

**Thumbnail Image:**



Feb 07, 2024 by [Corneliu Bjola](#)

## **The "Dark Side" of Digital Diplomacy** <sup>[1]</sup>

Like many other technologies, digital platforms come with a dual-use challenge that is, they can be used for peace or war, for good or evil, for offense or defense.

The same tools that allow ministries of foreign affairs and embassies to reach out to millions of people and build “digital” bridges with online publics with the purpose to enhance international collaboration, improve diaspora engagement, stimulate trade relations, or manage international crises, can be also used as a form of “sharp power” to “pierce, penetrate or perforate the political and information environments in the targeted countries,” and in so doing to undermine the political and social fabric of these countries.

The “dark side” of digital diplomacy, by which I refer to the strategic use of digital technologies as tools to counter disinformation and propaganda by governments and non-state actors in pursuit of strategic interests, has expanded in the recent years to the point that it has started to have serious implications for the global order.

For example, more than 150 million Americans were exposed to the Russian disinformation campaign prior to the 2016 presidential election, which was almost eight times more the number of people who watched the evening news broadcasts of ABC, CBS, NBC and Fox stations in 2016. A recent report prepared for the U.S. Senate has found that Russia's disinformation campaign around the 2016 election used every major social media platform to deliver words, images and videos tailored to voters' interests to help elect President Trump, and allegedly worked even harder to support him while in office. Russian disinformation campaigns have also been highly active in Europe, primarily by seeking to amplify social tensions in various countries, especially in situations of intense political polarization, such as during the Brexit referendum, the Catalonian separatist vote, or the more recent "gilets jaunes" protests in France.

---

***For resource-strapped governmental institutions, especially embassies, this is clearly a major problem, as with a few exceptions, many simply do not simply have the necessary capabilities to react to, let alone anticipate and pre-emptively contain a disinformation campaign before it reaches them.***

Worryingly, the Russian strategy and tactics of influencing politics in Western countries by unleashing the "firehose of falsehoods" of online disinformation, fake news, trolling, and conspiracy theories, has started to be imitated by other (semi)authoritarian countries, such as Iran, Saudi Arabia, Philippines, North Korea, China, a development which is likely to drive more and more governments to step up their law enforcement efforts and digital counter-strategies to protect themselves against the "dark side" of digital diplomacy.

For resource-strapped governmental institutions, especially embassies, this is clearly a major problem, as with a few exceptions, many simply do not simply have the necessary capabilities to react to, let alone anticipate and pre-emptively contain a disinformation campaign before it reaches them. To help embassies cope with this problem, this contribution reviews five different tactics that digital diplomats could use separately or in combination to counter digital disinformation and discusses the possible limitations these tactics may face in practice.

Five counter-disinformation tactics for diplomats:

### **Tactic #1: Ignoring**

Ignoring trolling and disinformation is oftentimes the default option for digital diplomats working in embassies and for good reasons.

The tactic can keep the discussion focused on the key message, it may prevent escalation by denying trolls the attention they crave, it can deprive controversial issues of the “oxygen of publicity,” and it may serve to psychologically protect digital diplomats from verbal abuse or emotional distress.

The digital team of the current U.S. Ambassador in Russia seems to favor this tactic as they systematically steer away from engaging with their online critics. This approach stands in contrast with the efforts of the former Ambassador, Michael McFaul, who often tried to engage online with his followers and to explain the position of his country on various political issues to Russian audiences, only to be harshly refuted by the Russia Ministry of Foreign Affairs (MFA) or online users.


At the same time, one should be mindful of the fact that the ignore tactic may come at the price of letting misleading statements go unchallenged, indirectly encouraging more trolling due to the perceived display of passivity and of missing the opportunity to confront a particular damaging story in its nascent phase, before it may grow into a full-scale, viral phenomenon with potentially serious diplomatic ramifications.

## **Tactic #2: Debunking**

In the post-truth era, fact-checking is “the new black” as the manager of the American Press Institute’s accountability and fact-checking program neatly described it.

Faced with an avalanche of misleading statements, mistruths and ‘fake news’ often disseminated by people in position of authority, diplomats, journalists and the general public require access to accurate information in order to be able to take reliable decisions. It makes thus sense for embassies and MFAs to seek to correct false or misleading statements and to use factual evidence to protect themselves and the policies they support from deliberate and toxic distortions. The #EuropeUnited campaign launched by the German MFA in June 2018 in response to the rise of nationalism, populism and chauvinism, is supposed to do exactly that: to correct misperceptions and falsehoods spread online about Europe by presenting verifiable information about what European citizens have accomplished together as members of the European Union.

The key question, however, is whether fact-checking actually works and if so, under what conditions?

Research shows that misperceptions are widespread , that elites and the media play a key role in promoting these false and unsupported beliefs, and that false information actually outperforms true information. Providing people with sources that share their point of view, introducing facts via well-crafted visuals, and offering an alternate narrative rather than a simple refutation may help dilute the effect of disinformation, alas not eliminate it completely.

While real-time fact checks can reduce the potential for falsehoods to “stick” to the public agenda and go viral, direct factual contradictions may actually strengthen ideologically grounded beliefs as disinformation may make those exposed to it extract certain emotional benefits. This is why using emotions in addition to facts may prove a more effective solution for countering online disinformation, although the right format of fact-based emotional framing arguably varies with the context of the case and the profile of the audience.

### **Tactic #3: Turning the tables**

The jiu-jitsu principle of turning the opponent's strength into a weakness may also work well when applied to the case of counter-disinformation strategies.

The use of humor in general, and of sarcasm in particular, could be reasonably effective for enhancing the reach of the message, deflecting challenges to ones' narrative without alienating the audience, avoiding emotional escalation, and undermining the credibility of the source.

The case of the Israeli embassy in the U.S. using a “Mean Girls” meme in June 2018 to confront Ayatollah Ali Khamenei's hateful tweet about Israel being a “malignant cancerous tumor” that “has to be removed and eradicated” is instructive: it was widely shared and praised on social media and proved effective in calling attention to Israel's plea for a harsher international stance towards Iran.

On a slightly different note, the sarcastic tweet of the joint delegation of Canada at NATO in Aug 2014 poking fun at the statements of the Russian government about its troops entering Crimea by “mistake,” showcased Canada's commitment to European security and the NATO alliance and further undermined the credibility of Kremlin in the eyes of the Western public opinion.

While memetic engagement is attracting growing attention as a possible tool for countering state and non-state actors in the online information environment, one should also bear in mind the potential risks and limitations associated with this tactic. It is important, for instance, to understand well the audience, not only for increasing the effectiveness of the memetic campaign, but more critically for avoiding embarrassing situations when the appeal to humor may fall flat or even backfire, thus undermining one's own narrative and standing. The overuse of memes and humor may also work against public expectations of diplomatic conduct, which generally revolve around associations with requirements of decorum, sobriety and gravitas. Most importantly, memetic engagement should not be conducted loosely, for entertaining the audience, but with some clear objectives in mind about how to enhance the visibility of your positions or policies and/or undermine those of the opponent.

### **Tactic #4: Discrediting**

A stronger version of the jiu-jitsu principle mentioned above is the tactic of discrediting the opponent. The purpose in this case is not to undermine the credibility of the message, but of the messenger itself so that the audience will come to realize that whatever messages come from a particular source, they cannot be trusted.

This tactic should be considered very carefully, and should be used only in special

circumstances, as it would most likely lead to an escalation of the online info dispute and would probably trigger a harsh counter-reaction from the opponent. The way in which this tactic may work is by turning the opponent's communication style against itself: amplifying contradictions and inconsistencies in his/her message, exposing the pattern of falsehoods disseminated through his/her channels of communication, and maximizing the impact of the counter-narrative via the opponent's "network of networks."

Following the failed assassination attempt of Sergei Skripal and his daughter in March 2018, pro-Kremlin accounts on Twitter and Telegram started to promote a series of different conspiracies and competing narratives, attached to various hashtags and social media campaigns, with the goal, as one observer noted, to confuse people, polarize them, and push them further and further away from reality. In response to this, the FCO launched a vigorous campaign in which it took advantage of the Russian attempt to generate confusion about the incident by forcefully making the point that the 20+ different explanations offered by Kremlin and Russian sources, including the story that the assassination might have been connected to Skripal's mother-in-law, made absolutely no sense and therefore whatever claim Russian sources might make, they could be trusted.

While the campaign proved effective in further undermining the credibility of Kremlin as a trustworthy source and convincing partners to back up U.K.'s position in international fora, it should nevertheless be noted that the bar set by Russian authorities after the invasion of Crimea and the shooting down of MH17 was already low. In addition, while the tactic of discrediting the opponent may work well to contain its influence online, it may do little to deter him/her from engaging in further disinformation as long as the incentives and especially the costs for pursuing this strategy remain unaltered.

### **Tactic #5: Disrupting**

One way in which the costs of engaging in disinformation could be increased is by disrupting the network the opponent uses for disseminating disinformation online.

This would imply the mapping of the network of followers of the opponent, the tracing of the particular patterns by which disinformation is propagated throughout the network, and the identification of the gatekeepers in the network who can facilitate or obstruct the dissemination of disinformation. Once this accomplished, the disruption of the disinformation network could take place by targeting gatekeepers with factual information about the case, encouraging them not to inadvertently promote "fake news" and falsehoods, and in extreme situations by working with representatives of digital platforms to isolate gatekeepers who promote hate and violence.

The Israeli foreign ministry has been one of the MFAs applying this tactic, in this case for stopping the spread of anti-Semitic content. Accordingly, the ministry starts first by identifying gatekeepers and ranking them by their level of online influence. It then begins approaching and engaging with them online, with the purpose of making them aware of the fact that they sit an important junction of hate speech. The ministry then attempts to cultivate relationships with these gatekeepers so that they may refrain from sharing hate content online. In so doing, the ministry can effectively manage to contain or quarantine online hate networks and prevent their malicious content from reaching broader audience.

If properly implemented, this tactic could indeed significantly increase the costs of

disseminating disinformation as opponents need to constantly protect and by case to rebuild their network of gatekeepers. They may also have to frequently re-configure the patterns by which they disseminate disinformation to their target audiences. At the same time, this tactic requires specialized skills for successful design and implementation, which might not be available to many embassies or even MFAs.

The process of engineering the disruption of the disinformation network also prompts important ethical questions about how to make sure this tactic is not abused for stifling legitimate criticism of the ministry or the embassy.

## Conclusions

As argued elsewhere, digital disinformation against Western societies works by focusing on exploiting differences between EU media systems (strategic asymmetry), targeting disenfranchised or vulnerable audiences (tactical flexibility), and deliberately masking the sources of disinformation (plausible deniability). The five tactics outlined in this paper may help MFAs and embassies better cope with these challenges if applied consistently and with a strategic compass in mind. Most importantly, they need to be carefully adapted to the context of the case in order to avoid unnecessary escalation.

Here are ten questions that may help guide reflection about how to decide what tactic is appropriate to use and in what context:

1. What type of counter-reaction would reflexively serve to maximize the strategic objectives of the opponent?
2. What are the risks of ignoring a trolling attack or disinformation campaign?
3. What type of disinformation has the largest potential to have a negative political impact for the embassy or the MFA?
4. To what extent giving the “oxygen of publicity” to a story will make the counter-reaction more difficult to sustain?
5. What audiences are most open to persuasion via factual information? What audiences are less open to be convinced by facts?
6. What type of emotions resonate with the audience in specific contexts and how to invoke them appropriately as a way of introducing factual information?
7. What type of humor works better with the target audience and how to react to situations when humor is used against you?
8. How best to leverage the contradictions and inconsistencies in the opponent’s message without losing the moral ground?
9. Who are the gatekeepers in the opponent’s network of followers and to what extent can they be convinced to refrain from sharing disinformation online?
10. Under what conditions is reasonable to escalate from low-scale counter-reactions (ignoring, debunking, ‘turning the tables’) to more intense forms of tactical engagement (discrediting, disrupting)?

**Note from the CPD Blog Manager:** *This piece was originally published by the Elcano Royal Institute [here](#), where you can find more references to source material referenced throughout the article.*

---