**Russian Hackers Find Ready Bullhorns in the Media - The New York Times**

As the dust settles on Russian interference in the United States election, journalists are confronting an aspect that has received less scrutiny than the hacking itself but poses its own thorny questions: Moscows ability to steer Western media coverage by doling out hacked documents. Reporters have always relied on sources who provide critical information for reasons. The duty, tricky but familiar, is to publicize information that serves the public interest without falling prey to the sources agenda. But in this case, the source was Russias military intelligence agency, the G. R. U. ” operating through shadowy fronts who worked to mask that fact ” and its agenda was to undermine the American presidential election. By releasing documents that would tarnish Hillary Clinton and other American political figures, but whose news value compelled coverage, Moscow exploited the very openness that is the basis of a free press. Its tactics have evolved with each such operation, some of which are still unfolding. Thomas Rid, a professor of security studies at Kings College London who is tracking the Russian influence campaign, said it goes well beyond hacking: Its political engineering, social engineering on a strategic level. Great powers have long meddled in one anothers affairs. But Russia, throughout 2016, developed a previously unseen tactic: setting up fronts to seed into the press documents it had obtained by hacking. Doing public relations work in order to get the hacked material out as an exclusive story with the Daily Caller or Gawker or the Smoking Gun, that is new, Mr. Rid said. That public relations work was initially done by two web presences that appeared this summer, Guccifer 2. 0 and DCLeaks, each posing as in the mold of Julian Assange, the WikiLeaks chief. Though neither acknowledged it, and the links were not immediately known, online security experts later concluded that both were Russian fronts. Guccifer 2. 0 claimed to be a Romanian freedom fighter who had hacked the Democratic National Committee. Using Twitters private message service, the account conducted weekslong exchanges with journalists, pointing them to certain documents that had been hacked from the D. N. C. and other targets. Whoever is doing this understands media. They understand the way that media works and how to manipulate media, said Sheera Frenkel, a BuzzFeed News reporter who interacted with the fronts throughout the summer. DCLeaks, established separately and with its own sets of hacked documents, claimed to be launched by the American hacktivists who respect and appreciate freedom of speech. The fronts sold the act by peppering their messages with slang and emojis. When Ms. Frenkel asked Guccifer whether it would release more D. N. C. documents, the reply came, Yeah baby :) Journalists who interacted with the accounts say their tone and facility with English varied widely, suggesting each was run by multiple users. A reporter with Motherboard, a technology site, quizzed Guccifer on the technical aspects of the hacking and on rudimentary Romanian. Guccifer failed both, lending credence to theories that it was a front. Those suspicions were initially restricted to security experts, trickling out only after firms such as ThreatConnect were able to unmask the fronts in detailed reports. In July, for instance, DCLeaks published emails belonging to retired Air Force Gen. Philip Breedlove. The Intercept, a site, covered the emails in a story that portrayed Mr. Breedlove as trying to foment hostility against Russia. The story did not note Russian links to the hack. Its lead author, Lee Fang, said he had no interactions with DCLeaks and pointed out that the groups suspected Russian ties were not widely publicized at that time. Some reporters were offered documents exclusively, a familiar tactic of government press offices and public relations firms that want to shape coverage. In September, DCLeaks contacted Peter Hasson, a reporter at the Daily Caller, a site, with an offer: access to hacked emails belonging to Colin Powell, the former secretary of state. The Daily Callers story also did not note the growing belief that the documents had been hacked by Russia and leaked as part of an influence operation. Mr. Hasson said he was unaware of the alleged Russian links at the time. After awareness grew, the front organizations dropped the pretense. The newest group called itself Fancy Bears Hack Team ” a breathtakingly overt reference to fancy bear, the name that some Western security groups use for G. R. U. hackers. Tom Cheshire, a reporter with the British network Sky News who has dealt with Fancy Bears, said they behaved almost more like a P. R. firm, really and were very businesslike, doling out scoops and trying to shape coverage. Its the sort of horse trading you do with all sorts of sources, really, Mr. Cheshire said, hitting on a key to the operations impact: the way that it played within the bounds of established journalistic norms. Any leak by any source ” Russian agent or citizen ” poses a similar set of quandaries for reporters. Do you emphasize the hacking itself in your coverage, knowing that this will undercut the sources agenda but could also be a disservice to readers by putting less focus on newsworthy information in the release? Do you withhold newsworthy documents, even only temporarily, to check their veracity and provenance? What if they have already been reported by other outlets that were shown the documents first? If they did turn out to be hacked as part of a hostile foreign operation, does that really make their contents less newsworthy? These are old questions for journalists, but they have taken on new urgency with the scale of Russias hackings and aims. Though the calculus of reporting on leaks may be familiar, one aspect of the Russian operation stands out: the lengths to which the fronts go to mask their identities and motives. Because the internet gives any outlet the potential to reach millions, all it takes is one leak to send the document flying across the web. Last year, hackers infiltrated the United States Agency, most likely in retaliation for accusations of doping among Russias Olympic athletes. But Fancy Bears struggled to place the stolen documents with American or British outlets. Reporters who saw the files said their news value did not outweigh the risk of serving Russian interests. When Fancy Bears offered the files to The Associated Press, the reporters instead published a story on the group itself. Fancy Bears ultimately persuaded sportswriters with Spiegel, a prominent German outlet, to report on emails that appeared to show American athletes requesting medical exceptions to take restricted drugs. The article noted a possible Russian link only in the final lines, alongside a quote from an American official arguing that the leak was intended to distract from doping. If mainstream outlets pass on a hacking, fronts can always pass the documents to peripheral outfits who will lend them less weight but can still send them across social media. That has often included the website InfoWars, which was founded by the radio host Alex Jones and often publishes conspiracy theories. Guccifer 2. 0 approached Mikael Thalen, a writer for InfoWars, with D. N. C. documents that showed Democrats plans for attacking Paul Manafort, a campaign manager to Donald J. Trump who had worked on behalf of the Ukrainian president Viktor Yanukovych, a Kremlin ally. Mr. Thalen had come to believe, after many interactions with the front groups, that they would reach out based on who would best carry the story the way they wanted it carried. He feared that Moscow was hoping InfoWars, by publishing the files, would muddy the water around accusations against Mr. Manafort, indirectly aiding Mr. Trumps campaign. Breaking with InfoWars usual reliance on such files, he declined to publish the documents. Because everyone has secrets, even if its only a few embarrassing personal emails, and because no network is impenetrable, skilled hackers can dig up compromising material on virtually any target. Democracies, which give privilege to competitive politics and free media, are particularly susceptible. An open society is by choice more vulnerable than a closed society to some form of influence operation, said Mr. Rid. That is why were strong, but its also why were weak. The more that journalists and readers understand the motivations of foreign government leakers, he argued, the better they will be able to place those leaks in context, undercutting the hackers agenda without hiding newsworthy information. He compared this to a healthy body developing antibodies against a disease ” foreign influence operations ” that cannot be wholly immunized against while maintaining democratic openness. Still, some media trends ” polarization, fake news, the nature of social media ” cut against those hopes. This polarized election presented itself as a target of opportunity of the first order, Mr. Rid said. Reporters may at times be hindered by a lack of transparency between media organizations, which are often highly competitive and prize speed and scoops. This has left reporters vulnerable because they cannot easily pool lessons on spotting foreign operations or, say, warn one another that a certain front is exaggerating the newsworthiness of its latest leak. The more light shone on this, the more information you have when dealing with a source, the better decisions youre going to make, Mr. Cheshire said. Mr. Thalen, the InfoWars reporter, said he was increasingly turning down leaks that he knows his audience would read avidly and reward with acclaim, but that he considered exaggerated to advance Russian interests. Still, he was unsure it had made much difference. A lot of people have swayed their reporting with their biases, and I didnt want to do that, he said. People are believing what they want to be true.

**Max Fisher**

**2017**