



OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

22 APRIL 2022

DHS-IA-IF-2022-04870

FOREIGN INFLUENCE

(U) Moscow's Invasion of Ukraine Impeding Reach of Russian State Media in the West

(U//FOUO) Scope Note: This product continues to expand on our analysis of Russian state-sponsored messaging efforts targeting Western audiences, including operational shifts and challenges for Russian actors, such as their probable increase in use of US social media platforms that offer more permissive operating environments.^a

(U//FOUO) Russia's invasion of Ukraine has spurred Western governments, social media companies, and individuals to limit or disengage from Russian state media outlets, likely degrading many outlets' ability to directly message to Western audiences through 2022. This Western response impedes the ability of critical elements of Russia's influence ecosystem to recruit and retain culturally adept media talent, shape in-country reporting, maintain a perception of media independence, and generate revenue. These setbacks affect multiple facets of RT's and Sputnik's operations, hampering the prospects for a speedy reconstitution of their Western-facing efforts. These actions, and others being considered by Western countries, go well beyond previous efforts to counter Moscow's use of its state media outlets to spread mis-, dis-, and malinformation (MDM), such as deplatforming, foreign agent registration, and social media labeling of content.

- *(U) BANS, CLOSURES:* On 1 March, the European Union (EU) banned RT and Sputnik – Russia's principal state media outlets – preventing broadcasts and content hosting in the Union, according to EU legislation. Two days later, RT America announced it would cease production and close its US offices; and on 18 March, the UK revoked RT's broadcasting license, according to Western media reporting.

^a *(U//FOUO)* For previous I&A assessments on Russian MDM tactics, please see “*(U) ADMINISTRATIVE REVISION: Russian Malign Influence Use of Permissive Social Media Platforms*” (IA-48020-21), dated 3 March 2021 and “*(U) Non-English Targeting of Audiences in the United States by Russian, Iranian, and Chinese Foreign Influence Entities*” (IA-49902-21), dated 6 July 2021.

- (U) **DEPLATFORMING, BLOCKING ADS:** Many US-based companies and online services have removed Russian state media outlets from their platforms, application stores, or news feeds, at least partially in response to the EU ban, according to technology and business news reporting (see Appendix). They also sought to de-rank Russian state media content in search results, block the ability for Russian state media to advertise on their platforms, and increase efforts to label this content as false or affiliated with Moscow.
- (U) **RESIGNATIONS, SEVERED TIES:** Some US- and Europe-based journalists and editors associated with these pro-Russian outlets have resigned over disagreements with their employers' messaging slant on the Russia-Ukraine crisis, according to a UK trade magazine. As of 28 February, at least three senior editors of RT's video news subsidiary, Ruptly, have quit, including the chief marketing officer, according to an international news agency. In late February, a California-based affiliate of Ruptly cancelled its service agreement and severed all contact with RT, according to a senior manager's Twitter account.



(U) Picture included in senior manager's tweet about severed relationship with RT.

(U) Criminal Hacker Disruptions

(U) In response to Russia's invasion of Ukraine, criminal hackers self-identifying as members of the group Anonymous declared "cyber war" on Russia and claimed that they were disrupting access to Russian websites, including conducting distributed denial-of-service attacks against Russian state media outlet websites, according to a UK newspaper. These disruptions can temporarily limit online readership of these Russian outlets.

(U//FOUO) **Russia's efforts to circumvent Western punitive actions, such as redirecting state media users to alternative hosting platforms or pivoting to more covert channels, are unlikely to reach Western audiences as widely as legacy infrastructure.**

Despite these setbacks, Moscow has a strong desire to shape international media narratives, suggesting the Kremlin will pursue other avenues to reach foreign audiences, based on a history of RT by UK-based scholars and a DOJ indictment. Moscow has viewed RT and Sputnik outlets as alternatives to US and European outlets to counter Western media narratives, according to comments provided to a US newspaper. Moscow also continues to push its narratives through its covert English-language proxy websites and accounts, despite public exposure of their ties to Russian intelligence services and Kremlin-linked individuals.

- *(U)* RT's Twitter handle urged its followers to join alternative online platforms — like the Canada-based video streaming service Rumble — that have not yet imposed limits on Russian state media content targeting Western audiences, according to RT social media posts and US news reporting. As of 18 March, RT's Rumble account had a total of 36,000 subscribers, compared to late February when it had almost 4.6 million subscribers to its now-blocked YouTube account, according to their respective social media accounts.
- *(U)* US audiences visit RT and Sputnik's websites substantially more often than all covert Russian proxy outlets combined, according to commercial data on website traffic trends. On a three-month basis in early 2021, RT and Sputnik received roughly 29.7 and 5.6 million US visits respectively, while different proxy outlets received between 5,000 and 612,000, according to this data.
- *(U)* Russian state media outlets could also divert messaging attention to associated non-English-language channels, such as RT en Español and RT Arabic, in an attempt to reach Western audiences with additional language skills. Although the overall number of US-based, non-English language RT and Sputnik consumers remains an intelligence gap, US English speakers still outnumber Spanish-speaking citizens by more than five to one, and the EU included RT en Español in its 1 March ban, according to US Census data from 2020 and EU legislation.

(U) Chinese State Media Echoing Many Russian Narratives

(U//FOUO) Chinese English-language state media has provided an alternative avenue for Russian MDM to reach Western audiences, circumventing Western punitive actions. Following the Russian invasion of Ukraine, Chinese state media outlets began amplifying Russian allegations of US-funded bioweapon labs in Ukraine, portrayals of NATO as the aggressor through decades of US-led eastward expansion, and assertions that Western sanctions are unlikely to be effective. However, Chinese-state media did not amplify some other Russian-backed narratives, such as the claim that Nazis ran Ukraine.

(U) Appendix: Influence-Related, Private Sector Restrictions on Russia Since Ukraine Invasion^b

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Service	(U) Platforms	(U) Steps
Audio/video streaming	YouTube, Twitch, TikTok, Roku, Spotify	Account and channel removals, blocked ads and ad revenue, state-sponsored content labels
Search engines	Microsoft Bing, Google	De-ranked Russian state media searches, removed content from generated news feeds
Microblogging and networking	Meta (including Facebook and Instagram), Reddit, Telegram, Twitter	State-sponsored content labels, blocked ads, hiding discussion threads, banning corresponding links, account removals, geoblocking
Broadcast media	DirecTV	Cancelled programming
Application marketplaces	Apple App Store, Google Play Store	Removed Russian state media applications from app stores

^b (U) This table only includes international telecommunications and hosting platforms that took action against Russian state media outlets. A larger body of international businesses have ceased operating in Russia or prohibited Russian citizens' use of their services in response to the invasion.

Source, Reference, and Dissemination Information

Source Summary Statement

(U//FOUO) We assess that Russia's invasion of Ukraine has spurred Western governments, social media companies, and individuals to limit or disengage from Russian state media outlets, likely degrading the outlets' ability to push Kremlin narratives to English-language and other European audiences. We have **high confidence** in this assessment based on a body of reliable US and international news reporting, as well as credible US and EU Government information. While we are unable to determine the veracity of the information contained within the cited tweet, we do note that this social media post originated from the verified Twitter account of Maffick's chief executive officer; therefore, this individual would have routine access to this information and be able to disseminate it publicly.

(U//FOUO) We assess that Russia's efforts to circumvent Western punitive actions, such as redirecting state media users to alternative hosting platforms, in addition to its use of covert channels, are unlikely to be as effective in reaching US and European audiences as legacy RT and Sputnik infrastructure. We have **moderate confidence** in this assessment based on Western news reporting of mixed reliability and a collection of social media accounts and websites operated by Russian and Chinese state actors.

Definitions

(U//FOUO) **Foreign Influence:** Any covert, fraudulent, deceptive, or unlawful activity of foreign governments – or persons acting on their behalf – undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting US democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives.

- *(U//FOUO)* **Covert Influence:** Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action.
- *(U//FOUO)* **Overt Influence:** Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda.

(U//FOUO) **Disinformation:** An adversary's use of false or misleading information created or spread intentionally with the purpose of altering a specific target audience's attitudes or behavior to benefit the information's creator.

(U//FOUO) **Malinformation:** An adversary's deliberate use of otherwise verifiable information with malicious intent, such as by amplifying the information selectively or out of context, or to the detriment of specific persons.

(U//FOUO) **Misinformation:** An adversary's use of false or misleading information. An adversary's intent can change misinformation to disinformation.

Privacy, Civil Rights, Civil Liberties, Intelligence Oversight Notice

(U//FOUO) US persons linking, citing, quoting, or voicing the same arguments raised by these foreign influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open source information while protecting privacy, civil rights, and civil liberties.

Dissemination

(U//FOUO) Federal, state, local, and private sector stakeholders.

Warning Notices & Handling Caveats

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) All US person information has been minimized. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.