



NATIONAL INTELLIGENCE COUNCIL

ASSESSMENT

19 August 2020

NICA 2020-06885D

Foreign Threats to 2020 US Federal Elections

(U) Key Takeaways

Scope Note: This is a downgraded version of a paper originally published on 19 August, 2020, and includes information current as of that date. This paper updates NICM 2020-32, [REDACTED]

[REDACTED] and NICM 2020-033, [REDACTED] which also addresses China's broader influence efforts. This paper does not make assessments about the impact of these efforts on the US. It also does not discuss efforts that the IC cannot attribute to foreign actors.

(U) Ahead of the 2020 US elections, foreign states will continue to use covert and overt influence measures in their attempts to sway US voters' preferences and perspectives, shift US policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

- [REDACTED] Foreign states or other actors may seek to compromise our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results. We judge that Russia, China, Iran, as well as many nonstate actors, have the capability to conduct such activities, although it would be difficult for them to

manipulate voting processes at scale and without detection.

[REDACTED] We are primarily concerned about ongoing and potential influence activity by Russia, China, and Iran.

- [REDACTED] We assess that Russia is using a range of measures primarily to denigrate former Vice President Biden and what it sees as an anti-Russia establishment. For example, it is directing or encouraging proxies to spread claims about Vice President Biden. Some Kremlin-linked actors are also seeking to boost President Trump's candidacy on social media. More broadly, Moscow's efforts seek to amplify social discord in the US and undermine Washington's global standing.
- [REDACTED] We assess that China prefers that President Trump be defeated; in the past few months it has stepped up public rhetoric criticizing his Administration, which it recognizes may affect the election. Although [REDACTED] Beijing did not intend to try to affect the election, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] online [REDACTED] influence, and collecting

(U) This assessment was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council [REDACTED]

Questions may be directed to the NIO [REDACTED]

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

derogatory information about US public officials [REDACTED]

- [illegible]

██████ We also are monitoring for signs that other countries or nonstate actors such as criminal groups are acting on their preferences for the election and attempting to covertly influence public opinion, disrupt election operations, or jeopardize election data with tactics such as the use of ransomware.

(U) Election Terminology

(U [REDACTED]) **Election influence** includes overt and covert influence activities of foreign governments or actors serving as agents of, or on behalf of, foreign governments intended to directly or indirectly affect a US election—including activities targeting candidates, political parties, voters or their preferences, or political processes. **Election interference** is a subset of election influence involving the technical aspects of the election, including activities targeting voter registration, casting and counting of ballots, and the reporting of results.

(U) **Russia**

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED] President Putin and senior Russian officials are overseeing efforts by proxies—[REDACTED]
[REDACTED]
[REDACTED]—to spread claims about former Vice President Biden as well as Ukrainian politicians and alleged Ukrainian influence in the 2016 US election. These claims include that when the former Vice President was in office, he engaged in criminal activity in his dealings with Ukraine and individuals tied to Ukrainian energy firm Burisma. Derkach, Kilimnik, and other proxy actors

NIC

NATIONAL INTELLIGENCE COUNCIL

affiliated with the Russian Government are advancing such narratives with US officials and other prominent persons as well as online, including through personal interactions and audio and documentary film releases via US and Ukrainian media outlets.

- [REDACTED] These figures are conspiring to intensify their efforts as the election approaches to orchestrate a high-profile corruption scandal implicating former Vice President Biden and the Democratic Party at the peak of the 2020 US presidential campaign. Their aim is to defeat the former Vice President and ensure the President's victory. Some of these proxy actors anticipate that Ukraine-themed narratives about Democratic corruption will play a decisive role in the election and that US persons are key to propagating these narratives.

[REDACTED] Since our assessment in May, [REDACTED] Russia continues to use state media, social media, and other online media platforms to denigrate the former Vice President, the Democratic Party, and the US political "establishment," and to promote divisions in the country. This content has largely been favorable to the President, but on occasion it criticizes his administration for policies that run counter to Russian interests.

- [REDACTED] Russian actors have circulated narratives about voter fraud resulting from mail-in balloting and called some US primary voting processes "rigged" by the Democratic Party.
- [REDACTED] Some Russian actors have shifted their focus from social media to on-line news sites. Since last year, the Lakhta Internet Research (LIR) troll farm, Russia's Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Russian Federation (GRU) have employed cadres of US and other foreign authors to create anti-American and US-focused political content on English-language news platforms, including

"United World International," [REDACTED]

[REDACTED] These groups leverage their US contacts to seed their narratives more broadly into Western media, [REDACTED]

[REDACTED] We continue to assess that Russia's understanding of US electoral dynamics and its assessment of who is likely to win will guide its calculus as the election approaches. Ongoing cyber operations could inform or fuel further influence efforts. For example, as of June 2020, [REDACTED] reconnoitered multiple state and local government websites [REDACTED]; we do not know the purpose of this effort. In July, a commercial cybersecurity company believed [REDACTED] may have targeted a US political organization, probably unsuccessfully, though we cannot independently attribute the activity. Russia for years has targeted and collected information about current and former US Government officials, which it could leak to the public at any time.

(U) China

[REDACTED] *We assess that China prefers that the President—whom Beijing sees as unpredictable and tough on China—does not win reelection. Although [REDACTED] Beijing did not intend to try to affect the election, [REDACTED] online [REDACTED] influence, and collecting derogatory information about US public officials [REDACTED]*

NIC

NATIONAL INTELLIGENCE COUNCIL

China uses mostly enticements and occasionally coercion to extract more pro-China positions and to punish those whom Beijing views as opposed to China's interests. It also employs disinformation and critical statements attacking the US Government's handling of the COVID-19 pandemic and other issues, such as the closure of the Houston Consulate, Hong Kong, the legal status of the South China Sea, and China's efforts to dominate the 5G market. [REDACTED] a pro-China network of online accounts posted video content critical of President Trump before it was deactivated by social media platforms; [REDACTED]

We assess Beijing probably calculates that a concerted effort to [REDACTED] influence the Presidential election would [REDACTED] backfiring and offer uncertain benefit, but [REDACTED] also recognizes [REDACTED] critical statements might affect the race.

- [REDACTED] a newspaper owned by the Chinese [REDACTED] claimed that economic measures Beijing could take against supporters of legislation and lawsuits seeking compensation from China over the COVID-19 pandemic may impact US state and congressional races. This is the first time we have observed Beijing issue a public warning that suggests it is willing to impose economic costs that could affect US elections.

[REDACTED] we judge that China will [REDACTED] evaluate the implications of various electoral outcomes on its interests. If Beijing were to assess that the increasingly downward trajectory in US-China relations threatened China's rise and could not be dealt with using existing tools, it might attempt to more directly thwart the President's reelection, including by leaking information [REDACTED] or through online [REDACTED] influence network.

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

NIC

NATIONAL INTELLIGENCE COUNCIL

[REDACTED]

the 2020 US elections by carrying out opportunistic intrusions against US private-sector entities in efforts to collect information on US political candidates, campaigns, donors, and voter data. [REDACTED]

[REDACTED]

- [REDACTED] Beijing has expanded its cyber collection of data related to

Threats to Election Infrastructure

[REDACTED] We assess that hostile actors could exploit Internet-connected election infrastructure—such as voter registration databases, pollbooks, and state or local election officials' websites—because of its ease of access and comparative lack of security. These systems are designed for accessibility, commonly through web portals, making them vulnerable to a range of malicious cyber activities. A committed adversary could potentially use access to these systems to disrupt or sow doubts about our democratic election processes.

[REDACTED] We assess that hostile actors could also manipulate systems that count or tabulate votes—such as voting machines—on a localized basis, but it probably would be difficult to coordinate a campaign to alter voting results on a wide scale. Post-election audits and paper trails also most likely would uncover such efforts in the nearly all US states. Similarly, foreign actors would have difficulty coordinating a large scale campaign to manipulate mail-in voting, and robust postal tracking probably would detect any large-scale effort.

[REDACTED] Cyber operations targeting the reporting of electronic tabulation results could delay reporting but probably would not affect the integrity of certified results. Denial of service attacks would also delay public access to results.

(U) Iran

[REDACTED] *Iran is conducting an influence campaign to undermine the current President and US democratic institutions, and to divide the country in advance of the 2020 elections.* Tehran sees the current administration as promoting regime change in Iran,

[REDACTED] a view that increases the Iranian leadership's interest in trying to prevent the President's reelection. Iran's efforts probably will focus on online covert influence, such as spreading disinformation on social media and recirculating anti-US content. [REDACTED]

[REDACTED]

- [REDACTED] Supreme Leader Khamenei probably has authorized the influence campaign. These efforts focus largely on creating or amplifying social media content that criticizes the President and recirculating existing news reports, memes, and hashtags focused on US civil unrest, domestic protests for racial justice, mail-in voting, and the administration's handling of the COVID-19 pandemic.

- [REDACTED]

NIC

NATIONAL INTELLIGENCE COUNCIL

[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED] Over the past two years, social media companies have removed thousands of Iranian-origin inauthentic accounts—some with links to the Iranian Government—that have shared information critical of both the current President and other

presidential candidates and that even impersonated a candidate in 2018. Tehran also uses these accounts to attempt to influence US audiences by promoting messages aligned with Iranian policies. [REDACTED]

[REDACTED] Tehran's links to some of these efforts.

[REDACTED] Iran could attempt to manipulate or attack election infrastructure—as it has in elections in the Middle East and South Asia—but we do not have any information indicating that it intends to do so in the United States. It could also seek to collect and publicly release damaging information.

- [REDACTED] In January, Iranian-contract cyber actors tried to compromise a server associated with a US business involved in election infrastructure, [REDACTED]

[REDACTED] FBI worked with the company to remediate the problem.

- [REDACTED] In June, Google announced that Iranian-linked cyber actors had unsuccessfully attempted to spearfish email accounts associated with campaign staffers working for the US President. Iran pursues such efforts in part to acquire derogatory information it could release publicly, as well as to inform its broader aims of weakening the US and damaging its standing abroad.

(U) Other Foreign Actors

[REDACTED] A range of other foreign actors have expressed preferences for the outcome of the election. We have reporting on a few that have either considered or taken steps to attempt to covertly influence US voters, presidential candidates, or US politics surrounding the election. For example:

- [REDACTED] Senior Turkish officials, including President Erdogan, believe that segments of the US Government have an entrenched, anti-Turkey viewpoint, and as a result have sought to covertly influence US politicians' and political candidates' thinking on

NIC

NATIONAL INTELLIGENCE COUNCIL

Turkey. Ankara's efforts have, over the past year, included covert funding of US municipal election campaigns, unregistered lobbying efforts, and messaging on social media by state-owned outlets.

- **Criminal or other nonstate groups** also have the capability to compromise US election infrastructure. Gaining access to election-related systems could allow them to disrupt the voting process, steal sensitive data, or undermine confidence in the election results, but we do not know whether any of them have specific plans to do so. Some incidents have already occurred; in April, unidentified actors used ransomware to compromise the computers of a Virginia county administrator and vote registrar, [REDACTED]

[REDACTED] Other foreign actors have preferences for the outcome of the US presidential election, and in the runup to November 2020 they may express their views in statements to the press, in diplomatic channels, or privately. Most probably will make only oblique or tempered public comments to avoid the appearance of trying to shape the outcome of the election. For example:

- **German** Chancellor Merkel almost certainly would prefer that President Trump not win reelection because of personality conflicts

between the two leaders and her perception that the current administration's policies have complicated Germany's, the EU's, and NATO's geopolitical positions, [REDACTED]

[REDACTED] In public remarks in July, she implicitly criticized the President's response to the COVID-19 pandemic, and in June she cited the 2020 election as a "risk factor" for the EU during a private video call with other European leaders.

- [REDACTED] In mid-2019, **Saudi** Crown Prince Muhammad Bin Salman expressed concern that Riyadh would lose US support for its priorities if the President were to lose the election in 2020, [REDACTED]
[REDACTED]
[REDACTED] the President was the most Saudi-friendly of any US President, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

NIC



NATIONAL INTELLIGENCE COUNCIL

Efforts by Selected Countries To Manipulate US Political Landscape

This graphic describes efforts by selected countries to attempt to manipulate aspects of the US political landscape over at least the past four years. It is not intended as a comparison of the scope, scale, or level of effort of each country's influence

activity. For example, the scope and scale of China's current influence activity at the state and local far outpaces Russia's and Turkey's, and Russia has leaked intelligence-acquired information more often than Iran.



Not observed, not aimed primarily at United States, or only symbolic



Preliminary or preparatory steps, with or without specific intent



Observed



EFFORTS

		RUSSIA	CHINA	IRAN
Public opinion (<i>overt</i>)	<i>Releasing press statements, state-run media content</i>	Observed	Observed	Observed
Public opinion (<i>covert</i>)	<i>Covertly messaging on social media</i>	Observed	Observed	Observed
National leaders/policy	<i>Covertly influencing Executive Branch or Congressional leaders' thinking or policies</i>	Observed	Observed	Observed
State or local leaders/policy	<i>Covertly influencing state or local government leaders' thinking or policies</i>	Observed	Observed	Not observed, not aimed primarily at United States, or only symbolic
Leaking intelligence-acquired information	<i>Publicizing information gathered through intelligence operations to damage a US political figure or organization</i>	Observed	Preliminary or preparatory steps, with or without specific intent	Observed
Election processes	<i>Targeting, accessing, or manipulating election processes or election-related systems</i>	Observed	Preliminary or preparatory steps, with or without specific intent	Preliminary or preparatory steps, with or without specific intent
Legal processes	<i>Influencing US law enforcement investigations, prosecutions, or other aspects of the US legal process</i>	Observed	Preliminary or preparatory steps, with or without specific intent	Not observed, not aimed primarily at United States, or only symbolic
Economic leverage	<i>Offering economic inducements to secure policy concessions</i>	Not observed, not aimed primarily at United States, or only symbolic	Observed	Not observed, not aimed primarily at United States, or only symbolic
Punitive measures	<i>Retaliating for US decisions or actions</i>	Observed	Observed	Not observed, not aimed primarily at United States, or only symbolic

NIC • 2007-00866