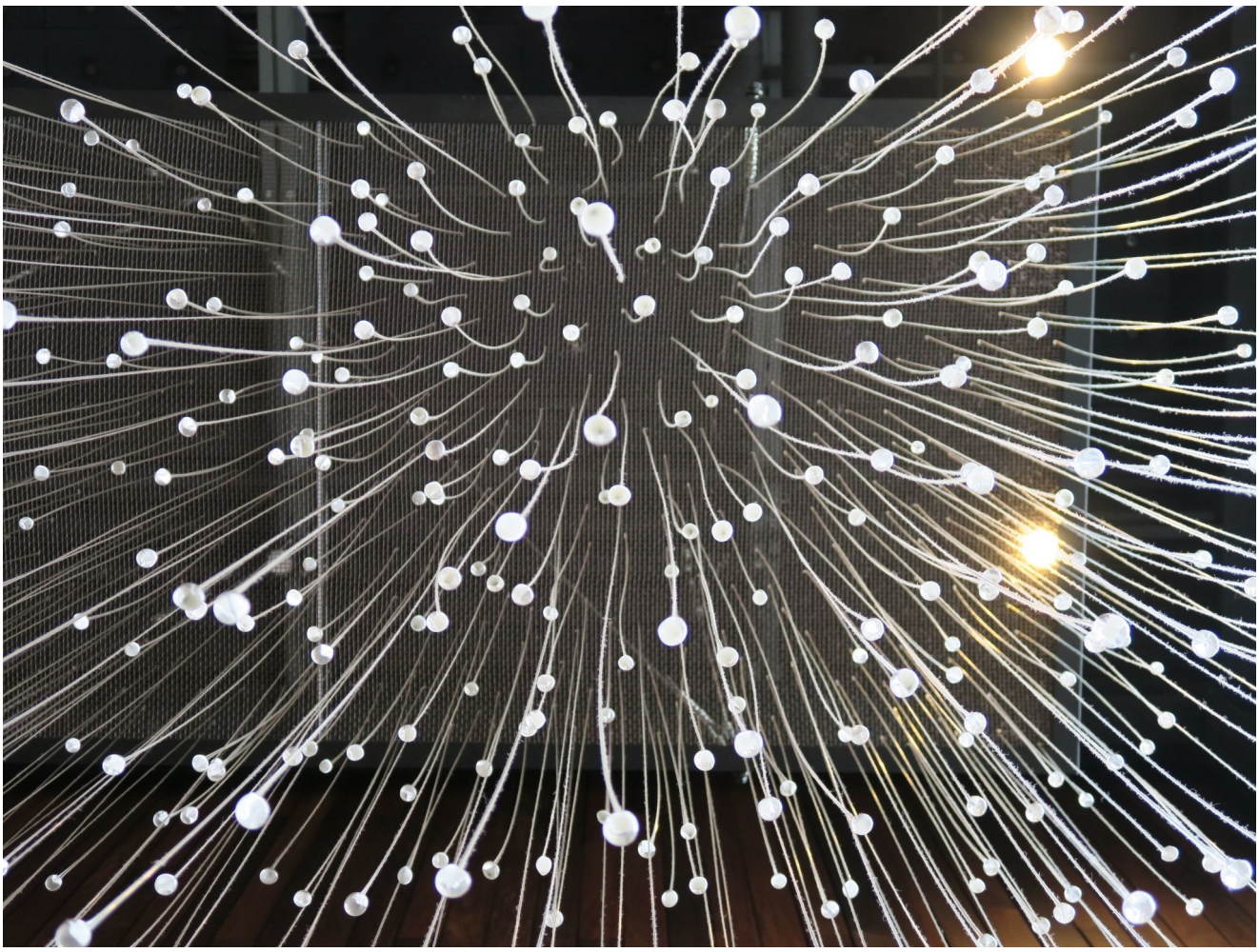
SCOTCH: A framework for rapidly assessing influence operations

atlanticcouncil.org/blogs/geotech-cues/scotch-a-framework-for-rapidly-assessing-influence-operations/

May 24, 2021



Digital Policy Disinformation Extremism Media Politics & Diplomacy Technology & Innovation
By Sam Blazek, PhD

Most of humanity now engages with digital and social media, in large part through smartphones. This new reality has cross-sectoral impacts and has changed the nature of conflict. For instance, in *LikeWar: The Weaponization of Social Media,* Peter Singer and Emerson Brooking note how the information landscape altered the dynamics of the recent war in Syria:

How information was being accessed, manipulated, and spread had taken on new power. Who was involved in the fight, where they were located, and even how they achieved victory had been twisted and transformed. Indeed, if what was online could swing the course of a

battle—or eliminate the need for battle entirely—what exactly, could be considered war at all?

The increased involvement of digital technology and media in war requires innovative frameworks for understanding information warfare and influence operations. Based on experience assessing hundreds of influence operations across six continents over the past seven years, this paper offers a new framework for professionals engaged in analyzing, understanding, and countering them.

Characterizing frameworks for influence operations

Geopolitical influence operations may be defined as those that i) are either coordinated or supported by a state actor and ii) seek to influence an audience in the interests of said actor. Such activities have been used for millennia to gain tactical or strategic advantage in combat and competition; however, the global proliferation of information technology has dramatically enhanced their scale, speed, and reach. Individuals charged with recognizing and forestalling such threats utilize many projects and platforms aimed at detecting, quantifying, forecasting, and countering influence operations. However, these efforts all rely on some characterization of *what these operations are* and *how they work*. Unfortunately, the rapid speed of change of the battle space has caused practitioners and researchers alike to struggle with defining threats and attacks.

In spite of the many existing tools, datasets, case studies, and processes that these teams have either acquired or built, **there is little consensus on how practitioners and decision makers describe and address influence operations**. As a result, they talk in circles with varying amounts of shared context or situational awareness and struggle to quickly adapt and respond as a community to social media innovations. For example, as the Atlantic Council's DFRLab recently noted, policy makers lack a cohesive strategy to combat the malicious use of real-time audio and video broadcasting.

In addition, many neglect the facts that the battlespace is highly complex and that its features are both evolving and interdependent. Society witnesses technological evolution in real-time in discussions with families and peers because the platforms in question are ubiquitous, but it is difficult to define threats, activities, and objectives in a shared operational and analytical language—as a result, researchers and policy makers struggle to validate and communicate their observations. For instance, understanding how both coordination by bad-faith actors and organic irony poisoning can morph ironic misinformation into genuine disinformation across communities is intuitive. Nonetheless, characterizing and developing practical countermeasures for these mechanisms is a remarkable challenge.

Existing taxonomies of influence operations tend to be incomplete—for example, the Carnegie Mellon BEND framework and the earlier 4Ds framework characterize only the means and some tactical objectives of individual and mass behavioral exploitation. MITRE's ATT&CK framework, as well as AMITT, a library and clearinghouse of incidents and TTPs

supported by fellow Atlantic Council Fellows Dr. Pablo Breuer and Ms. SJ Terp, formally categorizes adversarial tactics, techniques and procedures (TTPs), while specific frameworks such as Graphika's ABC(D) focus on the "who," the "what," and some of the "how" of operations. These frameworks provide excellent summaries of certain key elements of influence operations but fail to address the big picture.

A few "big picture" models do exist, nonetheless. One example is the Malign Foreign Influence Campaign Cycle developed by the US Department of Justice (DOJ) Cyber Digital Task Force. However, given DOJ's institutional objective of establishing a solid basis for legal action, the rigor and sophistication of the framework may be unwieldy for practical, time-sensitive use, and for deeper social and behavioral study.

All these frameworks can provide value to those addressing influence operations. However, as influence operations grow in complexity and technical sophistication, operators and analysts continue to lag in one key area: characterizing operations succinctly and effectively to colleagues and decision makers. Many describe their work using ad-hoc mental models in large part because existing classification schemes are either too simple to describe the nuances of complex operations or too specific to comprehensively summarize the entire information battlespace.

One key point that most will intuitively recognize, but that is too often absent from formal frameworks, is that the technical affordances of an information environment dictate available adversary tactics. Social media sites, news platforms, and mobile messaging apps form an operational landscape, and the features of each platform are all features that can be operationalized—hashtags, comment or reply capabilities, live video streams, shared-interest sub-groups, privacy settings, rebroadcast capabilities, advertising and ad targeting systems, chat rooms, and so on. Just as these features comprise the many ways that people digitally communicate with one another and browse content, they are also the means of capturing and refocusing attention on which bad-faith actors rely.

Introducing SCOTCH

In seeking a comprehensive yet succinct framework to serve the operational community, it is important to follow a **Bottom Line Up Front (BLUF)** philosophy: if a framework cannot be used to both quickly describe an operation and easily distinguish it from others, it does not work. Based on this approach, this paper has developed and operationalized the **SCOTCH Framework** for characterizing influence operations.

This framework was developed in close partnership with planners and operators within the United States Government (USG) and allied governments, analysis and data science teams across USG and NGO spaces, and several researchers and investigators from major news organizations and academic institutions. Operators examined how information is communicated to decision makers through chains of command, and how they might improve

these information flows to enhance both situational awareness and decision making. Researchers examined how they sought to identify, contextualize, and communicate findings in order to improve resource allocation in a resource-constrained, data-rich environment.

The SCOTCH framework enables analysts to **comprehensively and rapidly characterize** an adversarial operation or campaign. Further, it is built to enable researchers and policy makers to explore the underlying facets and constructs of influence, propaganda, and psychological operations in an organized and straightforward way. In doing so, SCOTCH helps to bridge the research and policy communities and to identify dimensions of these operations that merit greater attention. The framework may be used at both the strategic and tactical levels of analysis. SCOTCH can characterize both a single operation and an overarching campaign.

The acronym describes:

S – *Source*

C – *Channel*

O – *Objective*

T – *Target*

C – *Composition*

H – *Hook*

Source

The **source** of a campaign may be identifiable individuals associated with a state or non-state actor, cutouts, “bots”, or a third party such as a moderator. In many cases, the source may not immediately be known to an analyst. During the 2020 US presidential election, the source was occasionally the platform itself, as Twitter, Facebook, and other platforms took measures to counter and limit the spread of what the managing organizations determined dangerous influence operations.

Channel

Both the platform and its associated features or affordances are **channels**. A channel may be a news site, an online game and its chat features, an advertising platform, a social media platform, an online forum or chat room, and so on. Features of interest may include the availability and searchability of hashtags or viral content (and the existence of unsupervised “virality” algorithms), the existence of in-platform “groups” or subcommunities, the ability to

live-stream video, the persistence and public visibility of posted content over time, and the ease of creating a new account and/or sharing new content. Such features create what some call a “dancing competitive landscape” for varied forms of attention and influence.

Objective

As with the source, when monitoring influence operations in real-time, the **objective** may be heavily obfuscated. However, objectives may still be indirectly inferred given prior experience with an adversary and its tradecraft.

Some of the most powerful influence operations are those that galvanize populations to pursue new objectives themselves. For example, in reviewing the QAnon conspiracies, a plurality of hypotheses exists regarding the group’s actual objectives: an attempt to destabilize civil relations within the United States, a mechanism of making sense of abstractions such as “federal power,” to which many have limited exposure, a religious movement, or a cash grab, to name a few. Analysts must apply their experience and hypothesis testing abilities carefully in making a determination and must also recognize that objectives may change over time within a campaign— were any of these the *original* objective(s) of “Q”? In the case of QAnon, organizing a group with shared, extreme views may be understood as an objective in and of itself; once achieved, new objectives become attainable, ranging from further entrenching members’ beliefs, to doxxing and harassment, or even to real-world violent attacks.

Target

Conservatively, a **target** can be defined as the intended audience of a campaign over a specific channel. The target may be demographically and/or geographically bounded or characterized by shared beliefs. In terms of scope, the direct targets of a campaign may be users of an app, players of a game, individuals who meet particular advertising criteria, individuals who are characterized by social media platforms’ ad tech as members of some demographic category, members of a particular online community or network, subscribers of particular publications, and so on. An adversary may choose a “target-channel” pair based on the coverage of the target population afforded by the channel, as well as the sharing mechanisms baked into the design of the channel. In this way, available targets are determined in large part by the available channels and features, and in some cases, they can be further scoped by the personal data and metadata available to these channels about their users. The feasibility of targeting a particular group may also be mediated by a channel’s algorithmic capabilities, which are frequently opaque.

Composition

The **composition** refers broadly to the specific language or image content used in an influence operation. In many cases, it refers simply to the content being shared. However, in more sophisticated operations, it can also include technical details, such as the generation and employment of deepfakes or synthetically generated text and the structure and presentation of the materials. This category is also moderated by the **channel** and the **hook** (below), since the social channels and exploitation mechanisms leveraged will naturally inform the type of media content that may be generated and shared.

Hook

Typically, the **hook** of an influence operation represents both the technical mechanisms of exploitation, which are closely tied to the composition and channel(s), as well as the psychological phenomena being exploited. The hook relates to the tactics of persuasion and diffusion leveraged in the operation or campaign. These two constructs (persuasion and diffusion) are both *complementary*—by design, particular diffusion or injection techniques best serve particular strategic objectives—and occasionally *substitutionary*, wherein less convincing content that is more widely shared may achieve the same objective as highly persuasive content that is less widely shared.

SCOTCH example

At the campaign level, a hypothetical example of a SCOTCH characterization is: **Non-State Actors** used in an attempt to **Undermine the Integrity of the 2020 Presidential Election** among **Conservative American Audiences** using **Fake Images and Videos** and capturing attention by **Hashtag Hijacking** and **Posting in Shared-Interest Facebook Groups via Cutouts.**

An influence campaign may feature multiple exemplary items within each category and may include multiple sub-branches representing a series of **individual operations**. For instance, in the above campaign, a careful reader may identify and distinguish two separate operations, both characterizable using SCOTCH. In one, hashtag hijacking (a **hook**) was used to draw the general public (a **target**) to a particular narrative or shared-interest community (an **objective**). In the other, extreme content (including fake images and videos – a **composition**) hosted on low-quality media outlets (another **channel**) is injected directly into this community (a different **target** and **hook**) in order to harden group beliefs through collective sensemaking and social identity-building activities (a different **objective**). SCOTCH quickly and accurately summarizes both operations, as well as the broader campaign.

The benefit of this framework is twofold. First, it is lightweight: SCOTCH characterizations are succinct and intuitive, leading to short, comprehensive summaries that can be easily briefed and/or indexed. The above campaign characterization may remind many readers of headlines from major media outlets, and it takes only moments to read and interpret.

Second, SCOTCH offers decision makers the comprehensive information needed to understand an operation, and it provides sufficient information to take counteractions that specifically cater to the **source(s), channels, objectives, targets, composition, and hooks** observed. It captures the key parameters of an operation or a campaign and enables easy comparison between distinct operations without becoming unwieldy. To achieve the same using other frameworks, an analyst would need to draw from ABC(D), ATT&CK, and BEND all at once:

- BEND for the behavioral, social network, and narrative hooks employed
- ABC(D) for the sources, channels, and content composition observed in the operation, as well as channel-specific technical hooks
- ATT&CK for characterization of and insight into the source and its behavioral & technical patterns, including common targets and channels

Conclusion

The SCOTCH framework is both a general-purpose framework for operational analysis and characterization and a starting point for deeper study and decision making. Strategic planners may use SCOTCH to frame adversarial operations as one component in a broader operational and sociotechnical context. From a research standpoint, SCOTCH provides a single framework for researchers to characterize influence operations to behavioral, technical, operational, political, and commercial audiences. Operationally, it seeks to enhance analysts' sensemaking capabilities by covering **all key points** and to enable them to quickly and succinctly summarize their observations. However, there are still missing pieces. For instance, the framework does not provide for a more substantial explanation of how a campaign may play into existing narratives in a nation or community. But in a bottom-line up front (BLUF) environment, brevity is often an advantage.