

### MANEUVER AND MANIPULATION: ON THE MILITARY STRATEGY OF ONLINE INFORMATION WARFARE

Tim Hwang

Ongoing discussion around the Russian development of hybrid warfare and the revelations about meddling in the 2016 U.S. Presidential election have focused the public's attention on the threats posed by coordinated campaigns of propaganda and disinformation. These recent events have also raised concerns around the broader challenge posed by the emergence of a "post-fact society," the notion that the weakening ability for civil society and the public to analyze truth and falsity is creating a threat to the health and sustainability of democratic institutions.

Technology and the Internet, in particular, play a key role in shaping the flow of information through society. Not surprisingly, the role of these systems in enabling new types of information warfare has figured prominently in the discussion as policymakers and scholars begin to develop their thinking about the appropriate response to these issues. Platforms such as Facebook and Google have been seen as having had a significant role in facilitating Russian propaganda efforts, incentivizing the distribution of false information, and encouraging the creation of extremist "filter bubbles."

As the defense community develops its approach to countering present-day online propaganda and disinformation techniques, it will need to place concerns around immediate threats into a broader understanding of the nature of the challenge. It will require, in short, an articulation of a broad and flexible, unified, strategic concept that encompasses the aspects of military, diplomatic, economic, informational, and other matters regarding the strategic situation. This monograph offers an initial sketch of such a concept, proposing one approach to characterizing the strategic situation in the current information space and, based on that, some conjectures about the effective conduct of online information warfare.

The threat and use of operations that aim to shape perceptions, beliefs, and behaviors are, of course, not new to the theory or practice of warfare. Whether directed at the public or adversaries on a battlefield, these activities—to a greater or lesser extent—have long been part of the discussion of psychological operations, information operations, military operations other than war, counterinsurgency, and public diplomacy, among others. In the context of the Internet and technology more broadly, more recent concepts of computational propaganda and, less recently, netwar, also offer a precedent.

This monograph draws on and adapts this lineage of thinking and others to the current technological and informational environment. Specifically, it argues the following:

- Modern information warfare falls somewhere between topics in the defense space. On the one hand, online disinformation efforts continue a long lineage of thinking and tactical innovation around the use of persuasion and influence in conflict. On the other, these topics are a salient, novel form of threat online that introduces a new set of themes into the discussion of cybersecurity and cyberwarfare strategy. In developing an effective, strategic concept which captures the nature of modern information warfare and the manner in which it is best conducted, the former needs to be married with the latter.
- Reviewing published strategic works on online information warfare in the United States, Russia, China, and among nonstate actors, suggests that the theoretical frameworks in the space remain frustratingly incomplete and vague. These texts are mostly silent on the nature of modern information warfare, the conduct of modern information warfare, and the effective means of defending against campaigns of information warfare.

- Modern information warfare is characterized by a cartographic shift: social behavior is now directly observable at many different scales at remarkably low cost. One can observe social reactions to a stimulus as it occurs and compare these reactions across both time and space. These developments and the concentration of this data in a small set of platforms change the nature of information flow and open new possibilities for the strategic development of information warfare.
- This cartographic shift influences the aims of information warfare. Conflicts shift from contests over the adoption or rejection of certain ideas and points of view to contests over the network structure of relationships and strength of ties within a population. Victory in these conditions entails capturing the ability to shape these networks toward desired ends, while defeat entails the inability to deny this influence to an adversary.
- Liberal democracies face special challenges in this environment because they must defend the aggregate amount of social capital or trust within society. Liberal democracies must also defend a particular arrangement of social capital—one that gives independent civil society and public institutions a primary role. This requirement forces liberal democracies to construct defensible publics. This effort requires the creation of public systems of detection, support for robust social networks within society, and clear policies

around the conditions for state intervention in the information space.

\*\*\*\*\*

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute’s homepage at <https://ssi.armywarcollege.edu/>.

\*\*\*\*\*

Organizations interested in reprinting this or other SSI and USAWC Press executive summaries should contact the Editor for Production via e-mail at [usarmy.carlisle.awc.mbx.ssi-editor-for-production@mail.mil](mailto:usarmy.carlisle.awc.mbx.ssi-editor-for-production@mail.mil). All organizations granted this right must include the following statement: “Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College.”



**This Publication**



**SSI Website**



**USAWC Website**