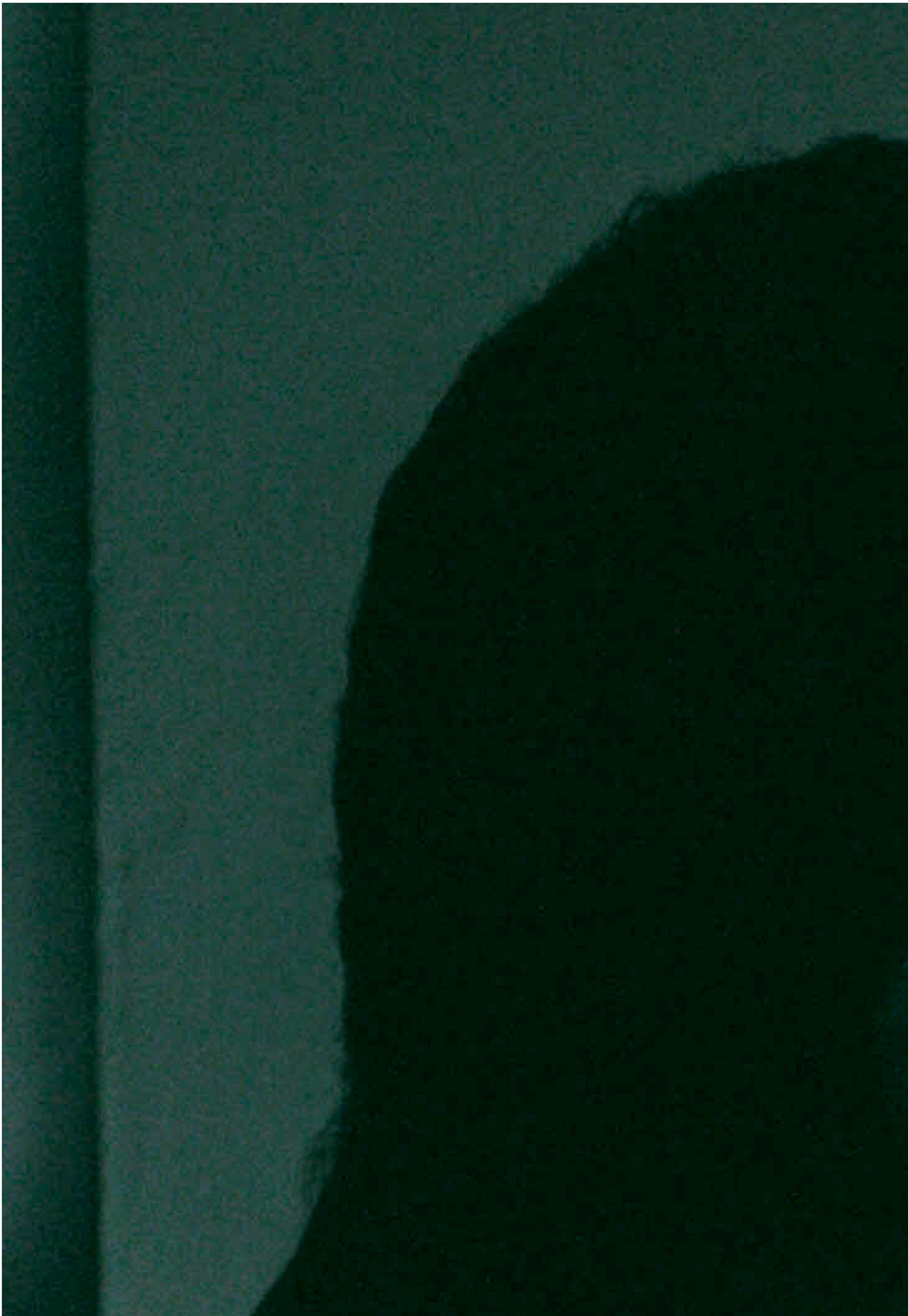
Thumbnail Image:



Mar 05, 2018 by Mark Dillen

Needed: Digital Detectives [1]

The latest news in the probe into Russian interference in the 2016 U.S. election should send an alarm throughout the U.S.—indeed, throughout the world.

U.S. Special Counsel Robert Mueller has found sufficient evidence to indict a Russian troll farm closely tied to Russian President Vladimir Putin for manipulating social media accounts in order to defeat Hillary Clinton's candidacy.

We don't know yet whether this effort was critical to her defeat, but it does raise again the question of what can and should be done to try to prevent such efforts in the future.

So far, it must be noted, there is no indication that the Trump Administration—or even Congress—have responded with anything approaching sufficient determination. (As I write this, the Department of State has just announced the start of an effort to "counter state-sponsored disinformation," but this comes more than a year after getting the mandate to act!)

The Economist, in its latest cover story, trenchantly observes: "In the cold war, America fought Russian misinformation with diplomats and spies. By contrast, Mr. Mueller acted because [Obama and Trump] fell short."

So if Trump won't act and Mueller can only act once laws are broken, maybe for now we need to rely on the private sector.

The first step is to get social media leaders to act. Mark Zuckerberg at Facebook is belatedly promising to reduce their receptivity to bots and other fakery. (Listen to this NYT podcast for a rundown on Facebook's response to Russian meddling on FB.)

The next step might be called, for want of a better term, hybrid journalism. Its practitioners are not always journalists and they often don't work for journalistic organizations. However, they aim to serve the public in the same way that real journalism does: by striving to uncover and disseminate the truth. What they do differently is exploit the new field of digital forensics to sift through enormous amounts of data in pursuit of the story.

Examples of this discipline are out there. One of the first to gain attention several years ago was Bellingcat (www.bellingcat.com), a UK-based group of self-described “citizen journalists” who played a key role in proving the cause of the shoot down of Malaysian Airlines Flight 17 over eastern Ukraine on July 17, 2014. Anyone interested in understanding what happened on that day, when a Russian missile brought down a Boeing 777 carrying 298 passengers and crew, should read Bellingcat’s data-driven analysis. It is a remarkable piece of investigative work, coming as it did entirely from open source information, filling in the gaps in ordinary journalistic accounts. (The ongoing scandal, of course, is that after months and years of official investigations, in particular a full inquiry led by Dutch specialists and international transportation authorities, the Russian government continues to deny any responsibility and vetoed a UN Security Council resolution that would have created a tribunal to bring the guilty to justice.)

The evolution of digital forensics is seen in the more recent effort by the Atlantic Council, a Washington D.C.-based think tank, to study and expose disinformation. The Council’s Digital Forensic Research Lab is trying to expand on the Bellingcat example by establishing a “cross sectoral” network of “digital Sherlocks” that will proliferate the skills and knowledge to effectively counter disinformation. They have already written a number of studies that have been important in unmasking Russian-linked fake news and disinformation campaigns. The Lab’s post from last August, “Twelve Ways to Spot a Bot,” is particularly relevant now that U.S. intelligence community leaders have testified before Congress that Russia’s digital interference in the U.S. political process continues. The Lab will be holding a conference on their work in Berlin June 22-23.

Another sophisticated effort to monitor Russian disinformation in real time—rapid response is critical—is called Hamilton68, a project of the German Marshall Fund of the United States. Their Web dashboard is a clear and user-friendly resource. Their goal, as they put it, is:

> *…to help ordinary people, journalists, and other analysts identify Russian messaging themes and detect active disinformation or attack campaigns as soon as they begin. Exposing these messages will make information consumers more resilient and reduce the effectiveness of Russia’s attempts to influence Americans’ thinking, and deter this activity in the future by making it less effective.*

Other important centers of digital research may help provide ideas for how we move forward—as citizens, journalists and citizen-journalists.

The Tow Center for Digital Journalism at Columbia University, while dealing with all forms of digital journalism, is narrowing the gap between the practice of journalism and the analysis of how social media treat news and current events. George Washington University, too, is home to academic research focusing attention on the misuse of social media by international actors.

These digital detectives working in the public space are critically important in addressing issues that Putin, Trump and their allies are trying to obfuscate, or at least ignore. The takeaway from all this seems to be: if the U.S. government will not move proactively to expose foreign disinformation attacks, then it’s up to journalists, analysts and activists—digital detectives—to do so.

Photo by João Pessoa via Unsplash