sciencespo.aix

EXAMEN D'ENTREE EN DEUXIEME ANNEE 2022

Epreuve de Langue (durée conseillée 1h30)

ANGLAIS

The Economist, 7 August 2021

THE GREAT hope of the 1990s and 2000s was that the internet would be a force for openness and freedom. As Stewart Brand, a pioneer of online communities, put it: "Information wants to be free, because the cost of getting it out is getting lower and lower all the time." It was not to be. Bad information often drove out good. Authoritarian states co-opted the technologies that were supposed to loosen their grip. Information was wielded as a weapon of war. Amid this disappointment one development offers cause for fresh hope: the emerging era of open-source intelligence (OSINT).

New sensors, from humdrum dashboard cameras to satellites that can see across the electromagnetic spectrum, are examining the planet and its people as never before. The information they collect is becoming cheaper. Satellite images cost several thousand dollars 20 years ago, today they are often provided free and are of incomparably higher quality. A photograph of any spot on Earth, of a stricken tanker or the routes taken by joggers in a city is available with a few clicks.

Human Rights Watch has analysed satellite imagery to document ethnic cleansing in Myanmar. Nanosatellites tag the automatic identification system of vessels that are fishing illegally. Amateur sleuths have helped Europol, the European Union's policing agency, investigate child sexual exploitation by identifying geographical clues in the background of photographs. Even hedge funds routinely track the movements of company executives in private jets, monitored by a web of amateurs around the world, to predict mergers and acquisitions.

OSINT thus bolsters civil society, strengthens law enforcement and makes markets more efficient. It can also humble some of the world's most powerful countries.

In the face of vehement denials from the Kremlin, Bellingcat, an investigative group, meticulously demonstrated Russia's role in the downing of Malaysian Airlines Flight MH17 over Ukraine in 2014, using little more than a handful of photographs, satellite images and elementary geometry. It went on to identify the Russian agents who attempted to assassinate Sergei Skripal, a former Russian spy, in England in 2018. Amateur analysts and journalists used OSINT to piece together the full extent of Uyghur internment camps in Xinjiang. In recent weeks researchers poring over satellite imagery have spotted China constructing hundreds of nuclear-missile silos in the desert.

Such an emancipation of information promises to have profound effects. The decentralised and egalitarian nature of OSINT erodes the power of traditional arbiters of truth and falsehood, in particular governments and their spies and soldiers. For those like this newspaper who believe that secrecy can too easily be abused by people in power, OSINT is welcome.

The likelihood that the truth will be uncovered raises the cost of wrongdoing for governments. Although OSINT might not prevent Russia from invading Ukraine or China from building its gulag, it exposes the flimsiness of their lies. Eliot Higgins, Bellingcat's founder, is right when he describes his organisation as "an intelligence agency for the people". No wonder that Russia's spy chief railed against it, most recently just this month.

Liberal democracies will also be kept more honest. Citizens will no longer have to take their governments on trust. News outlets will have new ways of holding them to account. Today's open sources and methods would have shone a brighter light on the Bush administration's accusation in 2003 that Iraq was developing chemical, biological and nuclear weapons. That would have subjected America's invasion of the country to greater scrutiny. It might even have prevented it.

Some will warn that OSINT threatens national security—as when, for example, researchers use data from fitness trackers to reveal remote CIA outposts and radar satellites to locate American missile-defence systems. But, if OSINT can tell the

world about such things, a country's enemies are already able to know them. Pretending otherwise does not make states any safer.

Others will point out that OSINT can be wrong. After the Boston Marathon bombing in 2013 internet users scrutinised the crime scene and identified several suspects. All were innocent bystanders. Or OSINT could be used by bad actors to spread misinformation and conspiracy theories.

However, every source of information is fallible and the scrutiny of imagery and data is more empirical than most of them. Hence, when OSINT is mistaken or malign, competing OSINT is often the best way to put the record straight. And over time, researchers and investigators can build a reputation for honesty, sound analysis and good judgment, making it easier for people to distinguish trustworthy sources of intelligence from charlatans.

The greatest worry is that the explosion of data behind open-source investigations also threatens individual privacy. The data generated by phones and sold by brokers let Bellingcat identify the Russian spies who last year poisoned Alexei Navalny, an opposition leader. Similar data were exploited to pick out a senior Catholic priest in America, who resigned last month after his location was linked to his use of Grindr, a gay dating app.

The privacy of individuals in a digital age is fraught with trade-offs. At the level of states and organisations, however, OSINT promises to be a force for good. It is also unstoppable. Before the invasion of Afghanistan in 2001, America's government was able to buy up virtually all the relevant commercial satellite imagery. Today too much data is available for that to be possible. A world where many American, European, Chinese and Russian satellite companies vie to sell images is one of mutually assured surveillance. This is a future that open societies would be wise to embrace. Tools and communities that can unearth missile silos and unveil spies will make the world less mysterious and a little less dangerous. Information still wants to be free—and OSINT is on a mission to liberate it.

I. Comprehension. Answer the questions. /8

1. Which title suits best? **1 point**.

   a. Open-source intelligence is a dangerous tool.
   b. The promise of open-source intelligence.
   c. How to become private detectives in an ever-changing world.
   d. Authoritarian countries' increasing use of open-source intelligence.

2. **Right or wrong?** Write 30 words **maximum** for each question. Please do not quote from the text, use your own words.

   a. According to the journalist, OSINT discloses contradictory information that harms the truth. **2 points**.

   b. According to the journalist, OSINT endangers national security and democracy. **2 points**.

   c. The text says that competition between OSINT sources is positive. **1 point**.

3. "*The privacy of individuals in a digital age is fraught with trade-offs*". Explain. 40 words maximum. **2 points.**

II. **ESSAY.** What information source do you trust the most? OSINT or the mainstream media? Why? 300 words (+/- 10%) **/12**