

### شبکه نفوذ سایبری چگونه عمل می‌کند؟

فضای مجازی در سراسر دنیا به میدان گاه بات‌ها و ترول‌ها برای نفوذ در افکار عمومی و جنگ روانی تبدیل شده است.

این مقام فیسبوک همچنین می‌گوید: «دو سوم این بیش از دوپست شبکه‌ای که حذف کردیم و به تمامی یا به صورت نسبی بر روی مخاطب بومی تمرکز داشته است».

منا اعلام کرده که نتیجه تحقیقات آن‌ها حذف این شبکه‌های نفوذ سایبری در ۶۸ کشور مجزا بوده است که به حداقل ۴۲ زبان مختلف فعالیت می‌کردند «از زبان آمهاری [اتیوپی] گرفته تا اردو، از روسی گرفته تا چینی».

منا مدعی است که بسیاری از حملات از سوی روسیه صورت می‌گیرد. از آنجا که در آمریکا روسیه دشمن شماره یک شناخته می‌شود، آن‌ها علاقه دارند که بر نقش این‌گونه کشورها در عملیات‌های پنهان تاکید کنند. در حالی که پیش از این ماه گذشته منا تایید کرد که حساب‌های وابسته به ارتش آمریکا اقدام به انتشار پروپاگاندا ضد روسیه، چین و ایران به زبان‌های محلی می‌کردند.

مدیران شرکت منا اعتقاد دارند که شیوه‌ها و تاکتیک‌های متفاوتی در این عملیات‌های سایبری شناسایی شده استفاده شده است. این شیوه و تاکتیک بستگی به مبدا این عملیات دارد. «این که به سازمان‌های اطلاعاتی روسیه مرتبط باشد یا متعلق به موسسات بازاریابی باشد و یا نهادهایی که سرمایه‌گذار روسی تحریم شده باشند». تاکتیک‌ها طیف متنوعی دارد از کامنت‌های اسپم بر گزارش‌های خبری و شبکه‌های اجتماعی گرفته تا «تشکیل نهادهای رسانه‌ای با فعالیت در بیش از یک پلتفرم که خبرنگاران واقعی را استخدام می‌کنند تا برای آن‌ها بنویسند». در این مورد آخر، بدون این که خبرنگاران خود بدانند، فی‌الواقع برای سازمان‌هایی خارجی فعالیت کرده‌اند و در راستای اهداف آن‌ها نوشته‌اند.

شش سال پیش مداخله سایبری روسیه در انتخابات ۲۰۱۶ آمریکا اتفاقی بسیار شوکه‌کننده قلمداد شد. اتفاقی که به گفته دموکرات‌های آمریکایی باعث پیروزی دونالد ترامپ شد. روسیه متهم گشت که از طریق لشکر بات‌ها و ترول‌های سایبری‌اش اقدام به ایجاد دودستگی در مردم آمریکا کرده است. انتشار اخبار جعلی در حجمی گسترده نکته برجسته این کمپین مخفی بود.

پس از این اتفاق نهادها و رگولاتورهای مختلف در سراسر دنیا شبکه‌های اجتماعی را تحت فشار گذاشتند که کمپین‌های مشابه که از طریق فضای مجازی اقدام به دنبال نفوذ در افکار عمومی هستند را شناسایی کنند؛ و حال کمپانی منا، بزرگترین شرکت حوزه شبکه‌های اجتماعی که سه پلتفرم فیسبوک، اینستاگرام و واتس‌آپ به آن تعلق دارد اذعان دارد که این کمپین‌های سایبری اکنون به اوج فعالیت خود رسیده‌اند. منا می‌گوید که ۲۰۰ عملیات سایبری را شناسایی و منهدم ساخته است.

منا در گزارشی که ۲۴ آذر منتشر کرده است با اشاره به اقدام قضایی صورت‌گرفته علیه این کمپین‌های نفوذ مخفی، می‌گوید که مسئله در حال حاضر به یک مشکل جهانی تبدیل شده است و بیش از ۱۰۰ کشور مختلف از افغانستان تا زیمبابوه هدف این کمپین‌ها قرار گرفته‌اند.

مسئول سیاست‌گذاری امنیتی منا، ناتانائیل گلیچر (Nathaniel Gleicher) در گفتگو با خبرنگاران می‌گوید: «اگرچه اغلب مداخلات خارجی مورد توجه رسانه‌ها قرار می‌گیرد، اغلب این عملیات‌های رفتارهای برنامه‌ریزی شده غیرواقعی (CIB) که منا شناسایی کرده است همان کشورهایی را که این عاملان در آن هستند، هدف قرار می‌دهد».





متا معتقد است که مداخلات روسیه در ایالات متحده بیشترین تاثیر را در شبکه‌های اجتماعی داشته است. این به خاطر این است که اغلب پلتفرم‌های شبکه اجتماعی در آمریکا مستقر هستند و به خاطر فشارهای سیاسی در این کشور دقت بیشتری به این مسئله شده است.

در رابطه با منطقه غرب آسیا و کشورهای خلیج فارس، گزارش متا تاکید دارد که این منطقه وضعیت بسیار پیچیده‌ای در حوزه عملیات‌های نفوذ سایبری دارد. «در منطقه خلیج فارس دولت‌ها از طریق عملیات نفوذ مخفیانه سایبری، رقیبان منطقه ای‌شان را هدف قرار می‌دهند. این‌گونه عملیات‌ها تلاش می‌کند حوزه نفوذ ژئوپلتیکی این کشورها را گسترش دهد و از ابزارهایی جدید برای نفوذ ژئوپلتیکی بهره ببرد».

به‌طور مثال متا متوجه شده که «یک شبکه ایرانی از عربستان سعودی و آمریکا انتقاد می‌کند؛ یک شبکه سعودی یافته شد که ایران، قطر و ترکیه را هدف قرار داده است. عملیات نفوذی از قطر، ترکیه و مراکش شناسایی شد که از قطر و ترکیه حمایت می‌کند و عربستان، امارات و دولت مصر را نقد می‌کند و همچنین شبکه‌ای از مصر شناسایی شد که از امارت حمایت می‌کند و از قطر و ترکیه انتقاد می‌کند».

## در شرایط سیاسی اجتماعی اخیر کشور ما می‌توان تاثیر این شبکه‌های مخفی نفوذ سایبری را به وضوح مشاهده کرد

تبدیل کردن شکاف‌های اجتماعی به گسل‌های برگشت‌ناپذیر، ارائه منظری کاملاً سیاه از وضعیت کشور، ترویج گفتمانی که در نهایت به نفع منافع ملی مردم ایران نیست و تنها به سود کشورهای رقیب ایران است، از جمله ویژگی‌هایی است که در فضای سیاسی کشور مشاهده می‌شود.

پیش از این نیز دانشگاه استنفورد به همراه موسسه گرافیکا گزارشی منتشر کرد از اکانت‌های جعلی وابسته به ارتش آمریکا که در سه حوزه ایران، چین و روسیه فعالیت می‌کردند. در حوزه ایران این حساب‌ها که در اختیار قرارگاه مرکزی ارتش آمریکا (سنتکام) بودند، خود را ایرانی جا می‌زدند و به انتشار و بازنشر اخبار جعلی می‌پرداختند و تصویری کاملاً سیاه از وضعیت کشور ارائه می‌کردند. برطبق این گزارش هدف آنها، ایجاد دودستگی و تفرقه بین مردم ایران و خشمگین کردن زنان ایرانی بود. متا نیز چندی پیش این مسئله را تایید کرد.

اما باید در نظر داشت بات‌ها، ترول‌ها و موارد پیشرفته‌تر آن در این کمپین‌های نفوذ و عملیات سایبری بیشتر به دنبال جنگ نرم و روانی هستند. آن‌ها تلاش می‌کنند بر افکار عمومی اثر بگذارند و ذهن مردم را به سمت و سویی که می‌خواهند بکشانند.

اساساً در جنگ روانی به مردم گفته نمی‌شود که چه چیز مهم است و چه چیز مهم نیست. بعضی از کلمه «جنگ روانی» چنین برداشت می‌کنند که گویی هیچ مشکلی در مملکت نیست و تنها مشکل بازنمایی مغرضانه رسانه‌هاست. در حالی که اساساً طبق فرمایش مقام معظم رهبری رسانه‌های بیگانه مانند مگس‌های روی زخم هستند.







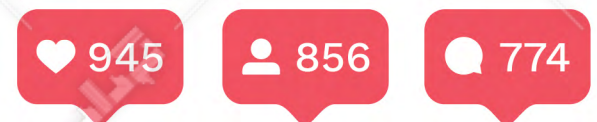




## روند تغییرات در شبکه روابط بین صفحه‌های پرمخاطب اینستاگرام ایرانی

مسئله دیگر جنگ روانی استفاده از اینفلوئنسرها به شکلی کاملاً پنهان است. همانطور که در گزارش ما آمده بود که در طی عملیات نفوذ از خبرنگاران و اینفلوئنسرها بدون اطلاع آن‌ها در راستای منافع نفوذ استفاده می‌شود، در ایران نیز ما شاهد این مسئله هستیم. اینفلوئنسر گونه جدیدی از کنشگری در شبکه‌های اجتماعی است که با سلبریتی و ... تفاوت دارد. اینفلوئنسر با مخاطبان خود نوعی نزدیکی و قرابت دارد و این باعث حس خودمانی بودن می‌شود. در نتیجه این وضعیت معمولاً احساس شک در مخاطب نسبت به گفته‌های او سرکوب می‌شود.

اینفلوئنسرها پتانسیل بالایی برای تبلیغات سیاسی دارند. مثلاً وقتی یک اینفلوئنسر درباره مسائل سیاسی نظر می‌دهد، مخاطبان او سیاسی نیستند که بتوانند با دقت صحبت او را بسنجند و در ضمن به خاطر علاقه عاطفی به اینفلوئنسر امکان این که حرف او را «باور» کنند، بسیار بالاست. در داده‌های گراف بالا مشاهده می‌کنیم بین اینفلوئنسرهایی که در حوزه‌های مختلف فعالیت می‌کردند، همگرایی رخ داده است و این نشان‌دهنده افزایش استفاده از اینفلوئنسرها برای تبلیغات سیاسی است.



باید در نظر داشت کمپین‌های نفوذ سایبری استفاده صرف از اینفلوئنسرها و هجمه از بالا به پایین نیست. بلکه جنگ روانی با استفاده از اکانت‌های جعلی صورت می‌گیرد که خود را «مردم» جا می‌زنند. با استفاده از اکانت‌های کوچک، اما پرتعداد است که جنگ روانی شکل می‌گیرد. دلیل این مسئله این است که می‌خواهند به طور مصنوعی این احساس را ایجاد کنند که موضع سیاسی این اکانت‌های جعلی، موضع «اکثریت» مردم است و «همه» روی آن اتفاق نظر دارند.

ذهن انسان به‌طور غیرارادی از مخالفت با نظر اکثریت واهمه دارد و در نتیجه، صدای مخالفان این جریان نفوذ سایبری سرکوب می‌شود. این همکاری در غالب همراه شدن اینفلوئنسر با «مردم» نشان داده می‌شود. اما واقعیت این است در نهایت این «همراه‌شدن‌ها» سود خاصی برای مردم عادی ندارد. اینفلوئنسرها قرار نیست به خیابان بیایند. آن‌ها صرفاً در حال مشروعیت‌بخشی به آرمان‌های خاصی هستند و این آرمان‌ها تحت تاثیر جنگ روانی و عملیات‌های نفوذ پنهان است.

این مشروعیت‌سازی‌ها در طی جنگ روانی برای خواسته‌های مردم نیست. مشکلاتی که مردم به‌طور ملموس در زندگی‌شان حس می‌شود، نیاز به مشروعیت‌تراشی ندارند. اما اینفلوئنسر در طی جنگ روانی بخشی از «مردم» جا زده می‌شود تا زمینه را برای مشروعیت‌تراشی چیزهایی مانند حمله نظامی آماده کند.

نقطه اوج جنگ روانی، تنبیه از پایین به بالاست. عملیات نفوذ سایبری در نهایت به حذف صدای مخالف ختم می‌شود، هرکسی که موضع مخالف بگیرد، یا حتی سکوت کند، متهم می‌شود و او توسط حساب‌های جعلی تحت فشار قرار می‌گیرد.

به عبارت دیگر در جنگ روانی با ساختن توهم «اکثریت» از طریق حساب‌های جعلی، تمام صداها مخالف سرکوب می‌شود. توجه داشته باشید لزوماً تمام کسانی که در این فرایند شرکت می‌کنند، فیک و جعلی نیستند. اکانت‌های جعلی در حقیقت نقش سیاهی لشکر را ایفا می‌کنند تا احساس «اکثریت» بودن را تشدید کنند.