



# POLITICS OPEN-SOURCE WARFARE

Over the next decade, **new model armies** will use network-based strategies to **disrupt social, economic, and political systems** and wage **meme warfare**.

The responses are likely to fall into two camps: Many systems and states will experience autoimmune responses, in which repeated efforts at restoration cripple the systems they seek to protect. More successful, platforms for resilience will focus on system innovations that enable flexibility and a capacity to absorb disruption.



**INSTITUTE FOR THE FUTURE**  
Ten-Year Forecast  
Perspectives 2008  
SR-1140  
www.iftf.org

## FOURTH-GENERATION WAR: OPEN INNOVATION AND SUPER-EMPOWERMENT

The past decades have seen the rise of what analysts now recognize as “Fourth-Generation warfare” (following line-and-column state warfare, firepower/attrition warfare, and maneuver warfare). Fourth-Generation warfare (4GW) builds on the increasing strength of collaborative networks, the globalization of culture, and the widespread availability of digital technologies. The result is heavily networked, decentralized, highly adaptive military actors, often without loyalty to a particular state and particularly troublesome to traditional state militaries. Think guerilla warfare 2.0.

In this model of decentralized power and ubiquitous communication the individuals can rapidly gather resources, coordinate with other small units, modify or improvise strategies, and take action without lengthy consultation of military leaders. Tactics and techniques spread virally and are rapidly prototyped in a manner similar to open source innovation. Such actions are extremely difficult to anticipate and prepare for—almost every response is immediately obsolete. This is *superempowerment*—the ability of relatively small groups to inflict damage disproportionate to their size.

## CONSEQUENCES: SYSTEMIC FAILURE

This isn't a crude argument that such forces are “stronger” than conventional militaries. In a stand-up fight against a modern army, the guerillas will likely lose. However, in an insurgency, where stand-up fights can be avoided, the modern army may find winning nearly impossible. But even talking about winning and losing in this context is simplistic. Networked insurgencies are best at

forcing costly stalemates, relying on tactics such as provocative meme warfare and the disruption of the core physical and moral infrastructure supporting modern society.

Most often, traditional institutions facing an open-source conflict respond with measures that end up either weakening their own ability to withstand attacks or actually strengthening the opposing insurgency. Such responses are akin to an autoimmune disorder, a system failure in which defensive efforts actually damage the body's health. These responses may even trigger a feedback condition, where the self-inflicted damage leads to further autoimmune reactions.

## EFFECTIVE STRATEGIES: PLATFORMS FOR RESILIENCE

Traditional institutions can, however, take advantage of the same drivers that enable the new insurgencies. And in fact, many argue that *resilience*—supported by flexible, transparent social and technological networks—can minimize the threat from open-source warfare by *absorbing* attacks rather than *resisting* them. Resilience focuses on system responsiveness and the management of consequences.

Ultimately, this story is not just about warfare. It will play out over the next decade across a variety of institutions and industries. The ongoing friction between conventional models and emergent, networked phenomena reveals a deeper strategy: in a complex, disruptive environment, stability is more likely to arise from flexibility than from rigidity. In an environment without significant disruptive pressure, it's easy to conflate stability and stasis—but under pressure of new model armies, stability and stasis may be antithetical.