



OSINT techniques have been applied for good purposes like helping discern true news from fake ones. There are many examples, so let's focus on Ukraine's invasion by Russia. Like in all conflicts, both countries have tried to steer the rhetoric and achieve the international community's support: in the case of Russia, to gain justification for its invasion, and in the case of Ukraine, to obtain weapons and military equipment. One of the best-known examples where OSINT has been applied is the Bucha massacre. In this town near Kyiv, the Ukrainian army discovered numerous corpses in the streets when they entered the town after Russian troops withdrew on March 31st. In response to the accusation of an intentional civilian massacre, Russian Foreign Minister Sergei Lavrov claimed that the videos released from Bucha were "staged" and that the alleged dead bodies were actors. OSINT investigations with analyses of satellite images from before the withdrawal of Russian forces have verified that the position of the bodies in these images is the same as in the videos released by the Ukrainians once they were able to re-enter Bucha. This kind of OSINT verification in real-time has provided a more accurate measure of the horrors that occurred in Ukraine, which in turn has led to great political pressure for Western governments to punish Russia and arm Ukraine.

Nevertheless, there is a dark side to OSINT as well: anything that an open source analyst can find can also be found (and used) by criminals. An example of this can be seen in the rise of the so-called "CEO fraud", a type of phishing scheme that, although it cannot be considered "open source", benefits a great deal from OSINT data. In this form of cybercrime, employees are tricked into paying an invoice or making a money transfer from the company's account to that of the criminal following the instructions of an email supposedly sent by the CEO or another high-ranking director. For these attacks, the scammers usually gather as much information as possible from the company –in general– and the target –in particular– to get a good understanding of how the company operates and to make their messages as credible as possible. We tend to think that phishing emails are quite obvious and that we will surely not be caught falling for them, but, as data shows, that is not so true. In Spain alone, 94% of companies suffered at least one serious cybersecurity incident in 2021, and the great majority also confirmed at least one successful phishing attack. The more information the attacker has about you, the more personalised the scam email will be and the more likely you are to fall for it.

Once OSINT has been explained, one thing must be made clear: open source intelligence is just that, a process by which OSINT information is analysed to create useful and actionable knowledge. It should therefore not be associated with hacking, physical and cyber security testing, covert operations, or any other security-related offerings. Having said that, when OSINT is applied to security issues, as with other kinds of investigations, ethical questions may arise. Am I violating this entity's right to privacy? I can do this technique... But should I? With the never-ending flow of information available at a click, it can be tempting to test one's own limits, and consequently one's ethical boundaries. Therefore, an important issue to always have in mind is to be aware of what is legal and what is not in the jurisdiction to which you are subject. OSINT can be extremely powerful when used effectively and ethically. When conducting research, the following questions should be considered: what is the purpose of the research? Can the information be obtained in a more ethical way? What are the consequences of obtaining this information? Regarding OSINT, I find myself in the position to use a quote that is so very trite and cliché, but sadly, also true: "With great power comes great responsibility."