**The Value of Open Source Intelligence (OSINT)**

*After the January 6, 2021 Assault on our Capital Building, a powerful new force emerged that served to collect data to support law enforcement*

The January 6, 2021 assault on our Capital building was covered on national television which provided a broad view of some portions of the national event. This being the age of cell phones and amateur photographers and video amateurs, hundreds of images, still and video, were captured, mostly for personal recording. Others believed they were capturing bits and parts of a major historical event.

The plethora of images from multiple angles captured by curious citizens, provided an extremely detailed history of the activities on that ominous day. Those images included the killer(s) and victims killed by firearms, and others, including serious harm. The homicide of Capitol Police officers, were filmed for posterity. This recent development of open source data collection is known as **Crowdsourcing**. It is not a new phenomena, but has turned into a hot phenomena, as camera technology, especially cell phone cameras with high quality lenses are recording crimes in progress. Many people can now capture images/videos in high definition that are useful to the government.

The video recording of crime in progress was the domain of the police and government agencies, including intelligence and counter-intelligence agencies. When criminal acts are captured as the crime occurs, criminals cannot deny their presence at the scene of a crime. Often the criminal act is caught on film. That's marvelous!

The ubiquitous cell phone has change history and today, the public is provided access, to all types of events from birthday parties to criminal activities ranging from robberies to homicides (and many other events, including police brutality.) These moments in history, captured on camera, sometime in real time, can send either a policeman or criminal to jail.

This 21st Century phenomenon, is having earthshaking impact on modern history. For instance:

Hundreds of videos were filmed by hundreds of cell phones. Were it not for these thousands of videos and photos, most of the insurgents would have never been identified and prosecuted. According to the FBI, the received 12,000 pages of digital evidence to identify and investigate more than 550 rioters active on January 6, 2021. Facial recognition technology was very useful in identifying many of the culprits.

As Congress investigates the January 6, 2021 event, those who chose to deny that anything unusual took place when our Capital was assaulted will have little credibility and their motives questioned.

Without the credible evidence captured in digital format, deniers of the event would be able to cast a shadow of doubt that those who attacked our Capital were just tourists visiting and welcomed by the Capital police. Without all those cameras, hundreds of insurrectionists would have never been identified and prosecuted for attacking our democracy.

**=======================================================SOURCE:**

[***https://www.foreignaffairs.com/reviews/review-essay/2021-06-22/spies-us?amp***](https://www.foreignaffairs.com/reviews/review-essay/2021-06-22/spies-us?amp)

**Spies Like Us**

*The Promise and Peril of Crowdsourced Intelligence*

**By Amy Zegart, Foreign Affairs, July/August 2021**

On January 6, throngs of supporters of U.S. President Donald Trump rampaged through the U.S. Capitol in an attempt to derail Congress’s certification of the 2020 presidential election results. The mob threatened lawmakers, destroyed property, and injured more than 100 police officers; five people, including one officer, died in circumstances surrounding the assault. It was the first attack on the Capitol since the War of 1812 and the first violent transfer of presidential power in American history.

Only a handful of the rioters were arrested immediately. Most simply left the Capitol complex and disappeared into the streets of Washington. But they did not get away for long. It turns out that the insurrectionists were fond of taking selfies. Many of them posted photos and videos documenting their role in the assault on Facebook, Instagram, Parler, and other social media platforms. Some even earned money live-streaming the event and chatting with extremist fans on a site called DLive.

**Amateur sleuths immediately took to Twitter, self-organizing to help law enforcement agencies identify and charge the rioters. Their investigation was impromptu, not orchestrated, and open to anyone, not just experts**. Participants didn’t need a badge or a security clearance—just an Internet connection. Within hours, this crowd-sourcing effort had collected hundreds of videos and photographs before rioters could delete them or social media platforms started taking them down. Beyond merely gathering evidence, citizen detectives began identifying perpetrators, often by zeroing in on distinctive features captured in images, such as tattoos or unusual insignias on clothing. Soon, law enforcement agencies were openly requesting more online assistance. By March, the volunteer community of amateur investigators had sent some 270,000 digital tips to the FBI; hundreds of suspects have now been arrested and charged.

This is the **emerging world of open-source intelligence**. Tracking criminals at home and adversaries abroad used to be the province of governments, which enjoyed a near monopoly over the collection and analysis of essential information. In the old days, law enforcement agencies had special access to data used for identifying perpetrators—such as fingerprint records—that ordinary citizens did not. Intelligence agencies had unique data, too; they were the only organizations with the resources and know-how necessary to launch billion-dollar satellites and collect information at scale. Publicly available information mattered, but information residing in government agencies mattered more.

Not anymore. Today, new technologies are enabling nonstate actors and individuals to collect and analyze intelligence, too—sometimes more easily, more quickly, and better than governments. Commercial firms are launching hundreds of satellites each year, offering low-cost eyes in the sky for anyone who wants them. More people on earth have cell phones than have running water, enabling them to post what they are seeing in real time from anywhere. More than half the world is online, producing and acquiring open-source intelligence even if they don’t know it. According to a 2019 World Economic Forum report, Internet users post some 500 million tweets to Twitter and 350 million photos to Facebook every day.

Bellingcat is a key member of this new open-source intelligence ecosystem. Formally founded in 2014, Bellingcat eludes easy definition. It conducts activities traditionally performed by a wide variety of players, including journalists, activists, hobbyists, and law enforcement agencies. Led by Eliot Higgins and a small staff, Bellingcat draws on the work of thousands of volunteers from around the world, united by a shared passion for using openly available information to investigate crimes, battle disinformation, and reveal wrongdoing. The group’s name was inspired by a fable about a cat that terrorizes a group of mice. The mice are faster than the cat, but they realize they cannot protect themselves unless they hear the cat coming. Their solution: find a brave mouse to hang a bell on the cat’s neck. Higgins sees his mission as “belling” the cats of global injustice. He calls his organization “an intelligence agency for the people,” an “open community of amateurs on a collaborative hunt for evidence.”

In We Are Bellingcat, Higgins traces his improbable journey from college dropout and video-game player to open-source intelligence pioneer. After the 9/11 terrorist attacks, in 2001, Higgins, a British citizen then in his 20s, was struck by the slowness of traditional media. “News was happening so fast,” he writes, “and the papers were so slow.” He became obsessed with current affairs and started joining online message boards. By 2011, when the Arab Spring protests were erupting across the Middle East, Higgins was arriving early to his office job to scour the Internet for news. It was then that he had a realization: reporters were often posting more information in their personal Twitter feeds than in their published stories; social media had facts that traditional media did not.

Higgins eventually moved from consuming information to producing it, posting comments on the Something Awful message board and The Guardian’s live blog, then creating his own blog under the handle Brown Moses, after the Frank Zappa song of the same name. His self-described forte was using Google Earth to determine the locations of events and identifying unusual weaponry he found in photos. Imagery, he discovered, could be a gold mine in the hands of a careful investigator. Photographs often contained telltale clues—a distant road sign, a certain type of tree, a time of day, a specific kind of munition—that the subjects and photographers themselves didn’t realize were present. “What people mean to show is not all they are revealing,” writes Higgins.

Bellingcat is best known for investigating the shootdown of Malaysia Airlines Flight 17, which crashed in Ukraine in 2014, killing all 298 people onboard. The Russian government insisted that Ukrainians were behind the tragedy and launched disinformation campaigns to spread false narratives and sow confusion. Bellingcat uncovered the truth: the plane was shot down by a Russian Buk surface-to-air missile supplied by Russian special operations forces to pro-Russian separatists in Ukraine, who likely mistook the civilian airliner for a Ukrainian military plane. The amateur investigators at Bellingcat found all sorts of ingenious sources to piece together the Buk missile’s secret transport from Russia to Ukraine. They used pictures and videos of separatist military hardware that Ukrainians liked to post on social media; dashboard camera footage of daily drives in the region, which car owners posted on YouTube (a popular local hobby); an app called SunCalc, which measures shadows in pictures to pinpoint the time of day of an image; and Instagram selfies of a Russian undercover soldier posing at the border. Bellingcat’s volunteers identified the specific Russian military unit and individuals involved. They even pinpointed the exact weapon that shot down the plane by tracking photos of its transport and identifying the unique pattern of bumps and tears that appeared on a rubber part of the Buk transporter’s exterior.

Bellingcat has notched many other successes: unearthing and compiling overwhelming evidence that Syrian President Bashar al-Assad used chemical weapons against his own citizens; identifying neo-Nazis involved in violent protests in Charlottesville, Virginia, in 2017; and unmasking members of a Russian hit team that in 2018 tried to assassinate a former Russian military officer who had spied for the British and was living in the United Kingdom. In one case, Bellingcat investigators identified someone photographed assaulting an African American man in Charlottesville by examining social media photos of white nationalist rallies held in the summer (when it was hot and people tended to open their shirts) and matching the distinctive pattern of moles at the top of the suspect’s chest. In another case, Higgins saw a late-night video tweeted by a Syrian activist, Sami al-Hamwi, that showed a man picking through strange turquoise canisters on the ground in Syria. “Anyone know what this weird [bomb] is?” Hamwi asked. Higgins found another video from the same area showing a split shell that had fins and a distinctive shape. Another amateur sleuth sketched it and posted the drawing so people could more easily hunt for matches at specialty weapons sites online. Eventually, Higgins concluded that the videos showed parts of a Russian-made RBK-250-275 cluster bomb, a widely denounced munition that releases bomblets that often fail to explode, posing risks for civilians (including children) who later find them. The turquoise canisters the man was picking through on the video were live bombs.

This track record has brought Bellingcat a level of attention and renown that Higgins scarcely could have imagined when he started the project; the once obscure blogger now sits on the Technology Advisory Board of the International Criminal Court. He recounts this unlikely tale with fascinating detail and fervor, making We Are Bellingcat a mix of memoir, manifesto, and police procedural: CSI for the international relations set.

**WISE CROWDS, DANGEROUS MOBS**

Perhaps unsurprisingly, We Are Bellingcat gives a glass-half-full view of open-source intelligence, focusing almost entirely on its promise and glossing over its potential risks. But the downsides are important to consider.

Bellingcat is part of an eclectic, expanding ecosystem that is home to a wide range of inhabitants with varying motives and capabilities. There are hobbyists, journalists, activists, academics, part-timers, profiteers, volunteers, fact checkers, conspiracy peddlers, and everything in between. Higgins’s outfit is one of the most capable and responsible members of this emerging world, with high standards for verification and a commitment to training. Those values are shared by a number of academic experts and former government officials who also conduct valuable open-source intelligence work. But open-source intelligence is a loose, unregulated field, open to anyone: there are no formal qualifications, rules, or standards. Operating online means that errors can go viral. And participants don’t risk losing a promotion or a job for making a mistake. Higgins disdains the hierarchy and bureaucracy of government intelligence agencies, but red tape has some benefits: the best intelligence agencies insist on rigorous hiring standards and procedures, formalized analytic training, mandatory peer review of intelligence products, and penalties for poor performance.

Higgins is also passionate about the benefits of crowdsourcing to find the truth. But a thin line separates the wisdom of crowds from the danger of mobs. The herd is often wrong—and when it is, the costs can be high. After two terrorists detonated explosives near the finish line of the Boston Marathon in 2013, killing three people and wounding more than 260, users of the online forum Reddit who were eager to crack the case identified several “suspects” who turned out to be innocent; the crowdsourced investigation quickly devolved into a digital witch-hunt.

Recent research has found that facial recognition algorithms—which are widely available and easy to use online—are far more accurate at identifying lighter-skinned faces than darker-skinned ones, increasing the risks that amateur sleuths, as well as government agencies, could wrongfully charge the innocent. That is exactly what happened to Robert Julian-Borchak Williams in 2020, an African American man who is the first known person in the United States to be charged with a crime he did not commit because his face was erroneously identified by a faulty facial recognition algorithm. After the January 6 siege of the U.S. Capitol, an anonymous Washington-area college student used imagery posted online and simple facial detection software to create Faces of the Riot, a website with 6,000 photographs of people believed to have been involved in the attack. “Everybody participating in this violence, [which] really amounts to an insurrection, should be held accountable,” said the student. But Faces of the Riot did not distinguish between people who broke into the Capitol complex and those who only attended protests outside it. Nor did the site’s image dump identify or remove mere bystanders, members of the press, or police officers.

Flawed open-source investigations can also lead intelligence officials and policymakers astray, sapping resources from other missions and priorities. In 2008, a former Pentagon strategist named Phillip Karber was teaching a class at Georgetown University when he decided to guide his students on an open-source intelligence investigation to uncover the purpose of a massive underground tunnel system in China. The existence of the tunnels had been known for years, but their use remained uncertain. Karber’s student sleuths produced a 363-page report that concluded that the tunnels were secretly hiding 3,000 nuclear weapons—which would have meant that China possessed a nuclear arsenal around ten times as large as what most experts and U.S. intelligence agencies believed, according to declassified estimates.

Experts judged that the report was flat wrong and found the analysis to be riddled with egregious errors. Among them, it relied heavily on an anonymous 1995 post to an Internet forum—a source that was “so wildly incompetent as to invite laughter,” wrote the nonproliferation expert Jeffrey Lewis. Nevertheless, the report was featured in a Washington Post article, was circulated among top Pentagon officials, and led to a congressional hearing. It was all a wild-goose chase that consumed the most valuable resource in Washington: time. As open-source intelligence grows, such distractions are likely to proliferate. Increasingly, U.S. intelligence agencies may have to serve as verifiers of last resort, debunking crowdsourced claims that make headlines instead of giving policymakers the intelligence they need.

Tracking criminals at home and adversaries abroad used to be the province of governments. Not anymore.

Open-source intelligence investigations also tend to focus on details to illuminate the big picture. In Higgins’s view, truth is truth, small things add up, and everyone knows it. This approach is seductive but riskier than it sounds. Intelligence is a murky business in which individual facts often support many competing hypotheses. In 1990, for example, U.S. satellite imagery clearly showed Iraqi forces mobilizing near the Kuwaiti border. But nobody knew whether the Iraqi leader Saddam Hussein was bluffing to gain leverage in his dispute with the Kuwaitis or whether he was really preparing to invade. The facts were obvious, but Saddam’s intentions were not.

Small truths can also lead to big distortions. Humans often place too much weight on information that confirms their views and too little weight on information that contradicts them. U.S. General Douglas MacArthur was blindsided by China’s entry into the Korean War mostly because he was convinced that the Chinese leader Mao Zedong wouldn’t dare join the fight; MacArthur put stock in intelligence that supported that belief and discounted anything that challenged it. Asking the wrong question can also produce information that is narrowly accurate yet highly misleading. Michael Hayden highlighted this danger during his 2006 confirmation hearing to serve as CIA director. “I have three great kids,” Hayden told the Senate Intelligence Committee, “but if you tell me to go out and find all the bad things they’ve done, . . . I can build you a pretty good dossier, and you’d think they were pretty bad people, because that was what I was looking for and that’s what I’d build up.” Truths can deceive even when nobody intends it. "

**WIDE OPEN**

The revolution in open-source intelligence is here to stay, and U.S. intelligence agencies must embrace it or risk failure. Innovators such as Bellingcat are harnessing publicly available information with new technologies in exciting ways. But like anything in intelligence, this emerging landscape holds both promise and pitfalls.

Maximizing the benefits and mitigating the risks of this open-source world requires action on three fronts. First, governments and nongovernmental actors need to develop closer partnerships to make it easier to collaborate and share open-source intelligence. Meanwhile, governments need to create intelligence agencies dedicated to open-source collection and analysis, which remains a peripheral activity in most intelligence bureaucracies. In the United States, the CIA, the National Security Agency, and other intelligence agencies have promising open-source initiatives underway. But these will not be enough: a new open-source intelligence agency is needed. Secret agencies will always favor secrets. Just as the U.S. Air Force was hobbled until it split from the army, open-source intelligence will remain underfunded, underpowered, and underutilized as long as it sits inside agencies whose missions, cultures, and capabilities are all designed for a classified world.

Finally, **nongovernmental open-source groups such as Bellingcat have work to do**. The ecosystem as a whole needs to codify and institutionalize best practices, create shared ethical norms, establish quality standards, and improve collection and analysis skills to reduce the risk of errors and other bad outcomes. Here, too, efforts are underway. Bellingcat is running training programs, and the Stanley Center for Peace and Security, a nonprofit, is convening international workshops with leaders in open-source intelligence to examine ethical challenges and develop recommendations for addressing them.

**Today, open-source intelligence is dominated by Americans and the United States’ Western democratic allies**. Many of the leading organizations are filled with experts who are driven by a sense of responsibility, who have exacting quality standards, and who work closely with government officials and international bodies. But the future is likely to bring more players from more countries with less expertise, less sense of responsibility, and less connectivity to U.S. and allied intelligence officials and policymakers. China already operates commercial satellites, and the internationalization of the commercial satellite business is expected to grow significantly in the next several years. The open-source world will soon be more crowded and less benign. Now is the time to prepare

============================================================

[***https://www.msnbc.com/opinion/how-fbi-s-most-wanted-capitol-rioters-are-being-hunted-n1270268***](https://www.msnbc.com/opinion/how-fbi-s-most-wanted-capitol-rioters-are-being-hunted-n1270268)

**How the FBI's most wanted Capitol rioters are being hunted online**

*It's the latest version of the wanted posted of the Wild West — and it's working.*

**June 10, 2021, By Frank Figliuzzi, *MSNBC* Opinion Columnist**

After the terrorist attacks of Sept. 11, 2001, a New York advertising executive conceived of a slogan that was eventually adopted by the newly formed Department of Homeland Security: "See something, say something." It was a plea for hyper-vigilance against another terrorist attack, asking the public to report anything — or anyone — suspicious. The slogan's creator, Allen Kay, told The New York Times that he based the phrase on the World War II mantra "loose lips sink ships," used as a reminder to everyone that speaking about troop or ship movements could have deadly consequences.

After the Jan. 6 Capitol riot, public tips about the identities of the rioters continue to stream into the FBI. They're part of a natural evolution in the average Joe's role in securing our democracy — we've moved from "keep your mouth shut" to "keep your eyes open" to a play-at-home variation of Call of Duty in which everyone can become a virtual bounty hunter. And so far, it's working — with certain caveats.

Five months on from Jan. 6, the authorities have brought charges against more than 400 rioters, often using the traditional tools of law enforcement, such as search warrants and confidential informants. But they’ve also relied on the crowdsourcing efforts of sedition hunters. In the days after the riot, the FBI saw a 750 percent increase in daily calls and electronic tips to its main hotline. The bureau still receives twice the normal volume of alerts. Such tips have proved helpful in “dozens of cases,” says Samantha Shero, an FBI spokeswoman. “The public has provided tremendous assistance to this investigation, and we are asking for continued help to identify other individuals."

This impressive public response wasn't simply spontaneous. It was prompted by the FBI's repeated, daily sharing of digital wanted posters, made up of still images and videos of unidentified participants at the Capitol riot. This unprecedented crowdsourcing of crime solving is the result of three factors.

Deputizing the public for digital detective work isn't without its problems

First, the overall numbers: The FBI's investigation of violence at the Capitol involves several hundreds of suspects who were digitally captured in images and videos from security surveillance, license plate readers, police officer body cameras, facial recognition technology, media coverage and — in a sign of the ubiquitous smartphone — the rioters themselves. In just one suspect's cellphone, the FBI recovered over 12,000 pages of digital evidence. The sheer number of suspects and the daunting amount of evidence to comb through meant the FBI needed the public's help.

Second is the good news part of this story: The concerted public effort to help the investigation reflects a recognition of the threat to democracy posed by those who breached the Capitol. The sentiments expressed by one "sedition hunter" in the Bloomberg piece seem to mirror the motivation of many:

Third, Americans are spending more time than ever before on their devices, even before the pandemic. That's both good news and bad news for investigators. It means people will continue to produce mountains of digital evidence that will have to be painstakingly processed for almost any criminal investigation. But it also means law enforcement will increasingly parlay American's collective online search skills into a mobilized army capable of a nationwide manhunt.

**Federal prosecutors expect to charge 550 in the Capitol riot**

But deputizing the public for digital detective work isn't without its problems. Things can go wrong when even well-meaning people skip the part where they're supposed to report their findings to law enforcement. Misidentifications can lead to wrongful accusations, and exposure of personal information could result in vigilantism and violence — the very thing that sedition hunters are trying to thwart. As described in Bloomberg, "A retired Chicago firefighter was falsely accused of participating in the riot after footage surfaced showing a lookalike hitting police with a fire extinguisher."

I reached out to Chris Sampson, chief of research for TAPSTRI, The Terror Asymmetrics Project on Strategies, Tactics and Radical Ideology, to get his thoughts about the work these digital detectives are performing:

The need for crowdsourced examination of available media from the Capitol insurrectionists is abundantly clear. Online sleuths are certainly contributing positively to the effort. However, there is no room for error in accusing people of a crime. The consequences to innocent people from misidentification are too steep to risk mistakes. It is still best to take available information and send it to legal authorities who have the proper legal power and forensic tools to follow up on those leads. But, we most certainly have found a better than average accuracy and caution in the work of the "sedition hunters" when compared to past efforts at online identification.

As Sampson alluded to, when it comes to an assault on our democracy, an all-hands-on-deck strategy is needed — but everyone needs to be rowing in the same direction. Crowdsourced solutions to crime are as old as the wanted posters in Wild West post offices and as contemporary as Amber Alerts for missing children. Now, instead of cattle rustlers or kidnappers, we're being asked to help identify a different kind of outlaw — the kind who tries to steal our democracy. Those outlaws won't stop their efforts just because some of them have been captured; neither should we.