Personal Freedom versus Stone Ghost

In recent years we have witnessed a series of cyberattacks perpetrated against both private and public institutions throughout North-America. Words like "cyberattack," "hacker," "ransomware," and "malware" have entered our everyday lexicon to the point of becoming almost banal. However, from the point of view of Western-style democratic states like Canada, these cyberattacks appear very serious when they threaten our national security. In the case of the U.S.A., I have already dealt with some of the categories of protected data under the heading of "national security" in my earlier essay *On American Power and Politics (Part II)*, published in this same website.

In this essay, I will try to deal with the radical transformation of the meaning of **personal freedom** as it relates to state power in an age of one singular, paramount and all-pervasive information and communications medium. To quote the United Nations website: "The use of algorithms can replicate and even amplify human and systemic bias where they function on the basis of data which is not adequately diverse. Lack of diversity in the technology sector can mean that this challenge is not adequately addressed." [1] Furthermore –as Marshall McLuhan already foresaw in 1964: "The 'message' of any medium or technology is the change of scale or pace or pattern that it introduces into human affairs… All meaning alters with acceleration, because all patterns of personal and political interdependence change with any acceleration of information." [2]

A hundred years ago and earlier, it was a very difficult and dangerous task for an agent of an enemy state to find and copy any top-secret document and then to transmit it to his or her intelligence agency. Decoding encrypted data took days if not weeks; and political decisions as to whether to and how to retaliate were slow and cumbersome. Multiple and diverse technologies were involved: Print, cryptography, invisible ink, mail, photography, telegraphy, telephony, radio, maritime luminous semaphore, etc.; each one requiring a different expertise. Today, on the other hand, because of the singular nature of the I.C.T.'s vehicle, any coder or programmer with some videogaming skills can practice espionage successfully in nano-seconds and not be caught before it's too late to counteract. Here are a couple of recent examples:

Royal Canadian Navy intelligence officer Sub-Lieutenant Jeffrey Delisle pled guilty on October 10th 2012 to charges including having downloaded and sold information from the "Stone Ghost" system to the Russian spy agency GRU. (He had downloaded said data by using a simple USB key.) He was sentenced to 20 years in prison, minus time served, on February 6th 2013, for contravening the *Security of Information Act*. [3]

Jack Teixeira –arrested by the FBI on April 13th 2023, in connection with a massive U.S. classified documents leak– was charged with unauthorized retention and transmission of national defense information, as well as unauthorized removal of classified information and defense materials. The 21-year-old suspect, a member of the Massachusetts Air National Guard, was responsible for posting a trove of highly classified documents to a social media platform popular with video gamers. [4]

The most notorious case is that of Julian Assange –an Australian activist and founder of *WikiLeaks*– who came to wide international attention in 2010 when *WikiLeaks* published a series of leaks from U.S. Army intelligence analyst Chelsea Manning, such as footage of a U.S. airstrike in Baghdad, U.S. military logs from the Afghanistan and Iraq wars, and U.S. diplomatic cables. In 2019 and 2020, the U.S. government indicted Assange, charging him with violating the Espionage Act of 1917. Assange has been incarcerated in H.M. Belmarsh Prison in London since April 2019, while the U.S. government's extradition effort is contested in the British courts. [5]

In Western-style democracies like ours, the concept of individual freedom is considered fundamental and inviolable, and is enshrined in our constitutions and human rights charters. Therefore, when empowered with the new I.C.T.'s, any curious person feels naturally entitled to explore, reveal and share any digital data, no matter how secret or forbidden they are proclaimed to be. However, these same states have civil and military intelligence agencies where other persons are entrusted with ensuring that top-secret and classified data are never revealed to the general public. And as we saw in the case of Assange, these interdictions are based on laws in most cases enacted more than 100 years ago, before the I.C.T. Revolution.

It seems unnecessary to add that espionage and draconian laws enforcing the exclusive right of certain empowered persons to restrict access to "sensitive" information have existed for millennia as far back as the pharaohs. That being said –and without herein condoning in any way the actions of the four individuals cited above– it seems clear to me that a great power differential exists between two kinds of persons: ordinary curious citizens and those few secret persons who hold the keys to "Intelligence" and "Classified" Data.

As George Orwell wrote in *Animal House*: "All animals are equal, but some are more equal than others."

Written by © Pascual Delgado, May 2nd 2024.

[1] https://www.un.org/en/un75/impact-digital-technologies

[2] Marshall McLuhan, *Understanding Media: The Extensions of Man.* (1964). pp. 8 & 178-179

[3] https://nationalpost.com/news/canada/canadian-navy-spy-sentenced-to-20-years-for-selling-secrets-to-russia and https://en.wikipedia.org/wiki/Stone_Ghost

[4] https://www.cnn.com/2023/04/10/politics/classified-documents-leak-explainer/index.html

[5] https://en.wikipedia.org/wiki/Julian_Assange