FTI JOURNAL
October 2014

GAME OF SHADOWS

The Growing Threat of Dark Public Relations

Bill Sims
Managing Director
Forensic & Litigation Consulting
FTI Consulting

FTI CONSULTING™

Public relations (PR) has an evil twin: dark public relations (DPR), sometimes also referred to as black PR. It involves the unethical damaging of a client's reputation or corporate identity; that is, it's about getting the bad word out — and creating that bad word out of lies and falsehoods if need be. It's the complete opposite of what PR should be about: protecting and promoting the image of a person, firm or institution.

DPR can involve a general blackening of a company's reputation or a more specific attack on a particular product or service line. DPR can take many forms: the collection and dissemination of negative media articles, the release of damning research from allegedly independent sources and virulent social media campaigns. Common DPR techniques include issuing misleading information on a competitor or identifying and spreading embarrassing information and dirty secrets that the DPR firm may have dug up through industrial espionage or competitive intelligence. Another form of DPR is the removal of negative posts from the Internet about the DPR firm's client or about the DPR firm itself, which makes fighting back difficult.

Dark Public Relations seemingly was made for our hyper-connected age, in which information (and disinformation) can be distributed globally in the virtual wink of an eye. It is not new, but, today, the practice of DPR's dark arts has been growing — especially in China, where such schemes have become almost institutionalized — and firms that specialize in DPR such as Yage Time Advertising and Xinxun Media (both shut down in 2013 after investigations by Chinese authorities, with Yage Time's founder arrested on bribery charges) have emerged on all continents for the sole purpose of creating negative images.

Despite a few government crackdowns, DPR is not going away; indeed, its practices and tools are becoming increasingly sophisticated. Companies, especially multinationals, need to be able to recognize DPR when they see it and have a playbook at hand for combatting it, along with an experienced team to execute the plan.

The Birth of the Black Arts

DPR originally was developed by government intelligence agencies to manipulate perceptions using the media — both print and online — to destroy reputations and deceive adversaries. In England, the Joint Threat Research Intelligence Group (JTRIG), a unit within the Government Communications Headquarters, uses social engineering to place erroneous information on the Internet to tarnish the reputation of its

Despite a few government crackdowns, DPR is not going away; indeed, its practices and tools are becoming increasingly sophisticated.

targets by manipulating online groups and their discussions. For example, the JTRIG uses "false flag operations" to purposely post material that is incorrectly attributed to someone else. "False victim blogs" are created to make the blogger appear to be a victim of wrongdoing by the person whose reputation the JTRIG wants to destroy. Another more well-known example of DPR is Edward Snowden's release of information about government-inspired attacks on WikiLeaks and the hacktivist group called Anonymous.

The DPR Toolkit

Due to the sensitive and underhanded nature of the work, very few DPR firms promote themselves as DPR specialists. The few that do usually stress that they work within legal boundaries, glossing over any ethical issues. Most, however, hide under the more general umbrella of public relations.

Although a DPR campaign can be short and focused, building it can be a long and complex project. Usually, it will begin with extensive information gathering. The DPR firm may employ professional investigators to ferret out embarrassing intelligence. And the firm may disguise the purpose of the intelligence collection from its own investigators to allay any ethical concerns they may have and also to provide their operatives with plausible deniability. Depending on the exact objective of the DPR campaign (and the client's budget), the campaign also may be a long-term, highly orchestrated attack designed to chip away at the targeted company's reputation and business over months or even years, using different methods to achieve the DPR firm's aims. Three dark public relations tactics are described below.

The "friendly" press

Using journalists who may or may not be on the payroll but who can be enticed by an easy, pre-packaged and colorful story, the DPR firm may be able to insert negative stories about its target into mainstream print and online media. For instance, in the case of one major international PR agency, acting for Facebook and working against Google, its DPR team contacted several journalists, some of whom were freelancers, offering to assist them in writing the story. In the case of the Asiacell initial public offering (IPO) in Iraq, it was easy for the IPO's opponents to plant abusive stories in publications hostile to the company due to their ownerships' sectarian or religious animosities.

Online anonymity

Through blogs and news groups, DPR firms cloaked in Internet anonymity sometimes start harmful discussions about a company or brand and replay them over and over to create a viral impact. Unlike planted articles, which tend to have some basis in fact, online anonymity means that these communications can be (and often are) based on information that's utterly false, as well as malicious.

In some cases, these online campaigns are fairly simple, but more sophisticated attacks may employ computer professionals to disguise internet protocol (IP) addresses (using proxy servers and other techniques) to ensure that the source remains hidden. Smear campaigns are as old as the spoken word, but the reality is that the anonymity and ease of access afforded by today's digital world also creates unprecedented opportunities to deface a brand or individual. In China, the popular social media services Qzone and Weibo have become battlegrounds for DPR, while in Taiwan, the phenomenon is rampant on popular local sites Wretch and Plurk. In Russia, the attacks take place on VK, previously known as VKontakte.

The specious report

Often very similar in style to short-seller-type market reports (and, on occasion, masquerading as such), these reports typically are produced by low-profile research companies acting for a DPR firm. The research organization rarely knows the client's name, and there frequently are several layers of deniability in order to protect the client's identity. The client hires the DPR firm, and the DPR firm engages a research company and gives it its marching orders (and sometimes inside information to get the process started.) Although the reports are designed to appear convincing, with data and, in some circumstances, so-called independent laboratory tests or interviews with well-known experts, FTI Consulting has found that these tests, statements and endorsements commonly turn out to have been manipulated or entirely fictitious. However, once a report has been issued and picked up by the media, the damage to the victim company has been done. Most of the time, refuting the facts directly does little more than magnify the negative impact as the refutation

Today, DPR campaigns no longer are used exclusively by small, shady companies employing similarly disreputable DPR providers.

invariably is married to the original, specious research in a vicious, repetitive cycle.

Getting the Bad Word Out

In recent times, DPR has spread across global boundaries and industries. Today, DPR campaigns no longer are used exclusively by small, shady companies employing similarly disreputable DPR providers. In 2011, Facebook admitted to orchestrating a smear campaign against Google. Facebook, as previously noted, hired a top public relations firm to develop a story about Google's new Social Circle product, exaggerating the privacy problems. Facebook's involvement came to light when the PR group contacted a well-known privacy advocate and asked him to put his byline on an op-ed the firm had written. The privacy individual subsequently posted his email exchanges with the PR firm on the Internet, exposing the campaign.

In another case, a website that attacked people who had been critical of Overstock.com, driving down its stock price, was revealed to have been operated (anonymously) by Overstock's director of social media. He claimed he ran the website independently of his employer.

More recently, in October 2013, Taiwan's Fair Trade Commission fined Korean giant Samsung $340,000 for spearheading an online smear campaign against rival HTC. Students had been hired by Samsung's local Taiwanese agent to write online articles attacking HTC and recommending Samsung phones.

On the political front, Russian President Vladimir Putin has been accused of hiring an army of social media propagandists combined with traditional media sources to support his narrative of a rampant and unmanageable Ukraine. Fabricated stories of atrocities carried out by Ukrainian extremists were disseminated by print and online journalists, who later were secretly awarded an Order of Service to the Fatherland.

Investigations by FTI Consulting's Global Risk & Investigations Practice on behalf of multinational clients operating in China revealed that companies increasingly face the threat of attacks on their reputation by domestic companies that have a history of using the media and DPR providers to undermine each other and now are using the same techniques to attack foreign competitors. Evidence points to a growing cadre of DPR specialists looking for opportunities to sabotage international brands on behalf of domestic Chinese companies. Some DPR firms in China provide companies with ruinous articles for attacking competitors and Internet post deletion services to help clients escape damaging news stories. The top DPR firms can offer negative article placement and Internet post deletion even for articles posted to the most popular news sites in China.

In late 2012, Caixin, a well-regarded Chinese media conglomerate providing financial and business news in print and online, released an exposé on the activities of the DPR industry in China, although, ironically, the story quickly was deleted from Caixin's website. The article focused on the actions of two companies, Yage Time Advertising and Xinxun Media, before they were investigated by the Chinese authorities and arrests made. However, there still are a number of other DPR firms operating in China, and if the goal is to have a negative news item about a competitor placed in a journal or have a derogatory story about a company removed from the web, there are plenty of firms that are more than willing to do so.

In the United States in 2013, the documentary "Blackfish" aired on CNN. The content was critical of SeaWorld, in Florida, claiming the entity mistreated dolphins, whales and other animals. Sometime after the film was broadcast, the Orlando Business Journal polled its readers, asking whether the documentary had changed [their] perception of SeaWorld. The result was quite unusual, with 99 percent of respondents stating that their opinion of the theme park had not changed since "Blackfish" aired. Upon further investigation, the Orlando Business Journal discovered that 54 percent of the responses came from a single IP address — an address owned by SeaWorld.

Even the world's largest online encyclopedia, Wikipedia, cannot shield itself from DPR. Germany's international broadcaster Deutsche Welle produced a short piece on how professionals in the PR industry had been abusing Wikipedia's open source policy in order to manipulate articles and shine a more positive light on clients' companies, pinpointing the work of major international players Daimler AG and Lufthansa.

Recognizing and Dealing with DPR

The deceptive character of DPR attacks makes it extremely difficult to establish if, in fact, they derive from consciously and maliciously orchestrated DPR or legitimate or even random social media and journalistic endeavors. Determining whether an attack is based upon fictitious or misleading information or whether it has a factual basis provides no real guidance, as DPR attacks may employ either.

However, establishing if an attack is based on fiction or fact should be the starting point for developing an appropriate response (either through in-house communications professionals or via outside strategic communications consultants).

The next step generally is to engage external investigative resources to ascertain if the attack is DPR related. Depending on the nature of the attack, the investigative steps should include:

Reviewing the most likely sponsors of a suspected DPR attack.

Establishing if the journalist or publication that has produced the attack has a history of similar attacks on other companies. Such a history could lead to the attack's sponsor.

Investigating a journalist's (or publication's) connections and relationships — again with an eye to discovering if there's a DPR sponsor behind the attack. This also applies to adverse research reports and the companies that produce these reviews.

In the case of harmful information disseminated through the Internet on blogs, chat rooms and so on, investigative steps could involve:

Establishing the background and motivations of the negative posts, looking at the initial stages and evolution of the spread of the posts.

Looking for evidence of a single source. This includes the analysis of user names and the activities of the primary bloggers, analysis of any commonalities in language and technical investigations by information technology professionals to identify IP addresses. (This may be difficult even for professionals. As noted, sophisticated DPR attacks often use proxy web servers that route the blogs through unrelated countries and, thus, disguise IP addresses.)

Professional resources should be employed for focused, discreet inquiries within the suspect instigators' locality, industry and network. Using sensitively handled investigations, FTI Consulting has had considerable success in identifying individuals and groups behind DPR campaigns and is experienced in formulating a coordinated and appropriate response strategy implemented by its strategic communications advisors, legal counsel and investigative resources.

DPR attacks are a fact of life. However, victims need not be victimized if they understand the nature of the attack and use the proper tools to combat it.

Bill Sims
Managing Director
Forensic & Litigation Consulting
FTI Consulting
William.Sims@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.