Spies and Disinformation

by Michael Curtis

Alec Guiness as John LeCarré’s cold warrior George Smiley

Please put on some speed and have someone watch over new technological developments. Almost 170 years ago in the 1840s, Countess Ada Lovelace, daughter of Lord Byron, and brilliant mathematician, pioneered and worked on a mechnical general purpose computer, considered to be the first computer program, invented even before computers existed. She died young, aged 36, but her influence is immense. She is a foremost role model for women in science, technology, engineering, and mathematics. Equally important, she inspired both computer pioneers, especially Alan Turing, considered to be the father of theoretical computer science and artifical intelligence, who helped break the Nazi ciphers code in World War II.

One of the tributes to Lovelace is that the computer language “Ada,”created in 1979 on behalf of the U.S. Department of Defense was named after her. Lovelace may well have understood the astonishing potential for computers and their impact on our lives. Yet, she might have been surprised by the revelations in recent weeks of the use made by Russians in using various devices, software control through computers,

iPad, or smart phone, and cyberware to gain information and disseminate false information, fake news, to sow dissent. So called BlackEnergy Malware is said to have been used by Russian cyber espionage groups in Ukraine to target power facilities and other utilities, and complex industrial operations.

That interference probably had little or no impact on or changed few votes in the 2016 presidential election nor does it suggest evidence of any Trump-Russian "collusion." But convincing revelations have been presented of the great extent of Russian attemps to gather intelligence and influence opinion in the U.S., as elsewhere, not so much by human individual spies or agents as by other virtual methods, especially social media.

Of course spies and use of other methods for information or disinformation are not new. In World War II various unusual devices were used to obtain information, ravens to deposit and retrieve objects, pidgeons to warn of the enemy, cats with electronic transmitters to eavesdrop on conversations.

Intelligence gathering and subterfuges are familiar in history. The Greeks used the Trojan Horse to enter and destroy the city of Troy and win the 10 year old war. Today, "Trojan warfare" infects computers, collecting information or making changes in a security system, and has been inserted in the U.S. by hackers probably sponsored by Russian sources.

Collecting information is familiar in the Bible. *Numbers* :13 reports that Moses sent 12 spies, one from each Hebrew tribe, from Acacia to scout for 40 days the land of Canaan, especially Jericho. Ten of them thought that the area was a land of milk and honey, but that the cities were large and fortified, and the people there were strong, and so they advised against advance. But two, Joshua and Caleb, were more positive, and insisted "We should go up and take possession of the land." And as Louis Armstrong sang to us, "Joshua fought

the battle of Jericho, and the walls came tumbling down."

Gathering intelligence and spying started early in the U.S, when the Second Continental Congress in 1775 set up the Committee of Secret Correspondence to attract foreign support for the American revolutionary cause. The Committee, in which Benjamin Franklin was the most active member, employed secret agents abroad to gain intelligence and conduct undercover operations.

Russian spying and attempts at disinformation are not new , but what is new is the sophistication and extent of the devices now employed.

Starting in the late 1920s , the Soviet Union used Russian and foreign born nationals, and U.S. and European citizens to transmit information of political, military, and industrial nature. It is sufficient to mention a few Americans who acted on behalf of the SU or were used by it: Earl Browder, General Secretary of the U.S. Communist party , the group controlled by J.Peters who recruited agents, the "Ware group," Alger Hiss, assistant Secretary of State, Harry Dexter White, assistant Secretary of the Treasury, Elizabeth Bentley, Julius Rosenberg executed, together with his wife Ethel, in 1953 for giving nuclear secrets, not to mention others who had infiltrated the U.S. atom bomb project.

Similarly in Britain, the Soviet Union began in the 1930s recruiting communist sympathizers, bright graduates from elite universities. The most notorious were the Cambridge Five, Kim Philby, Guy Burgess, Donald Maclean, John Cairncross, and Anthony Blunt, a leading art historian and Surveyor of the Queen's Pictures who confessed to being a Soviet spy.

A rather enticing and infriguing story has in February 2018 been published with allegations about Jeremy Corbyn, Labour Party MP for Islington in London since 1983, and now leader of the Labour Party, who met in 1986 and 1987 on at least three

occasions with Czech Communist “diplomats”, agents, part of the Soviet bloc. The question being currently asked is whether Corbyn was any kind of informer, or simply naive and innocent in what John Le Carre has called “a cause the world barely remembers.” Corbyn, given a code name COB, was regarded by the Czech spies as a “person of interest,” and was contacted by the Czech secret police that was dissolved in 1990 after the Soviet Union ended as did the Czechoslovak Socialist Republic, a satellite state of the Soviet Union.

Spies are still used, even if not as glamous and notorious as Mata Hari, the Dutch exotic dancer, executed in 1917 as a spy for Germany in World War I, but new technology has replaced the once simple spying devices, invisible ink, secret codes, blind drops on park benches or in hollow trees. They have been replaced by sophistication, doctored images, falsehoods posted on social media, documents intended to divide and sow discord and confusion among Americans, invention of fake personalities, use of Bots, software application that performs an automated task over the Internet, “troll farms,” state sponsored commentators who post deliberately inflamatory or provocative comments.

Noticable in all this were fake impersonations such as Black Lives Matter activists and white supremists, fake news, conspiracy theories, hacker attacks, dissemination of disinformation disguised as educational or scientific reports, activism in political blogs, participation in staged political rallies, posing as U.S. activists.

Detection of these activities is obviously difficult. Evidence now available illustrates the role of the Russian organization, the Internet Research Agency. This agency, employing 100 persons, and bankrolled by the shadowy figure , the 56 year old Vevgeny Prigoizhin, former small time criminal, hot dog street vendr, now restaurant and catering businessman known as “Putin’s chef,” has played a major role as an arm of Russian foreign policy, including financing a

Russian “troll factory.” IRA instructed its workers in the use of graphics and videos, employing people with coding and social media skills, and some English, to create fake personalities among other tasks. One of those tasks was a false video of an African-American woman being killed by white police officer in Georgia.

A formidable task is ahead for the U.S. institutions, governmental and private. Official governmental bodies are concerned with protection of national security and the public interest to overcome the foreign targeting of groups, by demography, geography, gender, and political points of view. Perhaps an even greater role must now be played by private US organizations.

No one favours censorship or silencing of dissent, but it is wise to recognize that the Internet is now a dangerous place used for improper purposes including organizing rallies, protests, and even distribution of bank cards and money transfers. Major companies, Facebook with its 2 billon users, Twitter, and Alphabet’s you tube are relucant to remove material, even if they contain falsehoods. They confine themselves mainly to those materisls promoting hate speech or child pornography. However, they must do more, to vet their sites more carefully, to limit the use of propaganda tools, to prevent any financing by foreign interests, and to be held more accountable to prevent foreign disinformtion campaigns.