UNCLASSIFIED//~~FOUO~~

ICA

INTELLIGENCE COMMUNITY ASSESSMENT

(U) Cyber Threats to the 2016 US Presidential Election

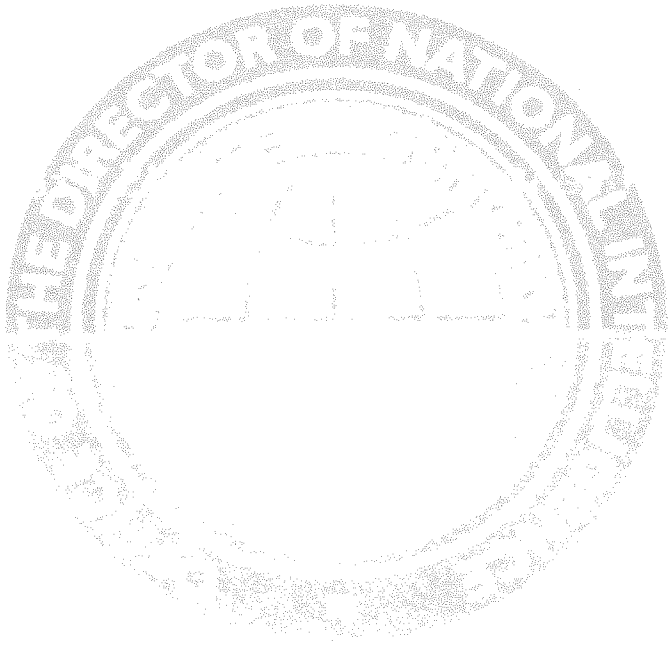
ICA 2016-37D | 16 September 2016

(U) This is an IC-coordinated Assessment.

UNCLASSIFIED//~~FOUO~~

INTELLIGENCE COMMUNITY ASSESSMENT

(U) This Intelligence Community Assessment was prepared for the National Intelligence Council under the auspices of the National Intelligence Officer (NIO) for Cyber Issues.



(U) Cyber Threats to the 2016 US Presidential Election

ICA 2016-37D
16 September 2016

(U) Key Insights

(U/~~FOUO~~) We have no indication that foreign adversaries are planning to manipulate or sabotage computer-enabled US election infrastructure at this time.

(U/~~FOUO~~) Foreign adversaries do not have and will probably not obtain the capabilities to successfully execute widespread and undetected cyber attacks on the diverse set of information technologies and infrastructures used to support the November 2016 US presidential election. This is not because adversaries lack considerable capabilities, but because the US electoral process is a highly decentralized, procedurally and technologically diverse activity and because the will of the voting public is itself dynamic, shifting up to the day of the election. These factors would make it difficult, although not impossible, for even highly capable adversaries to execute a widespread and undetected cyber attack.

(U/~~FOUO~~) The most likely cyber threat to the election may come from low-level, detectable, cyber intrusions and attacks that cause localized disruption but do not threaten the overall functionality of the election services or infrastructures. Nonetheless, even the perception that such low-level intrusions and attacks have occurred risks undermining public confidence in the legitimacy of the electoral process, the validity of the election's outcome, and the mandate of the winning candidate.

(U/~~FOUO~~) Russia, China, Iran, and North Korea can execute a variety of disruptive cyber attacks, including data corruption, distributed denial of service, and even data modification on some election infrastructure. Depending on the adversaries' level of access and the targeted system's vulnerabilities, some nation states and non-state actors could probably corrupt or deny many online election services and systems. Adversaries might also target the most contested or decisive locales and voting blocs in order to maximize the psychological impact of cyber attacks.

(U/~~FOUO~~) Despite the diverse nature of the computer-enabled US election infrastructure and the difficulties associated with anticipating decisive tipping points in advance—in cases where an election is decided by a few closely contested areas that also employ vulnerable technologies—**a targeted cyber attack on decisive locations might have significant impact on public confidence in the election or even potentially alter the apparent outcome.** Although we understand this scenario is unlikely, it remains a possibility that cannot be discounted.

(U) Contents

(U) Discussion

(U) Annexes

(U) Scope Note

(U) Information available as of 8 September 2016 was used in the preparation of this product. This ICA addresses the period between 8 September 2016 and 9 November 2016. Judgments might be revised during this timeframe if our understanding of adversaries' capabilities and intentions significantly change.

(U) Scope

(U//~~FOUO~~) This ICA assesses the threat of cyber attacks conducted by foreign actors against the 2016 US Presidential election process.

- (U//~~FOUO~~) This ICA does not provide a comprehensive overview of all cyber-enabled efforts to influence US or foreign voter perceptions nor does it assess potential objectives of specific foreign adversaries.

(U//~~FOUO~~) We lack detailed insight into the technical configurations, security practices, and network architecture of election information technologies (IT) and infrastructures across the United States, and base our understanding of them largely on meetings with subject matter experts and open source reporting.

(U) Assumptions

- (U) The cybersecurity of IT systems used in the 2016 presidential election will be at best comparable to the security of federal government IT systems.
- (U) No responsible entity will make any significant change that affects the connectivity of the domestic Internet infrastructure and the global Internet.
- (U) US policy regarding responses to cyber attack will not significantly change.

(U) Estimative Language

(U) Estimates of Likelihood convey judgments about the probability of developments or events. Confidence Levels provide assessments on the quality and quantity of source information. Annex A (Estimative Language) elaborates on these terms. We have "moderate confidence" in all judgments except as otherwise noted.

(U) Cyber Threats to the 2016 US Presidential Election

(U) Discussion

(U//~~FOUO~~) We have no indication that foreign adversaries are planning to manipulate or sabotage computer-enabled US election infrastructure at this time.

- (U//~~FOUO~~) Although many adversaries are capable of detectable, disruptive cyber attacks against computer-enabled US election infrastructure, **it is most likely beyond the means of our adversaries to use cyber attacks to affect a covert and widespread shift of the recorded votes to decisively favor a particular candidate during the 2016 US presidential election.** This is not because adversaries lack considerable capabilities, but because the US electoral process is a highly decentralized, procedurally and technologically diverse activity and because the will of the voting public is itself dynamic, shifting up to the day of the election. These factors would make it difficult, although not impossible, for even highly capable adversaries to identify and target enough ultimately decisive critical nodes.

(U//~~FOUO~~) Clandestine, Widespread Manipulation of Election Results Likely Beyond Capability of Adversaries

(U//~~FOUO~~) Foreign adversaries do not have and will probably not obtain the capabilities to successfully execute widespread and undetected cyber attacks on the diverse set of information technologies and infrastructures used to support the November 2016 US presidential election.

- (U/[redacted] Experts at a June 2016 conference sponsored by the US Government to analyze cyber threats to e-democracy suggested that **the decentralized nature of the US election system is a potential source of strength.** Although lamenting that the United States lacks centralized standards for its voter registration and voting systems, the experts asserted that the diversity of existing technical solutions, as well as the decentralized nature of the systems and the election process, create resilience. No single technical solution has been adopted across the entire country; instead, approaches differ widely across different localities, even within states, resulting in decentralized voting procedures and a variety of machines. **As a result, the potential impact of system-specific cyber exploits would probably be limited, and an adversary would need to compromise multiple systems in multiple locations to alter outcomes in a national election, increasing the likelihood of detection.**

- (U//~~FOUO~~) These experts further concluded that **data from legitimate elections generally exhibits statistical characteristics that can be measured against other elections, enabling detection of fraud in the weeks following an election.** Anomalous voting behavior is not always an indicator of fraud, and hiding some signatures of fraud is possible if the fraudster is aware of the signatures in question. However, experts believed that it would be difficult to conceal the full range of anomalies that a large-scale manipulation of votes would generate.

- (U//~~FOUO~~) Cyber operations against electronic voting machines, particularly those that do not provide a paper record of individual votes for auditing purposes, would be the most effective way to manipulate the votes without being detected, according to research by other academic and industry experts. These systems are usually not connected directly to the Internet, however, and to affect them would require physical access, supply chain compromise, or insider-enabled operations. The resource-intensive nature of such operations would make them difficult to conduct on a large scale.

- **(U//~~FOUO~~) System diversity and existing safeguards would likely prevent the undetected manipulation of election results, according to DHS. However, multiple technical pathways exist to undermine public confidence in the electoral process.**

(U//~~FOUO~~) Low-Level, Detectable Attacks Pose Most Likely Threat

(U//~~FOUO~~) The most likely cyber threat to the election may come from low-level, detectable, cyber intrusions and attacks that cause localized disruption but do not threaten the overall functionality of the election services or infrastructures. Nonetheless, even the perception that such low-level intrusions and attacks have occurred risks undermining public confidence in the legitimacy of the electoral process, the validity of the election's outcome, and the mandate of the winning candidate. **Foreign adversaries are more likely to focus election-related cyber operations on undermining the credibility of the electoral process than on clandestinely manipulating the vote outcome through cyber means.**

- (U//~~FOUO~~) Adversaries interested in decreasing voter confidence might be encouraged by the open questioning of the cybersecurity of the upcoming US election, based on numerous news and editorial reports in major media outlets globally since summer 2016. Growing public concern over the vulnerabilities of the US election systems would probably feed potentially sensationalized coverage of even local, low-level cyber attacks. This could enhance the impact of even low-level intrusions that are detected and publicized.

- (U//~~FOUO~~) Cyber activists may attempt disruptive cyber attacks, such as distributed denial of service (DDoS) attacks or web defacements, in the lead-up to and potentially during periods of vote processing.

- (U//~~FOUO~~) Even without linkage to any plan or intent to disrupt an election—criminals will continue to use cyber means to steal voter registration data, given previous operations targeting bulk personally identifiable information (PII). In addition, in its early stages, criminal compromise might be indistinguishable from an effort to disrupt and might be portrayed as evidence of registrant manipulation even when no manipulation actually occurred.

(U//~~FOUO~~) Targeted Attacks Within the Reach of Many Adversaries

(U//~~FOUO~~) Russia, China, Iran, and North Korea can execute a variety of disruptive cyber attacks, including data corruption, distributed denial of service, and even data modification on some election infrastructure. Almost all current and potential cyber adversaries—nations, criminal groups, terrorists, and individual hackers—now have a range of capabilities to exploit and, in some cases, attack unclassified US information systems via remote penetration from the Internet.

- (U//~~FOUO~~) US law enforcement organizations are currently analyzing cyber intrusions and attempts into several state election networks. These intrusions suggest there is a risk of additional incidents.

- (U//~~FOUO~~) Historically, Russia, China, Iran, and North Korea have been able to compromise a wide variety of the Internet-connected networks, despite US cybersecurity efforts. Because we assume that the cybersecurity of IT systems to be used for the 2016 election is at best comparable to the cybersecurity of federal networks, our adversaries probably could corrupt or deny many online election services and systems with sufficient preparation and system access.

- (U//~~FOUO~~) Despite the diverse nature of the computer-enabled US election infrastructure and the difficulties associated with anticipating decisive tipping points in advance—in cases where an election is decided by a few closely contested areas that also employ vulnerable technologies—**a targeted cyber attack on these locations might have significant impact on public confidence in the election or even potentially alter the apparent outcome.** Although we understand this scenario is unlikely, it remains a possibility that cannot be discounted.

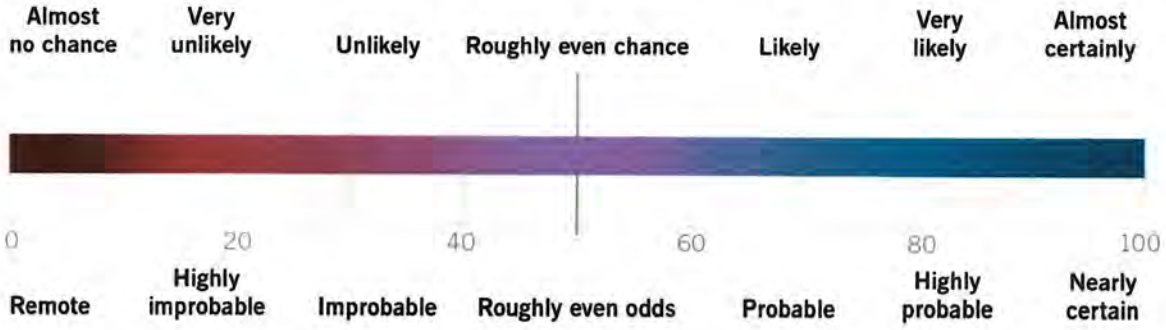
(U) Annex A

(U) ESTIMATIVE LANGUAGE

(U) Estimative language consists of two elements: judgments 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.

(U) **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 "probable" and "likely"—convey analytical assessments.

Percent



(U) **Confidence in the Sources Supporting Judgments.** Confidence levels provide assessments of the quality and quantity of the source information that supports judgments. Consequently, we ascribe high, moderate, or low levels of confidence to assessments:

- (U) **High confidence** generally indicates that judgments are based on high-quality information from multiple sources. High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong.
- (U) **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.
- (U) **Low confidence** generally means that the information's credibility and/or plausibility is uncertain, that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that reliability of the sources is questionable.

(U) National Intelligence Council

The National Intelligence Council manages the Intelligence Community's estimative process, incorporating the best available expertise inside and outside the government. It reports to the Director of National Intelligence in his capacity as head of the US Intelligence Community and speaks authoritatively on substantive issues for the Community as a whole.

NIC Leadership

(b)(3), (b)(6)

[redacted]

National Intelligence Officers

(b)(3), (b)(6)

[redacted]

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO