[redacted]

NATIONAL INTELLIGENCE COUNCIL
ASSESSMENT

7 April 2020 NICA 2020-027

(U) Cyber Operations Enabling Expansive Digital Authoritarianism

(U) Key Takeaway

(U[redacted] China and other authoritarian governments are using cyber espionage, attacks, and influence operations to extend the coercive reach of their ideological enforcement and political control efforts beyond their borders. In some cases, they are impinging on Western democracies' sovereignty and interests to enhance their domestic stability.

- [redacted] We assess that China and Russia are improving their ability to analyze and manipulate large quantities of personal information, allowing them to more effectively influence or coerce targets in the United States and allied countries.
- [redacted] We assess that Beijing will be able to exploit Chinese companies' expansion of telecommunications infrastructures and digital services and their growing use in peoples' daily lives to exert its digital authoritarianism.
- [redacted] Growing concern in Europe and other democracies about Chinese and Russian cyber actions and personal privacy creates an opportunity to propose alternatives to blunt digital authoritarianism.

(U) Cyber Accesses Facilitating Influence, Coercion Efforts

(U[redacted] Authoritarian regimes have developed strong cyber espionage capabilities that enable their influence and coercion operations. As these regimes have developed confidence and access, they have begun using tools once reserved for ensuring domestic stability to conduct cyber attacks and cyber-enabled influence operations against private citizens and organizations in other countries.

- (U) China has become increasingly bold using targeted cyber attacks against Western companies that it believes facilitate unrest in China. Beijing probably conducted cyber attacks in 2019 that disrupted the messaging application Telegram because of its use in the ongoing Hong Kong protests, according to Western press reporting and a cybersecurity company.[redacted]
- [redacted]

(U) This assessment was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber Issues. It was drafted by the National Intelligence Council. Questions may be directed to the NIO on secure[redacted].

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

(U) Efforts Capitalize With Cyber Espionage

(U[redacted] States' forays into expansive digital authoritarianism typically begin with the use of hackers to conduct remote cyber espionage. A variety of countries—probably including some not traditionally viewed by the IC as highly cyber-capable—are using hackers to spy on foreign private citizens and organizations, and even entire populations.

(U) This table is [redacted]

	Hacking Opposition	Hacking Foreign Media/Journalists	Hacking NGOs	Stealing Bulk Personal Data
CHINA	✓	✓	✓	✓
[redacted]	✓	✓	✓	
[redacted]	✓	✓	✓	✓
[redacted]	✓	✓	✓	✓
RUSSIA	✓	✓	✓	✓
[redacted]	✓	✓		
[redacted]	✓	✓	✓	
[redacted]	✓			

[redacted]

[redacted]

(U) Data Analysis Expanding Capabilities

[redacted] **We assess that China and Russia are increasing their ability to analyze and manipulate large quantities of personal information in ways that will allow them to more effectively target and influence, or coerce, individuals and groups in the United States and allied countries.** Their cyber espionage efforts have helped them acquire bulk data.

- [redacted]
- [redacted]
- [redacted]

[redacted] Adversaries almost certainly are already applying data-analysis techniques to hone their efforts against US targets.

- [redacted] [redacted] Chinese intelligence officials analyzed multiple US states' [redacted] election voter registration data, [redacted] to conduct public opinion analysis on the 2020 US general election.[redacted]
- [redacted]

[redacted] Commercial Accumulation of Data Raises Stakes of Breaches

(U[redacted] Commercial enterprises' collection and aggregation of vast quantities of personal data, as well as their willingness to share it with third parties, increases both the likelihood and the impact of data breaches. Since 2013, authoritarian states have stolen huge amounts of personal data, including from US firms.

- (U[redacted] The Russian Federal Security Service in 2013 sponsored a theft of 3 billion accounts from a US web services company, and Chinese intelligence services in 2017 stole 147 million from a US credit-reporting agency and almost certainly were responsible for the 2015 theft of 80 million records from a US healthcare insurance provider.[redacted]

- (U[redacted] Iranian hackers have engaged in widespread theft of personal information—particularly in the telecommunications sector and travel industry—to track targets of interest to the Iranian regime, according to cybersecurity researchers.[redacted]

- (U) Data brokers are a prime target because they draw from thousands of sources to aggregate categories of information. Among the categories are demographics, home and neighborhood, occupation, education, purchases, property ownership, income and financial status, health details, vehicle information, personal interests, travel, social media and technology habits, ethnicity, and religious and political affiliation.[redacted]

(U) China Postured To Expand Cyber-Enabled Authoritarian Efforts Abroad

[redacted] **We assess that Beijing will have increasing opportunities to use commercial channels to exert its digital authoritarianism in the next few years. Beijing will be able to exploit Chinese companies' expansion of telecommunications infrastructures and digital services, these enterprises' growing presence in the daily lives of populations worldwide, and Beijing's rising global economic and political influence.** Beijing has demonstrated its willingness to enlist the aid of Chinese commercial enterprises to help surveil and censor regime enemies abroad.

- [redacted]

[redacted]

- [redacted]

- [redacted]

[redacted] We assess that Beijing's commercial access to personal data of other countries' citizens, along with AI-driven analytics, will enable it to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship. Such access and analytics also will enable Beijing to tailor its use of a range of online and offline carrots and sticks to its targets outside China—potentially on a large scale.

- [redacted]

- [redacted]

- [redacted] Chinese company ByteDance—whose social media app TikTok has become one of the fastest growing apps in the United States[redacted] uses AI and manual auditing to filter content and strives to present a positive image of China[redacted]

- (U) China can draw on ample Western commercial models for large-scale algorithm-driven delivery of targeted content and behavior-shaping micro-incentives—from credit and discounts to games rewarding visits to chosen locations—based on big data analysis of personal information.[redacted]

[redacted] Adversaries Exporting Approach

[redacted] **We judge that China and Russia are using digital authoritarian capabilities to aid their allies and are allowing their firms to sell equipment and know-how on the open market.** Their efforts and sales go beyond what Western firms offer—such as AI-driven facial recognition and the ubiquitous surveillance environments marketed as "safe cities" that enable states' monitoring and suppression of their populace.

- [redacted]

(U) China Building on Domestic Success

[redacted] **China builds on its success at domestic repression when it conducts cyber operations in other countries.** China leads the world in using digital tools—including cyber intrusions—to repress internal dissent.

- (U) Chinese hackers routinely penetrate and surveil the computer networks and online accounts of Tibetan groups in China and other nations, according to open-source reporting.[redacted]

- (U) The local Public Security Bureau (PSB) in Zhengzhou is automating the linkage of facial images and mobile device identification numbers captured by surveillance equipment it installed at residential complexes, according to US press reporting citing a Zhengzhou PSB database. It is linking this data to a citywide surveillance network encompassing license plates, phone numbers, faces, and social media information.[redacted]

- [redacted]

- [redacted] China uses mass surveillance and AI-driven algorithmic tracking of its citizens' behavior at home to inform the use of soft or coercive incentives and disincentives to control them.[redacted]

(U) Commercial Sector Contributing to Proliferation

(U[redacted] Firms around the world sell capabilities and expertise that facilitate governments' internal and extraterritorial monitoring and repression. Many foreign cyber firms and their subsidiaries provide cyber intrusion tools worldwide, mostly targeting mobile devices, and several conduct offensive cyber operations.

- [redacted]

- [redacted]

- (U) In late 2017, Saudi Arabia engaged the services of Israeli cyber espionage firm NSO Group to assist with extensive surveillance of Saudi dissidents abroad, according to press reporting.[redacted]

- [redacted]

(U) Western Countries Seeking To Blunt Digital Authoritarianism

[redacted] **Growing concern in** [redacted] **cyber actions and personal privacy creates an opportunity to propose alternatives that would blunt digital authoritarianism while advocating for human dignity.** [redacted]

- (U[redacted]) In February 2020, the European Commission proposed a strategy for future AI regulation that aims to boost its use in Europe while addressing EU concerns about data privacy, according to [redacted] press reporting. This strategy is largely in line with earlier arguments by French President Emmanuel Macron that European leadership would better promote European values and ethics, such as fairness, transparency, and privacy.[redacted]

- (U[redacted]) In January, European Commission Vice President Vera Jourova said that China was increasingly using disinformation to undermine European democracy and try to preemptively gain obedience to Chinese goals through control of public discourse[redacted]

- [redacted] Since 2018, South Korea has been consulting with the EU about regulations on digital privacy[redacted] [redacted]

[redacted] As part of cooperative action, however, Europeans almost certainly would want to extend efforts to address growing public concern about transparency and control of their personal data held by US firms. Allies have become more critical of US technology firms and US policies regarding data privacy and the ethics of AI usage.

[redacted]