AMERICAN FOREIGN POLICY COUNCIL

Information Warfare Watch No. 9

December 9, 2021 **Ilan I. Berman**, **Joaquin Liviapoma**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Islamic Extremism; Public Diplomacy and Information Operations; Terrorism; Europe; Middle East

WHAT ISIS IS SAYING NOW ON SOCIAL MEDIA
In the wake of its ouster from its self-declared "caliphate" in Iraq and Syria, the Islamic State has been increasingly relying on "new media" to share its messages and prerogatives. The group's latest effort, communicated via the popular social messaging app Tiktok, is an attempt to recruit suicide bombers to carry out attacks in various Western nations during the upcoming Christmas celebrations. An investigation carried out last month by England's *The Sun* newspaper found that dozens of Tiktok accounts have been posting "ISIS propaganda and inciting hatred against non-Muslims." Many of these videos have urged supporters of the terror groups to launch mass-casualty attacks in the West "during the Christmas holiday." The effort has caused a number of countries, including the UK, to raise their terror alert levels in anticipation. (*The Sun*, November 20, 2021)

NEW TECH IN THE DISINFORMATION WARS
Disinformation and "fake news" is already a booming business, with real world costs to businesses and consumers estimated at some $78 billion last year. But the situation is poised to get significantly worse. Experts say that the growing maturity of artificial intelligence is propelling the rise of "deepfake" technologies that can create artificial images, videos and audio signals in ways that are increasingly difficult for consumers to discern from the real thing. These technologies - like voice cloning - have legitimate applications, but can also be used for nefarious purposes. For instance, notes Experian's David Britton, they can allow criminals "to successfully pass voice biometrics systems, or to dupe family members or acquaintances via phone, to send funds or to authorize approvals for access to sensitive systems, or to distribute funds to the fraudster." The technologies have the potential to roil global politics, too, if they're weaponized by political opponents of politicians - or by state-sponsored attackers - to fabricate fictitious statements or snippets of speech. (*Forbes*, September 21, 2021)

BELARUS CLAMPS DOWN AT HOME...
This Fall, amid growing criticism from Europe, the government of Alexander Lukashenko in Belarus launched a wide-ranging crackdown on national media. In October, Belarusian authorities labeled more than 100 channels on the popular social media platform Telegram as "extremist" pursuant to a new law restricting permissible media content. The new decree also targets Telegram users, who may now be held liable for subscribing to the banned media. Pursuant to the order, the Belarusian government warned via social media that it would "hold subscribers of extremist Telegram channels and chats criminally liable as members of an extremist group." (*The Moscow Times*, October 13, 2021)

...AND MISBEHAVES ABROAD
Minsk isn't just tightening its domestic media sphere, however. The Lukashenko government is also said to be behind a broad disinformation campaign aimed at Eastern Europe. According to a new report by U.S. cybersecurity firm Mandiant, Minsk is behind a disinformation and hacking effort that has targeted Eastern European NATO members since 2016. The campaign, known as Ghostwriter, tried to "instill conflict in the intergovernmental military group, obtain confidential information and spy on dissidents," the Associated Press has reported. NATO members that share borders with Belarus, such as Poland, Lithuania, and Latvia, as well as Ukraine, were the main targets of Ghostwriter. The disinformation efforts were focused on discrediting NATO and undercutting regional security through the hacking of "legitimate news outlets, government websites and spoofed emails." (*Newsweek*, November 16, 2021)

THE KREMLIN FINDS A NEW TARGET: TOR
TOR - an acronym for "The Onion Router" - is an encryption software that allows users to bypass web restrictions and surf the Internet anonymously. These features have made it an indispensable tool for opposition activists and democracy promoters in unfree societies, where access to the World-Wide Web is often closely monitored and severely limited. They are also the reasons why the software has become the latest target of the Kremlin in its widening crackdown on the flow of information inside Russia. "Russian censors have finally found a way to block the most famous online censorship circumvention tool" via new restrictions promulgated by state censor ROSKOMNADZOR, explains prominent Russian journalist Andrei Soldatov in the pages of *The Moscow Times*. The measures are part of "a systematic attack on technologies that could be used by the country's users to bypass censorship" that has been carried out by the Russian government in recent months.

"In the summer, Roskomnadzor blocked the first two VPNs, then the popular browser Opera killed support for its VPN," Soldatov writes. "In September, eight more popular VPNs were blocked. And then Apple turned off its Private Relay service in Russia. Private Relay was designed to encrypt all the traffic leaving the user's device so no one can intercept it. Apple has already been forced to turn it off in China, Belarus, Colombia, Egypt, Kazakhstan, Saudi Arabia, South Africa, Turkmenistan, Uganda and the Philippines, citing 'regulatory requirements' in those countries. Now it is Russia's turn."

The move, says Soldatov, is significant not only "because the software allows users to access websites and pages blocked by the authorities." "TOR was political from the beginning," and in recent years has been "largely seen as a technology developed and maintained by democratic countries to help activists in dictatorships bypass censorship in their countries." (*The Moscow Times*, December 7, 2021)
