NATIONAL INTELLIGENCE COUNCIL

INTELLIGENCE COMMUNITY ASSESSMENT

10 March 2021 ICA 2020-00078D

Foreign Threats to the 2020 US Federal Elections

This document is a declassified version of a classified report. The analytic judgments outlined here are identical to those in the classified version, but this declassified document does not include the full supporting information and does not discuss specific intelligence reports, sources, or methods.

This Intelligence Community Assessment was prepared by the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council and CIA, DHS, FBI, INR, and NSA, and coordinated with CIA, DHS, FBI, INR, Treasury, and NSA.

This page intentionally blank.

Background

This document is a declassified version of a classified report that the Intelligence Community provided to the President, senior Executive Branch officials, and Congressional leadership and intelligence oversight committees on 07 January 2021. The Intelligence Community rarely can publicly reveal the full extent of its knowledge or the specific information on which it bases its analytic conclusions, as doing so could endanger sensitive sources and methods and imperil the Intelligence Community's ability to collect critical foreign intelligence. The analytic judgments outlined below are identical to those in the classified version, but this declassified document does not include the full supporting information and does not discuss specific intelligence reports, sources, or methods.

Scope Note

This Intelligence Community Assessment (ICA), as required by Executive Order (EO) 13848(1)(a), addresses key foreign actors' intentions and efforts to influence or interfere with the 2020 US federal elections or to undermine public confidence in the US election process. It builds on analysis published throughout the election cycle and provided to Executive Branch and Congressional leaders. This ICA does not include an assessment of the impact foreign malign influence and interference activities may have had on the outcome of the 2020 election. The US Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US political processes or actors, election administration or vote tabulation processes, or public opinion.

- Pursuant to EO 13848(1)(b), after receiving this assessment, the Attorney General and the Secretary of Homeland Security, in consultation with the heads of any other appropriate Federal, State, or local agencies, will evaluate the impact of any foreign efforts on the security or integrity of election infrastructure or infrastructure pertaining to a political organization, campaign, or candidate in a 2020 US federal election, and document the evaluation in a report.

- Pursuant to EO 13848(3)(a), after reviewing this assessment and the report required by EO 13848(1)(b), the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security, will impose appropriate sanctions for activities determined to constitute foreign interference in a US election.

Definitions

For the purpose of this assessment, **election influence** includes overt and covert efforts by foreign governments or actors acting as agents of, or on behalf of, foreign governments intended to affect directly or indirectly a US election—including candidates, political parties, voters or their preferences, or political processes. **Election interference** is a subset of election influence activities targeted at the technical aspects of the election, including voter registration, casting and counting ballots, or reporting results.

Sources of Information

In drafting this ICA, we considered intelligence reporting and other information made available to the Intelligence Community as of 31 December 2020.

Foreign Threats to the 2020 US Federal Elections

10 March 2021 ICA 2020-00078D

Key Judgment 1: We have no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 US elections, including voter registration, casting ballots, vote tabulation, or reporting results. We assess that it would be difficult for a foreign actor to manipulate election processes at scale without detection by intelligence collection on the actors themselves, through physical and cyber security monitoring around voting systems across the country, or in post-election audits. The IC identified some successful compromises of state and local government networks prior to Election Day—as well as a higher volume of unsuccessful attempts—that we assess were not directed at altering election processes. Some foreign actors, such as Iran and Russia, spread false or inflated claims about alleged compromises of voting systems to undermine public confidence in election processes and results.

Key Judgment 2: We assess that Russian President Putin authorized, and a range of Russian government organizations conducted, influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US. Unlike in 2016, we did not see persistent Russian cyber efforts to gain access to election infrastructure. We have high confidence in our assessment; Russian state and proxy actors who all serve the Kremlin's interests worked to affect US public perceptions in a consistent manner. **A key element of Moscow's strategy this election cycle was its use of proxies linked to Russian intelligence to push influence narratives—including misleading or unsubstantiated allegations against President Biden—to US media organizations, US officials, and prominent US individuals, including some close to former President Trump and his administration.**

Key Judgment 3: We assess that Iran carried out a multi-pronged covert influence campaign intended to undercut former President Trump's reelection prospects—though without directly promoting his rivals—undermine public confidence in the electoral process and US institutions, and sow division and exacerbate societal tensions in the US. We have high confidence in this assessment. We assess that Supreme Leader Khamenei authorized the campaign and Iran's military and intelligence services implemented it using overt and covert messaging and cyber operations.

Key Judgment 4: We assess that China did not deploy interference efforts and considered but did not deploy influence efforts intended to change the outcome of the US Presidential election. We have high confidence in this judgment. China sought stability in its relationship with the United States, did not view either election outcome as being advantageous enough for China to risk getting caught meddling, and assessed its traditional influence tools—primarily targeted economic measures and lobbying—would be sufficient to meet its goal of shaping US China policy regardless of the winner. The NIO for Cyber assesses, however, that China did take some steps to try to undermine former President Trump's reelection.

Key Judgment 5: We assess that a range of additional foreign actors—including Lebanese Hizballah, Cuba, and Venezuela—took some steps to attempt to influence the election. In general, we assess that they were smaller in scale than the influence efforts conducted by other actors this election cycle. Cybercriminals disrupted some election preparations; we judge their activities probably were driven by financial motivations.

Please also see DNI memorandum: Views on Intelligence Community Election Security Analysis, dated January 7, 2021.

Foreign Threats to the 2020 US Federal Elections

10 March 2021 ICA 2020-00078D

Discussion

Foreign governments or other foreign actors often try to influence the politics and policies of other countries. They may, for example, advocate for and try to shape other countries' foreign policies in ways that benefit their political, economic, and military interests. These efforts range along a spectrum from public statements and foreign assistance efforts, to sanctions and other economic pressure such as boycotts, to covert or clandestine efforts such as covert messaging and recruiting agents of influence. When such activities are intended to directly or indirectly affect an election—including candidates, political parties, voters or their preferences, or political processes—the IC characterizes it as **election influence**. If a foreign government, as part of its election influence efforts, attempts or takes actions to target the technical aspects of elections—including voter registration, casting and counting of ballots, and reporting of results, the IC characterizes it as **election interference**.

In 2020, the IC tracked a broader array of foreign actors taking steps to influence US elections than in past election cycles, a development that may be explained by several factors. First, increased IC focus on this issue may have uncovered a higher percentage of efforts. Second, more actors may view influence operations as important tools for projecting power abroad. The growth of internet and social media use means foreign actors are more able to reach US audiences directly, while the tools for doing so are becoming more accessible. Third, some foreign actors may perceive influence activities around US elections as continuations of broad, ongoing efforts rather than specially demarcated campaigns. They may also perceive that such a continuum makes it more difficult for the US to single out and respond to specifically election-focused influence efforts. Finally, as more foreign actors seek to exert influence over US elections, additional actors may increasingly see election-focused influence efforts as an acceptable norm of international behavior.

Greater public and media awareness of influence operations in 2020 compared to past election cycles probably helped counter them to some degree. US Government public messaging as well as Government and private sector actions probably also disrupted some activities. For example, proactive information sharing with social media companies facilitated the expeditious review, and in many cases removal, of social media accounts covertly operated by Russia and Iran. Additionally, public disclosure of Russian and Iranian efforts and US Government sanctions on some of the responsible actors probably hindered their ability to operate deniably.

Election Interference

We have no indications that any foreign actor attempted to interfere in the 2020 US elections by altering any technical aspect of the voting process, including voter registration, ballot casting, vote tabulation, or reporting results. We assess that it would be difficult for a foreign actor to manipulate election processes at scale without detection by intelligence collection on the actors themselves, through physical and cyber security monitoring around voting systems across the country, or in post-election audits of electronic results and paper backups. We identified some successful compromises of state and local government networks prior to Election Day. We assess these intrusions were

parts of broader campaigns targeting US networks and not directed at the election. Some foreign actors, such as Iran and Russia, spread false or inflated claims about alleged compromises of voting systems to try to undermine public confidence in election processes and results.

Over the course of the election cycle, the IC, other US agencies, and state and local officials also identified thousands of reconnaissance or low-level, unsuccessful attempts to gain access to county or state government networks. Such efforts are common and we have no indications they were aimed at interfering in the election.

- Some of these government networks hosted, among a variety of other government processes, election-related elements like voter registration databases or state election results reporting websites. We have no indications that these activities altered any election processes or data.

- Defensive measures such as firewalls, up-to-date patching, cybersecurity training for government personnel, and separation of election-specific systems from other computer networks probably helped to thwart thousands of compromise attempts. Such measures probably also would have helped prevent the network intrusions we detected.

Russia's Efforts to Influence 2020 Election, Exacerbate Divisions in US

We assess that President Putin and the Russian state authorized and conducted influence operations against the 2020 US presidential election aimed at denigrating President Biden and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US. Unlike in 2016, we did not see persistent Russian cyber efforts to gain access to election infrastructure. We have high confidence in these judgments because a range of Russian state and proxy actors who all serve the Kremlin's interests worked to affect US public perceptions. We also have high confidence because of the consistency of themes in Russia's influence efforts across the various influence actors and throughout the campaign, as well as in Russian leaders' assessments of the candidates. **A key element of Moscow's strategy this election cycle was its use of people linked to Russian intelligence to launder influence narratives—including misleading or unsubstantiated allegations against President Biden—through US media organizations, US officials, and prominent US individuals, some of whom were close to former President Trump and his administration.**

Kremlin Direction of Influence Activity

We assess that President Putin and other senior Russian officials were aware of and probably directed Russia's influence operations against the 2020 US Presidential election. For example, we assess that Putin had purview over the activities of Andriy Derkach, a Ukrainian legislator who played a prominent role in Russia's election influence activities. Derkach has ties to Russian officials as well as Russia's intelligence services.

- Other senior officials also participated in Russia's election influence efforts—including senior national security and intelligence officials who we assess would not act without receiving at least Putin's tacit approval.

Actors, Methods, and Operations

We assess that Russia's intelligence services, Ukraine-linked individuals with ties to Russian intelligence and their networks, and Russian state media, trolls, and online proxies engaged in activities targeting the 2020 US presidential election. The primary effort the IC uncovered revolved around a narrative—that Russian actors began spreading as early as 2014—alleging corrupt ties between President Biden, his family, and other US officials and Ukraine. Russian intelligence services relied on Ukraine-linked proxies and these proxies' networks—including their US contacts—to spread this narrative to give Moscow plausible deniability of their involvement. We assess that the goals of this effort went beyond the US presidential campaign

to include reducing the Trump administration's support for Ukraine. As the US presidential election neared, Moscow placed increasing emphasis on undermining the candidate it saw as most detrimental to its global interests. We have no evidence suggesting the Ukrainian Government was involved in any of these efforts.

- A network of Ukraine-linked individuals—including Russian influence agent Konstantin Kilimnik—who were also connected to the Russian Federal Security Service (FSB) took steps throughout the election cycle to damage US ties to Ukraine, denigrate President Biden and his candidacy, and benefit former President Trump's prospects for reelection. We assess this network also sought to discredit the Obama administration by emphasizing accusations of corruption by US officials, and to falsely blame Ukraine for interfering in the 2016 US presidential election.

- Derkach, Kilimnik, and their associates sought to use prominent US persons and media conduits to launder their narratives to US officials and audiences. These Russian proxies met with and provided materials to Trump administration-linked US persons to advocate for formal investigations; hired a US firm to petition US officials; and attempted to make contact with several senior US officials. They also made contact with established US media figures and helped produce a documentary that aired on a US television network in late January 2020.

- As part of his plan to secure the reelection of former President Trump, Derkach publicly released audio recordings four times in 2020 in attempts to implicate President Biden and other current or former US Government officials in allegedly corrupt activities related to Ukraine. Derkach also worked to initiate legal proceedings in Ukraine and the US related to these allegations. Former Ukrainian officials associated with Derkach sought to promote similar claims throughout late 2019 and 2020, including through direct outreach to senior US Government officials.

We assess that Russia's cyber units gathered information to inform Kremlin decision-making about the election and Moscow's broader foreign policy interests. Through these operations, Russia probably gathered at least some information it could have released in influence operations. We assess Russia did not make persistent efforts to access election infrastructure, such as those made by Russian intelligence during the last US presidential election.

- For example, shortly after the 2018 midterm elections, Russian intelligence cyber actors attempted to hack organizations primarily affiliated with the Democratic Party. Separately, the GRU unsuccessfully targeted US political actors in 2019 and 2020; this activity aligned with the tactics of a larger intelligence-gathering campaign.

- In late 2019, GRU cyber actors conducted a phishing campaign against subsidiaries of Burisma holdings, likely in an attempt to gather information related to President Biden's family and Burisma.

- We judge that Russian cyber operations that targeted and compromised US state and local government networks in 2020—including exfiltrating some voter data—were probably not election-focused and instead part of a broader campaign targeting dozens of US and global entities.

Throughout the election cycle, Russia's online influence actors sought to affect US public perceptions of the candidates, as well as advance Moscow's long-standing goals of undermining confidence in US election processes and increasing sociopolitical divisions among the American people. During the presidential primaries and dating back to 2019, these actors backed candidates from both major US political parties that Moscow viewed as outsiders, while later claiming that election fraud helped what they called "establishment" candidates. Throughout the election, Russia's online influence actors sought to amplify mistrust in the electoral process by denigrating mail-in

ballots, highlighting alleged irregularities, and accusing the Democratic Party of voter fraud.

- The Kremlin-linked influence organization Project Lakhta and its Lakhta Internet Research (LIR) troll farm—commonly referred to by its former moniker Internet Research Agency (IRA)—amplified controversial domestic issues. LIR used social media personas, news websites, and US persons to deliver tailored content to subsets of the US population. LIR established short-lived troll farms that used unwitting third-country nationals in Ghana, Mexico, and Nigeria to propagate these US-focused narratives, probably in response to efforts by US companies and law enforcement to shut down LIR-associated personas.

- Russian state media, trolls, and online proxies, including those directed by Russian intelligence, published disparaging content about President Biden, his family, and the Democratic Party, and heavily amplified related content circulating in US media, including stories centered on his son. These influence actors frequently sought out US contributors to increase their reach into US audiences. In addition to election-related content, these online influence actors also promoted conspiratorial narratives about the COVID-19 pandemic, made allegations of social media censorship, and highlighted US divisions surrounding protests about racial justice.

- Russian online influence actors generally promoted former President Trump and his commentary, including repeating his political messaging on the election results; the presidential campaign; debates; the impeachment inquiry; and, as the election neared, US domestic crises. Influence actors sometimes sought to discourage US left-leaning audiences from voting by suggesting that neither candidate was a preferable option. At the same time, Russian actors criticized former President Trump or his administration when they pursued foreign policies—such as the targeted killing of Iranian General Qasem Soleimani in January 2020—at odds with Russia's preferences.

- LIR, which probably receives tasking and strategic direction from the Kremlin, pushed stories supporting former President Trump and denigrating President Biden after he became the presumptive nominee in April.

Evaluating Moscow's Calculus on the 2020 Election

We assess that Russian leaders viewed President Biden's potential election as disadvantageous to Russian interests and that this drove their efforts to undermine his candidacy. We have high confidence in this assessment.

- Russian officials and state media frequently attacked President Biden for his leading role in the Obama administration's Ukraine policy and his support for the anti-Putin opposition in Russia, suggesting the Kremlin views him as part of a reflexively anti-Russia US foreign policy establishment. Putin probably also considers President Biden more apt to echo the idea of American "exceptionalism," which he and other Kremlin leaders have often publicly criticized as problematic and dangerous.

- Moscow's range of influence actors uniformly worked to denigrate President Biden after his entrance into the race. Throughout the primaries and general election campaign, Russian influence agents repeatedly spread unsubstantiated or misleading claims about President Biden and his family's alleged wrongdoing related to Ukraine. By contrast, during the Democratic primaries Russian online influence actors promoted candidates that Moscow viewed as outside what it perceives to be an anti-Russia political establishment.

- Even after the election, Russian online influence actors continued to promote narratives questioning the election results and disparaging President Biden

and the Democratic Party. These efforts parallel plans Moscow had in place in 2016 to discredit a potential incoming Clinton administration, but which it scrapped after former President Trump's victory.

We assess Russian leaders preferred that former President Trump win reelection despite perceiving some of his administration's policies as anti-Russia. We have high confidence in this assessment based in part on the Kremlin's public comments about him and the consistency and volume of anti-Biden messaging we detected from Russian online influence actors.

As the election neared, Kremlin officials took some steps to prepare for a Biden administration, probably because they believed former President Trump's prospects for re-election had diminished.

- Putin—while praising former President Trump personally during an interview in October—noted that President Biden appeared willing to extend the New START Treaty (NST) or negotiate a new strategic offensive reduction treaty. The comments were consistent with Russian officials' view that a potential Biden administration would be more open to arms control negotiations.

Moscow almost certainly views meddling in US elections as an equitable response to perceived actions by Washington and an opportunity to both undermine US global standing and influence US decision-making. We assess that Moscow will continue election influence efforts to further its longstanding goal of weakening Washington because the Kremlin has long deemed that a weakened United States would be less likely to pursue assertive foreign and security policies abroad and more open to geopolitical bargains with Russia.

- Russian officials are probably willing to accept some risk in conducting influence operations targeting the US—including against US elections—because they believe Washington meddles similarly in Russia and other countries and that such efforts are endemic to geostrategic competition.

- Russian officials probably also assess that continued influence operations against the United States pose a manageable risk to Russia's image in Washington because US-Russia relations are already extremely poor.

Iran's Influence Campaign Designed to Undercut Former President Trump's Reelection, Sow Discord

We assess with high confidence that Iran carried out an influence campaign during the 2020 US election season intended to undercut the reelection prospects of former President Trump and to further its longstanding objectives of exacerbating divisions in the US, creating confusion, and undermining the legitimacy of US elections and institutions. We did not identify Iran engaging in any election interference activities, as defined in this assessment. Tehran's efforts were aimed at denigrating former President Trump, not actively promoting his rivals. We assess that Tehran designed its campaign to attempt to influence US policy toward Iran, distract US leaders with domestic issues, and to amplify messages sympathetic to the Iranian regime. Iran's efforts in 2020—especially its e-mails to individual US voters and efforts to spread allegations of voter fraud—were more aggressive than in past election cycles.

- We assess that Tehran's efforts to attempt to influence the outcome of the 2020 US election and Iranian officials' preference that former President Trump not be reelected were driven in part by a perception that the regime faced acute threats from the US.

- Iran's election influence efforts were primarily focused on sowing discord in the United States and exacerbating societal tensions—including by creating or amplifying social media content that criticized former President Trump—probably because they believed that this advanced Iran's

longstanding objectives and undercut the prospects for the former President's reelection without provoking retaliation.

Actors, Methods, and Operations

We assess that Supreme Leader Ali Khamenei probably authorized Iran's influence campaign and that it was a whole of government effort, judging from the involvement of multiple Iranian Government elements. We have high confidence in this assessment.

- Iran focused its social media and propaganda on perceived vulnerabilities in the United States, including the response to the COVID-19 pandemic, economic recession, and civil unrest.

During this election cycle Iran increased the volume and aggressiveness of its cyber-enabled influence efforts against the United States compared to past election influence efforts. This included efforts to send threatening e-mails to American citizens and to amplify concerns about voter fraud in the election.

- In a highly targeted operation, Iranian cyber actors sent threatening, spoofed emails purporting to be from the Proud Boys group to Democratic voters in multiple US states, demanding that the individuals change their party affiliation and vote to reelect former President Trump. The same actors also produced and disseminated a video intending to demonstrate alleged voter fraud.

- Since early 2020, Iranian actors created social media accounts that targeted the United States and published over 1,000 pieces of online content on the United States, though US social media companies subsequently removed many. Tehran expanded the number of its inauthentic social media accounts to at least several thousand and boosted the activity of existing accounts, some of which dated back to 2012.

Post-Election Activity

We assess that Iran continues to use influence operations in attempts to inflame domestic tensions in the US. For example, in mid-December 2020, Iranian cyber actors were almost certainly responsible for the creation of a website containing death threats against US election officials.

- We assess Iran is also seeking to exploit the post-election environment to collect intelligence.

We assess that Iranian actors did not attempt to manipulate or attack any election infrastructure.

- In early 2020, Iranian cyber actors exploited a known vulnerability to compromise US entities associated with election infrastructure as a part of a broad targeting effort across multiple sectors worldwide. Given the breadth and number of the targets, we judge that Iran did not specifically intend to use the results of this effort as part of its election influence campaign.

We assess that Iran primarily relied on cyber tools and methods to conduct its covert operations because they are low cost, deniable, scalable, and do not depend on physical access to the United States. Iranian cyber actors who focused on influence operations targeting the election adapted their activities and content based on political developments and blended cyber intrusions with online influence operations.

- As part of their influence operations, Iranian cyber actors sought to exploit vulnerabilities on US states' election websites, as well as news website content management systems.

- Iranian cyber actors sent spearphishing emails to current and former senior officials and members of political campaigns, almost certainly with the

intent to gain derogatory information or accesses for follow-on operations.

China Did Not Attempt to Influence Presidential Election Outcome

We assess that China did not deploy interference efforts and considered but did not deploy influence efforts intended to change the outcome of the US presidential election. We have high confidence in this judgment. China sought stability in its relationship with the United States and did not view either election outcome as being advantageous enough for China to risk blowback if caught. Beijing probably believed that its traditional influence tools, primarily targeted economic measures and lobbying key individuals and interest groups, would be sufficient to achieve its goal of shaping US policy regardless of who won the election. **We did not identify China attempting to interfere with election infrastructure or provide funding to any candidates or parties.**

- The IC assesses that Chinese state media criticism of the Trump administration's policies related to China and its response to the COVID-19 pandemic remained consistent in the lead-up to the election and was aimed at shaping perceptions of US policies and bolstering China's global position rather than to affect the 2020 US election. The coverage of the US election, in particular, was limited compared to other topics measured in total volume of content.

- China has long sought to influence US politics by shaping political and social environments to press US officials to support China's positions and perspectives. We did not, however, see these capabilities deployed for the purpose of shaping the electoral outcome.

Beijing probably judged risk of interference was not worth the reward

We assess that Beijing's risk calculus against influencing the election was informed by China's preference for stability in the bilateral relationship, their probable judgment that attempting to influence the election could do lasting damage to US-China ties, and belief that the election of either candidate would present opportunities and challenges for China.

- We judge that Chinese officials would work with former President Trump if he won a second term. Beijing since at least 2019 has stressed the need to improve bilateral ties after the election regardless of who won.

- In addition, China was probably concerned the United States would use accusations of election interference to scapegoat China. This may in part account for Beijing waiting until 13 November to congratulate President Biden.

We assess that Beijing also believes there is a bipartisan consensus against China in the United States that leaves no prospect for a pro-China administration regardless of the election outcome.

China probably expected that relations would suffer under a second term for former President Trump because he and his administration would press for further economic decoupling and challenge China's rise. It probably also believed that China in this scenario could increase its international clout because it perceived that some of the Trump administration's policies would alienate US partners.

- Beijing probably expected that President Biden would be more predictable and eager to initially deescalate bilateral tensions but would pose a greater challenge over the long run because he would be more successful in mobilizing a global alliance against China and criticizing China's human rights record.

- Beijing probably judged that Russia's efforts to interfere in the 2016 election significantly damaged Moscow's position and relationship with the United States and may have worried that Washington would uncover a Chinese attempt to

deploy similar measures to influence or interfere in the election and punish Beijing.

Beijing probably continued to collect intelligence on election-related targets and topics

China probably also continued longstanding efforts to gather information on US voters and public opinion; political parties, candidates and their staffs; and senior government officials. We assess Beijing probably sought to use this information to predict electoral outcomes and to inform its efforts to influence US policy toward China under either election outcome, as it has during all election cycles since at least 2008 and considers an acceptable tool of statecraft.

- We assess Beijing did not interfere with election infrastructure, including vote tabulation or the transmission of election results.

Minority View

The National Intelligence Officer for Cyber assesses that China took at least some steps to undermine former President Trump's reelection chances, primarily through social media and official public statements and media. The NIO agrees with the IC's view that Beijing was primarily focused on countering anti-China policies, but assesses that some of Beijing's influence efforts were intended to at least indirectly affect US candidates, political processes, and voter preferences, meeting the definition for election influence used in this report. The NIO agrees that we have no information suggesting China tried to interfere with election processes. The NIO has moderate confidence in these judgments.

This view differs from the IC assessment because it gives more weight to indications that Beijing preferred former President Trump's defeat and the election of a more predictable member of the establishment instead, and that Beijing implemented some—and later increased—its election influence efforts, especially over the summer of 2020. The NIO assesses these indications are more persuasive than other information indicating that China decided not to intervene. The NIO further assesses that Beijing calibrated its influence efforts to avoid blowback.

Other Actors

A range of additional foreign actors took some steps to attempt to influence the election. In general, we assess that they were smaller in scale than those conducted by Russia and Iran.

We assess that Hizballah Secretary General Hassan Nasrallah supported efforts to undermine former President Trump in the 2020 US election. Nasrallah probably saw this as a low-cost means to mitigate the risk of a regional conflict while Lebanon faces political, financial, and public health crises.

We assess Cuba sought to undermine former President Trump's electoral prospects by pushing anti-Republican and pro-Democrat narratives to the Latin American community. Cuban intelligence probably conducted some low-level activities in support of this effort.

The Venezuelan regime of Nicolas Maduro had an adversarial relationship with the Trump administration and we assess that Maduro had the intent, though probably not the capability, to try to influence public opinion in the US against the former President. We have no information suggesting that the current or former Venezuelan regimes were involved in attempts to compromise US election infrastructure.

Foreign Cybercriminals Disrupted Some Election Preparation

Profit-motivated cybercriminals disrupted election preparations in some US states with ransomware attacks intended to generate profit. We have no indications that these actors sought to use these attacks to alter election functions or data, nor do we have indications that they were acting on behalf of any government.

- For example, in late October, probably foreign ransomware actors demanded payment from a New York county after encrypting 300 computers and 22 servers on the network with Ragnarok malware that prevented it from connecting to a statewide voter registration system. County officials directed voters who had applied via email for an absentee ballot to call and verify their ballot application had been received and processed.

- We do not know whether cybercriminals specifically targeted election-related networks with profit-making schemes or whether their activity reflected a general targeting of state and local government networks that also happen to host election-related processes.

- We assess foreign cybercriminals probably did not work to interfere or influence the US elections on behalf of or at the direction of a nation state. We have low confidence in this assessment. We assess that some cybercrime groups probably operate with at least the tacit approval of their nation state hosts.

Foreign Hacktivists

The IC tracked a handful of unsuccessful hacktivist attempts to influence or interfere in the 2020 US elections.

- In November, hackers promoting Turkish nationalist themes breached and defaced a website previously established for a candidate in the US presidential campaign, according to US cybersecurity press.

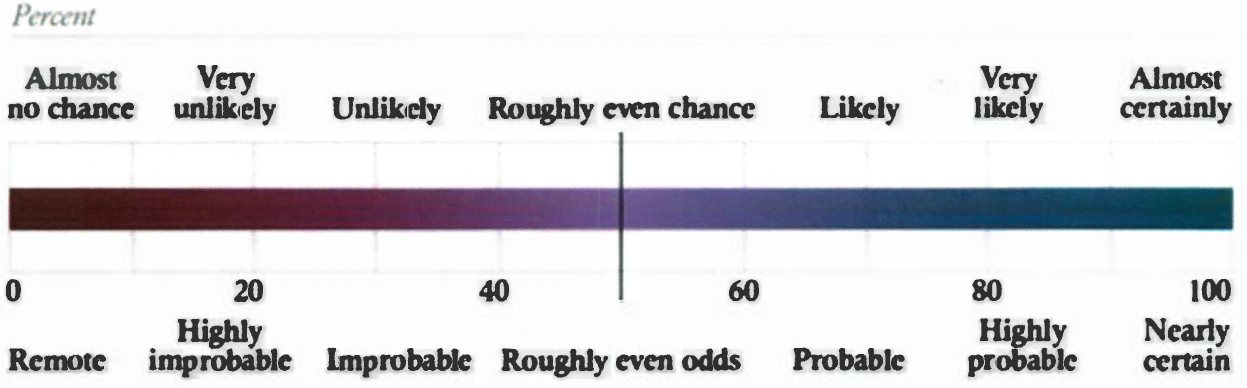
- In October, a hacker briefly defaced a presidential campaign website after gaining access probably using administrative credentials.

Estimative Language

Estimative language consists of two elements: judgment about the likelihood of developments or events occurring and levels of confidence in the sources and analytic reasoning supporting the judgments. Judgments are not intended to imply that we have proof that shows something to be a fact. Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation ,and precedents.

Judgments of Likelihood

The chart below approximates how judgments of likelihood correlate with percentages. Unless otherwise stated, the Intelligence Community's judgments are not derived via statistical analysis. Phrases such as "we judge" and "we assess"—and terms such as "probably" and "likely"—convey analytical assessments.



Confidence in our Judgments

Confidence levels provide assessments of timeliness, consistency, and extent of intelligence and open source reporting that supports judgements. They also take into account the analytic argumentation, the depth of relevant expertise, the degree to which assumptions underlie analysis, and the scope of information gaps.

We ascribe high, moderate, or low confidence to assessments:

- **High confidence** generally indicates that judgments are based on sound analytic argumentation and high-quality consistent reporting from multiple sources, including clandestinely obtained documents, clandestine and open source reporting, and in-depth expertise; it also indicates that we have few intelligence gaps, have few assumptions underlying the analytic line, have found potential for deception to be low, and have examined long-standing analytic judgements held by the IC and considered alternatives. For most intelligence topics, it will not be appropriate to claim high confidence for judgements that forecast out a number of years. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong even though we have a higher degree of certainty that they are accurate.

- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. There may, for example, be information that cuts in a different direction. We have in-depth expertise on the topic, but we may acknowledge assumptions that underlie our analysis and some information gaps; there may be minor analytic differences within the IC, as well as moderate potential for deception.

- **Low confidence** generally means that the information's credibility and/or plausibility is uncertain; that the inforation is fragmented, dated, or poorly corroborated; or that reliability of the sources is questionable. There may be analytic differences within the IC, several significant information gaps,high potential for deception or numerous assumptions that must be made to draw analytic conclusions. In the case of low confidence, we are forced to use current data to project out in time, making a higher level of confidence impossible.