Cognitive Hacking and the Role of Extra-Factual Information

A CONVERSATION WITH KELLY M. GREENHILL
Associate Professor and Director of the International Relations Program, Tufts University

FLETCHER FORUM: *Your forthcoming book,* Fear and Present Danger: Extra-factual Sources of Threat Conception and Proliferation, *focuses on "extra-factual" sources of political information. What does that term mean, and what are the implications of these sources of information?*

KELLY M. GREENHILL: Extra-factual information (EFI) comprises information that is either unverified or unverifiable at the time of transmission using what are known as secure standards of evidence, but which nevertheless can serve as an actionable source of knowledge about the world, both for those who believe the information to be true and for those who exploit

Kelly M. Greenhill's *research focuses on foreign and defense policy; the politics of information; the use of military force; and what are frequently called "new security challenges," including civil wars, (counter-) insurgencies, the use of migration as a weapon, and international crime as a challenge to domestic governance. In addition to her Ph.D. from M.I.T., Greenhill holds an S.M. from M.I.T., a C.S.S. from Harvard University, and a B.A. (with distinction and highest honors) from the University of California at Berkeley. Outside of Tufts University's Political Science Department, Greenhill serves as Research Fellow and as Chair of the Conflict, Security and Public Policy Working Group at Harvard University's Belfer Center and as Associate Editor of the journal International Security. Greenhill is the author of* Weapons of Mass Migration: Forced Displacement, Coercion and Foreign Policy *(Cornell Studies in Security Affairs), which won the 2011 International Studies Association's Best Book of the Year Award; and co-author and co-editor (with P. Andreas) of* Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict *(Cornell University Press); (with R. Art) of the eighth edition of* The Use of Force: Military Power and International Politics *(R&L); and (with P. Krause) of* Coercion: The Power to Hurt in International Politics *(Oxford University Press, ~~in press~~).*
2018.

the fact that others believe it to be true. Put simply, EFI encompasses not only false or misleading information but also unverified statements and other sources of non-factual knowledge, such as literature and common sense that may have little or no basis in objective reality, but can nevertheless feel viscerally true to certain audiences and thus influence their attitudes and behaviors.

As I show in my book, throughout history, savvy elites have strategically deployed EFI, consciously blending fact and fiction to sell both threats and corresponding policy responses by engaging in a kind of cognitive hacking: strategically triggering and manipulating individuals' cognitive and psychological biases as a means of achieving political-military objectives. While EFI content and delivery platforms have changed over time, the underlying mechanisms that make this kind of manipulation such an effective instrument of political influence have not. This should not be so surprising, since although technology has changed, the way our brains process information has not.

FORUM: *In previous fora, you've spoken of a "fundamental trust crisis" in the United States. What does this trust crisis look like, and how does it relate to EFI?*

GREENHILL: A functioning democracy requires a shared understanding of the rules of the game, of the veracity of information used to conduct politics, and of the credibility and reliability of public institutions. When this shared understanding is called into question, the fundamental foundations of democratic governance are threatened.

A functioning democracy requires a shared understanding of the rules of the game.... When this shared understanding is called into question, the fundamental foundations of democratic governance are threatened.

The decline in trust in key public institutions is not new. Trust has been declining in this country since the late 1960s or early 1970s—i.e., concomitant with the latter stages of the Vietnam War and the eruption of the Watergate scandal. However, recent flagrant and chronic insertions of EFI into our information ecosystem—both those that are strategic and intentional and those that are accidental and incidental—have definitely exacerbated and made trust problems significantly worse as well as created something of a vicious cycle. Recent Russian attempts to heighten discord and fuel distrust in the integrity of the U.S. electoral system (and of U.S. democratic institutions more broadly) is just one example. These problems are not unique to the United States, of course—nor are Russian attempts to undermine faith in democratic systems and institutions.

FORUM: *How does the challenge presented by extra-factual sources of information—which leads to this trust crisis—differ from or align with those posed by traditional forms of statecraft, such as subversion or espionage?*

GREENHILL: As EFI is commonly employed in subversion, espionage, and influence operations, they are deeply interconnected and always have been. For instance, EFI is routinely employed in influence operations at the strategic, operational, and tactical levels. More specifically, EFI can be used to increase the so-called "fog of war," thereby increasing strategic, operational, and/or tactical uncertainty. EFI can also be used as part of garden-variety deception schemes in order to generate ambiguity over, or misapprehension of, the objective situation (also known as facts on the ground). Finally, EFI can be deployed to strategically exploit and manipulate values, fears, and empathy within target populations to sow discord, heighten polarization, and recruit assets among disaffected populations.

FORUM: *What tools are available to states in countering fake news, rumors, and propaganda in the twenty-first century? How can they best be deployed given the rapid pace of the news cycle?*

GREENHILL: The answer depends on the nature of the particular problem one is trying to counter and who is wielding the weaponized EFI in question. It further depends on the nature of the state(s) deploying tools intended to combat EFI and the willingness of the leadership of the state(s) to use the tools available to them. There is great variation across the board on all of these dimensions. However, generally speaking, states have several kinds of tools at their disposal: education and awareness-raising; laws and regulations; intelligence operations; sanctions and other coercive tools; and information operations and counter-operations. Which tools or combinations thereof are most effective also varies across specific situations and environmental contexts. Put another way, what is, for instance, most effective in Estonia vis-à-vis Russian anti-NATO-focused influence operations may be rather different than what would be most effective within the United States in countering EFI surrounding the migration caravan being spread by non-state actors.

A further, arguably under-utilized tool is to actively do nothing, by which I mean self-consciously ignoring and not reporting on or responding to certain bits of fake news. Just because someone in a position of influence says something doesn't mean that it needs to be reported, and thereby amplified and repeated. As my own research has shown, having heard something before can make individuals two to eight-and-a-half times more likely to treat it as true or plausibly true whatever its baseline level of veracity. So, opting for the sound of silence can under some circumstances be a wise move.

FORUM: *President Trump's National Security Strategy emphasizes the need to counter Russia and China in a new era of great power competition. How have the parameters of great power competition changed from the twentieth century to the twenty-first century? How significant is the role of information and disinformation in this competition?*

GREENHILL: Although one cannot gainsay the importance of the internet as a vehicle for spreading information widely and at great speed, the most significant changes in great power competition arguably happened long before the advent of the twenty-first century. Namely, the decline in the profitability of territorial conquest and the increase in the possible costs of great power war with the advent of nuclear weapons.

At the same time, information has always been a very powerful instrument in great power rivalry, competition, and war. States work hard to maintain secrecy about their own intentions, capabilities, and operations in order to gain actionable intelligence about their adversaries' and competitors' intentions, capabilities, and operations, and, when in conflict, to minimize the fog of war for themselves while maximizing it for their counterparts. Here again, technologies have changed, but the parameters and objectives of the game have not.

Information has always been a very powerful instrument in great power rivalry, competition, and war.

FORUM: *As we consider the past one hundred years since the end of World War I, how do you think the growing challenge presented by disinformation in foreign policy will impact the future of diplomacy? Is the fundamental nature of diplomacy being challenged?*

GREENHILL: Consistent with my last answer, disinformation and deception have very frequently played a key role in successful diplomacy. Even close allies sometimes intentionally deceive each other if it is seen as in the deceiver's national interest. This is not to suggest that the truth does not have a very important role—it does!—but that the use of disinformation is not remotely new. Indeed, my book looks at cases from around the world—including, but not limited to, the United States, United Kingdom, Russia, and Germany—ranging in time from the late nineteenth century through the first decades of the twenty-first, in part to show just how much continuity we've seen across time and space in the strategic manipulation and exploitation of EFI for both political and military ends.

FORUM: *In your research on extra-factual sources of political information, have you found that regime or government type is a factor in how disinformation impacts states' foreign and defense policies?*

GREENHILL: Regime type can affect what tools and behaviors are viewed as legitimate and employable. For instance, the frequency with which what is known as "black" (versus "grey" and/or "white") propaganda may be routinely and unabashedly employed is as a rule different in liberal democracies than in illiberal authoritarian alternatives. Regime type can also affect what audience members will view as credible and plausible information. During much of the Cold War, for instance, information published in the state-run newspaper *Pravda* was treated with skepticism by many within the Soviet Union, while the opposite was true of the privately-held and run *New York Times* within the United States. Information content and context vary across time, space, and regime type, but EFI can and has been used to great effect in the security sphere (and far beyond it) in all types of regimes and with all manners of audience.

FORUM: *What are the most promising initiatives to counteract the negative effects of extra-factual sources of political information? How should the U.S. government use its resources to address threats in this space?*

GREENHILL: Here too the answer depends upon both what effects and what audiences you mean. Are the key constituencies foreign or domestic, for instance? Are they members of the general public or policymakers and political leaders? Is one trying to shut down the supply of information at its source(s), deter further dissemination, or counter or debunk false claims that have already made their way into the information ecosystem? So, again, there is no silver bullet, and no single solution; rather, answers are content and context dependent. At the same time, it is fair to say that both governments and content generators and disseminators should be using a wide array of both human and technical assets to both combat the effects of harmful EFI and deter further creation and promulgation.

FORUM: *What is the role of civil society in countering disinformation? How is the individual's responsibility and ability to address disinformation shifting as information technology continues to develop?*

GREENHILL: As my survey research and historical case studies have revealed, unfortunately civil society is not necessarily an effective bulwark against rumors, conspiracy theories, and other forms of EFI. Rather, depending on the worldviews and concerns of the members of a particular community, civil societies can both counter *and* spread EFI. The Nazis, for instance, had an extraordinarily well-developed civil society apparatus; it was just dedicated to spreading ideas that were hostile and deadly to those outside their community.

FORUM: *As we look toward future elections in the United States and around the world, what central lessons about disinformation campaigns should we learn from reflecting on the 2016 U.S. presidential election, the Brexit vote, and other recent elections?*

GREENHILL: One critical takeaway, which is too frequently underemphasized or even ignored, is that successful EFI-driven influence campaigns—which, again, are broader than disinformation operations—depend on receptive audiences. The messages that move people are those they are already inclined to believe or are open to possibly believing. Information that is widely viewed as preposterous (or as suspect given the source promulgating it) won't be effective. So, in countering such campaigns, key actors and decision makers need to address the underlying symptoms and sources of grievance, not simply the observable manifestations of them.

Successful EFI-driven influence campaigns... depend on receptive audiences.

At the same time, it bears noting that we still don't have a complete understanding of how broad and deep the problem we're facing is because bots, fake accounts, and other artificial inputs have distorted the observable picture of EFI and disinformation dissemination. We're learning more everyday, but there is still a great deal that we don't know, and to complicate things further, we're all chasing moving targets. *f*