Information Warfare Watch No. 5

July 20, 2021 **Ilan I. Berman**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; Public Diplomacy and Information Operations; China; Europe; Japan; Middle East; Russia

SAUDI ARABIA'S COMING MEDIA OFFENSIVE
The House of Saud is upgrading its media presence in, and messaging to, the United States. The Kingdom has reportedly allocated funding for the creation of a new digital media platform headquartered in DC. The effort, which will employ former journalists from a variety of outlets, including *Fox News*, *al-Jazeera* and *SiriusXM* radio, is being backed by the Kingdom's massive sovereign wealth fund, and will be overseen by the Saudi Ministry of Information. The platform has not yet been formally named, but appears to be an effort to enhance Riyadh's messaging and visibility in the U.S. in light of the more punitive posture vis-a-vis the Kingdom taken by the Biden administration as compared to its predecessor. The outlet expects to commence operations before the end of the current year, and has already secured studio space and contractors in the Washington, DC area. (*CNBC*, July 8, 2021)

ENGLAND'S CONTROVERSIAL "ONLINE SAFETY" BILL
Britain's parliament is mulling passage of a new bill establishing a "duty of care" on social media firms, and holding companies and internet service providers liable for online content deemed to be "harmful." The so-called "Online Safety Bill," a draft of which was published online in May, "places new duties on social media firms to remove harmful or illegal content," the *BBC* reports. If it becomes law, the measure would, among other things, provide Ofcom, the UK's official communications regulator, the power to block access to non-compliant websites and to fine companies at variance with the legislation as much as £18 million ($24.6 million).

The draft legislation is generating heated debate in the UK. Critics of the measure worry that, if passed, the bill would turn Ofcom into a "super regulator" of sorts, providing the agency with sweeping powers that could be used to curtail free speech. Other critics have a different complaint; that the bill will provide social media companies with too much power (and a pretext) to block speech they deem even marginally questionable. (*BBC*, June 23, 2021)

CHINESE DISINFO NOW TAKES AIM AT JAPAN
A decade ago, Japan's Fukushima Daiichi nuclear plant was destroyed in the worst atomic accident since the 1986 Chernobyl meltdown. Ten years on, the incident is at the center of a new propaganda and disinformation campaign being aimed at the Japanese government. Specifically, Tokyo has announced plans to release more than one million tons of treated wastewater from the facility into the Pacific starting in 2023 - a move that has been criticized by environmental groups and nearby nations, including China. Beijing has done more than simply object, however; according to research by the Institute for Strategic Dialogue, pro-China "super spreader" accounts on Twitter have been disseminating misinformation about the proposed Japanese policy, suggesting that the move will be dangerous. In doing so, the Institute notes, these accounts are mischaracterizing some scientific data about the Fukushima incident writ large, and ignoring Japanese scientific data that indicates the wastewater is now benign and safe. (*Coda Story*, July 15, 2021)

MOSCOW FOCUSES ON INFORMATION WARFARE
A new update to Russia's 2015 *National Security Strategy* has significantly increased its focus on information warfare - and the need to guard Russian citizens against foreign subversion. The new document dwells in particular on the imperative of developing "a safe information space" to protect Russian society and its citizens "from destructive information and [its] psychological impact." "Destructive forces abroad and within the country are making attempts to use objective socio-economic difficulties in the Russian Federation in order to stimulate negative social processes, exacerbate interethnic and interfaith conflicts, and manipulate in the information sphere," the strategy notes. In response, it lays out, Russia needs to create "a safe environment for the circulation of reliable information" at home, and to develop "a system for forecasting, identifying and preventing threats to the information security of the Russian Federation, [and] identifying their sources."

These priorities, experts say, are logical. "Russia sees itself as a target of persistent and ongoing information operations by the West against Russian Federation targets like the military and security organizations, along with critical infrastructure," notes Samuel Bendett of the Center for Naval Analyses. "This new national security strategy officially elevates these information and cyber threats to the level of an existential challenge to Russia's long-term survival." (gov.ru, July 2, 2021; *DefenseOne*, July 13, 2021)