoning in a London restaurant in 2006 of Alexander Litvinenko by radio active Polonium-210 sprayed in a cup of tea. The substance could be traced to a Russian nuclear power plant. In April 2018 an unsuccessful attempt was made to poison the former Russian spy and double agent Sergei Skripal in Salisbury, England, with the deadly

nerve agent gas Novichok.

The game is afoot. On July 16, 2020 Russia announced its intention to produce 200 million doses of an experimental vaccine for Covid 19 it was developing. This prompts suspicions it has been able to use data and intellectual property stolen from the west. Russian action stems from the reality that British and U.S. institutions, are leading efforts to produce a coronavirus vaccine and that both countries are trying to counter attacks by groups planning to steal information. Western groups are indeed highly active. At Oxford University, two groups, the Jenner Institute and the Vaccine group are working with the pharmaceutical company Astra Zeneca to develop a vaccine now named AZD1222, and in Imperial College, London trial vaccines have already been tried. In the U.S. a number of groups are working on a vaccine, Moderna, Mass, Pfizer and BioNTech, and Johnson and Johnson.

The newly revealed reports about Russia are that those drug firms and research groups involved in developing a coronavirus vaccine are being targeted by APT29, (advanced persistent threats), Russian state sponsored hackers, also known as the Dukes or Cozy Bear. There is a coordinated campaign of cyber attacks. This group, Cozy Bear, has been linked to interference in the U.S. election in 2016. Researchers at Kaspersky lab, controlled by the Russian FSB spy group, in 2015 with sophisticated networks hacked the U.S. State Department and White House networks. It uses various methods, including “phishing” emails and malware. Known as WellMess and WellMail, APT29 acts to find weaknesses and to target governments, think tanks, health care facilities, and the energy sector. It attempts to download files or plant viruses. It uses “phishing,” sending emails that the recipient thinks come from a trusted source. More specifically, it uses “Spear phishing” aiming at tricking a particular individual, often using some personal information about the person, to make it

appear more convincing. It collects “stolen credentials” to use later.

The report of July 15, 2020 makes it unmistakably clear that throughout 2020 the Russian APT29 targeted various organizations involved in Covid-19 vaccine development in Canada, the UK and U.S. through cyber raids on companies and universities involved in research on the virus vaccine in order to steal information and intellectual property relating to the development and testing of Covid-19 vaccines.

The race to develop a successful vaccine is moving rapidly. No doubt the first to develop one will gain priority and intellectual prestige as well as benefit commercially. What a pity that this vital intellectual and scientific activity is not proceeding as a world-wide communal activity, rather than one impaired by Russian malfeasance.