Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Emergent
Futures
Lab

Scenario Three: Systems Apart: Filtered, Throttled, Poisoned, or Collected?

Trends

Trend 1: *Near-complete fracture of public access to global Internet content*

Through expansions in country-level regulation, the inevitable thinning of the social media marketplace through competition, and increased government interest in the capacity for political influence through social media, the public opinion space of the internet has developed its own kind of geography, one based on friction and the blocking of data flow across boundaries.

Trend 2: *Continued expansion of social media as a means of political influence*

The global appetite for a social Internet in the consumer's back pocket has become a target too tempting for politics to leave alone. Social Media Intelligence (SOCMINT) grows as a mechanism for state power projection and domestic political influence.

Scenario Overview

Democratic governments had been in a rift with their private sectors for nearly a decade, with neither having sufficient impetus to face head-on the volatile creature of social media that has been in desperate need of repair at the institutional level and proven to be more toxic than beneficial. The ultimate trigger was chaos erupting from a Russian social media campaign targeted at users worldwide, leading national governments to reign in the laid-back tech firms and initiate regulatory action onto their platforms, not least to wrangle the beast that is virality. After all, the noxious disinformation movement—dubbed 'Right-eous Security'—reached tens of millions of individuals in less than thirty-four minutes. Such response in democratically aligned countries signaled an unfavorable shift towards the authoritarian model popularized by China, but a censored Internet was able to insure the Chinese users who faced less exposure to the disruption.

Following the Russian campaign, democratic countries began to legitimize the threat to their alliance arising from social media being wielded as a destabilizing tool by foreign entities. Moreover, the event activated a switch in the minds of government leaders across the ideological spectrum, leading them to wonder about, and fear, the entanglement of their social media industries with broader geopolitical tensions. Yet, the power of social media as a weapon to influence and disrupt civil society has not diminished and, at this stage, may be irreversible. In fact, Social Media Intelligence (SOCMINT) has become a standard in both Silicon and Shenzhenicon Valleys, albeit through different approaches, as a formal mechanism through which to exercise political influence.

Non-democratic countries, particularly those that struggled with regime instability, have developed rigid, well-structured internal systems to filter and manipulate the deluge of information coming from abroad so as to establish and reinforce strict social orders. The 'sorting and sifting' methods have become mechanical and have lend themselves to equally rigid, well-tailored societies to the extent that citizens' emotions are being controlled and puppeteered by the state. However, the Chinese systems have come under attack by foreign adversaries developing software intended to directly thwart the AI-infused filtering techniques implemented by the Chinese. What has occurred in China, an incumbent player in the censorship game, is revealing the mounting geopolitical tensions among rival nation-states as well as the ironically placed exposure and fragility inherent in such brittle networks.

Democratically aligned countries, on the other hand, have opted for a dramatically weakened private sector by means of heavy regulation and severe consequences for non-compliance. Virality has become a virtually unstoppable wave that policymakers and politicians, as well as a slew of second-tier actors, are given no choice but to ride it. An inability on the part of tech firms to systematically protect user data and get a handle on portentous churn in the social media marketplace has necessitated government solutions. This is no longer a trade-off between security and privacy but stability and censorship. With the public highly prone to self-damage by social media, attempts to 'purge' the platforms in this newly throttled and censored environment have only been overturned by the undying lure of, and addiction to, staying connected. Even private investors and board members, seeing stock values dropping across the social media board, have deflected to the state.

Governments have fed tech firms the carrot of direct public investment but not without forcing them to relinquish front-end control over user data in return. This intelligence gathering on the public has supported nation-level efforts to tame virality—deemed an official menace to national security—and has effectively translated into institutional surveillance. The state is now equipped with a microscopic lens into the intricacies of social media interactions that is used to preemptively and proactively ward off threats arising from the lethality of viral media. At the geopolitical level, aligned countries also use the intelligence to detect and intercept attack vectors that may undermine their alliance. The result of these structural shifts has been a loosely coupled panoptic system in which social media is publicly funded, the spread of information is carefully paced to avoid the slippery slope of virality, and a "free and open Internet" is now a far-off dream.

Depending on states' assessment of the risks posed by social media saturation, they have adopted either a filtering or throttling approach to deal with the immediate destabilizing impact on civil society and to reestablish some semblance of order. Over time, however, both tactics will start building into a broader conflict strategy put in place by states aiming to shape the global balance of power in their favor. At that point, they will have to contend with the prospect of a conventional war not centered on technology per se but almost entirely instigated by it.

20XX Vignette #3

Captain Wiggins steps back from her wall of screens. She's been on shift for over five hours. Even with the eye fatigue reduction lenses she could still feel her vision swimming against all the feeds spanning out in front of her. It has been almost three years since the social media companies of the world were forced to give in to state regulation of content. Since then, her tailored operations aimed at foreign influence have only gotten more complex, more nuanced, and far bolder.

The defensive side of the house spent most of last evening fending off viral attacks on TweetBook, promoting the purchase of jailbroken Huawei DLP ("datalife pocket") that promised free connectivity and only the best applications for US citizens seeking a better virtual life. It was one thing to jail a few CEOs but another entirely to prey upon the appetite of the US consumer for unfettered access to Fortnite. If it was just about playing games maybe it wouldn't matter, but the chat function in the DLP terminal spewed all sorts of bizarre messages and news stories that made it exceedingly difficult to take real news seriously. Game players on the DLP system simply didn't care enough to figure out what was true.

Wiggins sighed. If only it was simply about disaffected voters, but the problem wasn't just that. It was that these platforms also drank tsunamis full of data on the life patterns of our citizens. It was too hard to convince people that the Chinese cared when and how often they ate Papa Dominos ordered on the DLP platform. She knew that, on a long enough timeline, all of this information was being fed to an algorithm that developed entire patterns of life on all the major cities, and worse yet, on rural citizens who had too little access and even less time to sort through all the bullshit messaging.

On the offensive side of the house, though, was the real Faustian bargain. Since SOCMINT could be collected, it could also be used against a country. The more Wiggins knew about the capacity to nudge politics in one way or another, the more she wondered just how much preparation of the battlefield would start to look like full-on preventative, propagandistic warfare against near peer competitors. Because the Chinese systems were monitored so well, her teams were trying to influence the public as well as attack and poison these data systems at the technical level.

Near-Term Implications (6 months to 1 year)

- The viral nature of socially networked interaction is increasingly understood as a threat to state political stability.
- Some states opt to abuse the patterns of virality to disrupt political processes domestically and internationally. Eventually, in reaction to these efforts, social media saturated states will place limits on the influence that social media has on its own domestic political stability through regulation and taxation.
- Seeing only some results from this effort, countries will then implement actual front-end digital and physical controls on social media firms.
- However, there will be variation on that implementation of control along two variables: throttling or filtering of data. This variation will occur based on the first trend.

Long-Term Implications (> 5 years)

- What was first viewed as a poison is eventually weaponized with remarkable nuance. The purpose of throttling and filtering will begin to shape offensive military strategies as a mechanism for shaping great power politics through all phases of potential military conflict.

Scenario Author:

Dr. Nina Kollars is a non-resident fellow at the Modern War Institute at West Point and an editorial board member for the Special Operations Journal. Her research interests are on cyber security and military innovation.

Trey Herr is the Director of the Scowcroft Center for Strategy and Security's Cyber Statecraft Initiative at the Atlantic Council.

Will Loomis is a Program Assistant in the Scowcroft Center.

Twitter: @CyberStatecraft