Capacity to Address Natural and Man-Made Vulnerabilities: The Administrative Structure of U.S. Election System Security

Mitchell Brown, Lindsey Forson, Kathleen Hale, Robert Smith, and Ryan D. Williamson

ABSTRACT

This article examines the efforts of American state election offices to address election emergency preparedness including contingency planning and cybersecurity planning. The election infrastructure that supports election security is cataloged to reflect the networked nature of American public service and the characteristics of American federalism. Public data are collected to identify functions of state offices in providing training, resources, and direct assistance to local election administrators for contingency planning and cybersecurity preparedness. Relationships between state efforts regarding election contingency planning generally and cybersecurity planning are compared. We find significant relationships that suggest a strong institutional foundation predictive of enhanced capacity to address election security issues and degraded environments more broadly.

Keywords: elections, election administration, election emergency preparedness, election sciences, election security, networks, degraded environments, cybersecurity, contingency planning, DHS

INTRODUCTION

ELECTIONS ARE CRITICAL TO DEMOCRACIES, and probably at no other time have election administration systems been more important as they grapple with attacks and crises that challenge electoral integrity as well as face public scrutiny. The crises and attacks come from a combination of natural disasters and intelligent attacks. The 9/11 terrorist attacks on America in 2001 disrupted a primary election in New York City (Nagourney 2001). Out-

side the U.S., the information technology director of the Kenyan election system was kidnapped, tortured, and killed in an attempt to influence the outcome of the 2017 Kenyan presidential election (Odula 2017). In 2014, Russia launched a series of attacks designed to disrupt the Ukrainian presidential election (Watkins 2017). Hurricane Sandy prompted emergency voting measures in New Jersey and New York for the 2012 presidential primary election (Kaplan 2013). In 2016, Russian hackers again attempted to disrupt election operations by targeting state central voter files and local voter registration lists in the U.S. presidential election (Sanger and Edmundson 2019). In the fall of 2018, Hurricane Florence disrupted voter registration and early voting in North Carolina, and Hurricane Michael did the same in parts of Florida and Georgia (Slack 2018).

In the spring of 2020, governors and state chief election officials postponed primary and runoff elections and shifted voting processes in reaction to the worldwide COVID-19 pandemic and its

Mitchell Brown is a professor in the Department of Political Science at Auburn University in Auburn, Alabama, USA. Lindsey Forson is the cybersecurity program manager at the National Association of Secretaries of State in Washington, DC, USA. Kathleen Hale is professor in the Department of Political Science at Auburn University in Auburn, Alabama, USA. Robert Smith is the associate vice president for research at the National Intelligence University in Bethesda, Maryland, USA. Ryan D. Williamson is an assistant professor in the Department of Political Science at Auburn University in Auburn, Alabama, USA.

outbreak across the United States (Corasaniti and Saul 2020). The Democratic National Convention was postponed and the safety of voters and poll workers quickly rose on the national agenda, as did proposals for expansion of vote-by-mail and other methods of non-face-to-face voting and registration. The Department of Homeland Security (DHS) announced a new initiative to examine its mission, relationships, policy activities, resources, and internal operations, among other dimensions, in order to evaluate its role and activities in protecting the nation's critical infrastructure in degraded environments that could result from threats to cybersecurity, COVID-19, and future threats (Atlantic Council 2020). Guidelines and recommendations for electoral activities were issued by the International Foundation for Electoral Systems that include risk mitigation practices for in-person voter registration and election activities (2020).

Regardless of *how* election systems are disrupted, plans must be in place to address these problems. Quality management requires the development of operational contingency planning with a focus on security to face degraded election environments and to ensure seamless responses.

This article examines American state election offices' election emergency preparedness and security efforts, including contingency planning and cybersecurity planning. Election security exists within U.S. election systems and within the broader intergovernmental context of American federalism, which are characterized by several distinct features. One is the dual constitutional imperative that vests the power to conduct elections in both the states and the national government. National administrative authority in this area is essentially advisory, and state or local cooperation is largely voluntary outside voter registration administration (unless it is the consequence of judicial action). Another dimension of the American election context is the degree of authority invested in the nation's approximately 8,000 local election jurisdictions (counties and townships); American elections have been conducted at the local level from pre-Colonial times and that remains the case.¹ Local implementation (and particularly the exercise of local administrative discretion) contributed to exclusionary practices that led to federal oversight to protect the equal rights of voters. Additionally, political, economic, regional, cultural, and demographic variations across the population influence state policy cultures (see Elazar

1966 as foundational scholarship), creating numerous points of influence in the design and implementation of any public policy.

With these features in mind, we conduct an analysis of state activities to support election emergency preparedness and security. This is guided by two focusing questions. What are the emergent policy safeguards and operational contingencies for natural and man-made disasters and attacks? Have states engaged in these and how might responses at the state level vary? This study is the first of its kind to systematically describe the current state of emergency preparedness and security in American elections. In mapping and analyzing the foundational institutional context of election emergency security, we find a strong institutional foundation grounded in significant relationships between all levels of government, nonprofit groups, and the private commercial sector. These relationships illustrate the iterative nature of capacity building in public service and demonstrate the ability to develop the further capacity to address election security issues, emergencies, and degraded environments more broadly. This work also contributes to the broader comparative literature on electoral management, cybersecurity, and preparedness. While we do not necessarily delve into the comparative literature in this piece, we do provide a framework for analyzing election emergency preparedness and security that can be adopted in other contexts.

UNITED STATES ELECTION ADMINISTRATION SYSTEMS

The architecture of American elections is essentially a collection of systems. American elections are conducted through the interaction of all levels of U.S. government—federal, state, and local—in a complex intergovernmental dynamic characterized by complexity, interdependence, diffuse responsibility, coordination, and vulnerability (Hale, Montjoy, and Brown 2015; Hale and Slaton

¹In what follows, we acknowledge the limitations of using state level measures, given that elections are conducted at the local level. However, there is no census of local election offices and no national information about local office operations or effectiveness. Therefore, state-level measures are currently the best available proxy and have relevance given the relationships between local election operations and state offices.

2008). National election laws promote access and participation; e.g., the Voting Rights Act of 1965 and its amendments (VRA), the National Voter Registration Act (NVRA), the Americans with Disabilities Act (ADA), and the Help America Vote Act (HAVA). These national policies, and particularly the NVRA and HAVA, underpin the somewhat systematic role of state election offices, which is now focused primarily on establishing and maintaining electronic voter registration lists. By fiat of national and state constitutions, however, American elections remain entrenched in local governments; more than 8,000 counties, townships, and cities are responsible for administering elections within a web of myriad requirements that vary from state to state.

The earliest systematic studies of U.S. election administration demonstrated that this heterogeneous collection of systems and subsystems evolved from path dependent processes tied in many places to culture related to either colonization or the expansion and creation of new states (Ewald 2009; Harris 1928; 1934; Keyssar 2000). More broadly, beyond elections particularly, the U.S. political system is also characterized by pluralism and an intrinsic private sector role fueled by devolution. One of the tradeoffs for broad access to information and unrestricted access to the electorate in liberal democracies is that it facilitates the ability of other nations to play a role in U.S. elections. The administrative principle of transparency coupled with freedom of the press and open information exchanges mean that bad actors, if they so choose, have readily available information about the technology, processes, and many safeguards in place that support the U.S. electoral system, making it potentially more vulnerable to tampering.

The study of the science of administration has much to offer in understanding what is happening in the election administration contingency planning arena. A defining characteristic of American intergovernmental relationships is the limited ability of the national government to control subnational governments. Election security policy is not a matter of simply having the federal government tell states and localities what to do—constitutional imperatives structure this differently. The decentralized nature of the environment is compounded by myriad non-profit and for-profit organizations intertwined with the government in a network of relationships that is essential to government functioning.²

The governance mandates that support American intergovernmental organizational arrangements are important because they indicate the types of communication needed to produce compliance or alignment with common goals. Hierarchies rely relatively efficiently on command and control structures, centralized authority, and rules promulgated to align activities in a particular direction toward particular results (e.g., Goggin et al. 1980; O'Toole 1988). In the election administration environment, however, the public policy design and public administration literature suggest the need for institutional tools and mechanisms that facilitate information exchanges and a variety of methods of generating, synthesizing, and disseminating information (Hale 2011; Montjoy and O'Toole 1979; O'Toole 1988). These information processes reflect an evolving understanding of the role of networks in public service. Public sector capacity is critically dependent on the ability of networks of organizations to develop information about conditions and how to address them, circulate information among the relevant networks, vet the information through dialogue, and produce policy documents. Examples of these types of information include position papers, descriptions of issues, definitions of policy problems and conditions of positive or negative change, and guidance tools such as training, manuals, model programs, best practices, and standard operating procedures.

The contingency planning environment is characterized by interdependent network arrangements of public and private actors and the concepts of shared risk (Birkland 2006; 2015; Comfort 2012; Comfort, Boin and Demchak 2010), and has influenced the institutional architecture of American election security. That architecture evolved through two disparate national policy responses. First is the response to the 2000 presidential election and second is the response to the terrorist attacks of 9/11 in 2001. The 2000 presidential election generated new intergovernmental arrangements between localities and states through the HAVA, which increased the power of state election offices through requirements to develop plans to convert the nation to electronic voting systems and to create statewide electronic voter registration databases. State chief election officers (CEOs), established nearly a

²For more on the use of network theory in electoral management, see James (2020).

decade earlier under NVRA, gained new authority and responsibilities, and increased their presence with local election jurisdictions.

One consequence of 9/11 was the creation of the Department of Homeland Security, a new federal agency that subsumed a host of other agencies and created new organizational arrangements designed to integrate national security and law enforcement responsibilities across localities and states, as well as across the country. Both events fostered public policies structured around these new organizational arrangements, new relationships, and norms of formal and informal information exchange. Today's institutional architecture and organizational relationships in the election security arena are the legacy of those events. Moreover, all of these interrelationships and activities reside alongside the nation's natural disaster planning structures, both in the U.S. and around the world (see, e.g., Comfort 2012; Comfort, Waugh and Cigler 2012).

Organizations such as Information Sharing and Analysis Centers (ISACs), established as an outgrowth of the federal government response to 9/11, are critical for security information exchanges. Voluntary nonprofit membership organizations such as the Election Center bring people together at conferences and in training sessions to synthesize information from multiple sources and serve as a place for information to be vetted for networked learning (see Hale 2011 for a detailed discussion of the application in criminal justice innovation). ISACs, which predate widespread concern in the election administration cyber environment, have aided in the election administration community in terms of contingency planning for cyberattacks by providing a model for creating similar infrastructure.

tions in this complex space orient themselves to coordinate and collaborate with other necessary actors, and do they have the capacity to do so?

Public organizations choose different methods of coping with the environmental uncertainty that occurs when hierarchies and contracts provide only loose ties.³ Most recently, research about the networked environment of all public service operations indicate that methods of information exchange and the synthesized packaging of information as best practices, models programs, unique organizational collaborations, and systematic research are all critical in developing and sustaining capacity to meet current challenges and to develop capacity for the future (Agranoff 2017; Hale 2011). Together, these theories argue that we consider an array of possibilities in exploring contingency planning writ large and the related ability to respond to emergent conditions. When facing uncertain contextual conditions in running elections, governments will most successfully move beyond these to develop new coping mechanisms (either in advance or in the moment) when their agents are able to share information and resources across and within levels of government as well as outside of government, and are interested and engaged in problem solving. Contrasting this, governments will be less likely to rapidly respond when its agents are siloed, under-resourced, and committed to deontological adherence to standard operating procedures. Successful responses require advance planning and exercises to practice; successful responses also require careful networking and information sharing, as well as some autonomy and flexibility not typical of many government procedures.

CURRENT EFFORTS, ISSUES, AND VULNERABILITIES

In identifying areas of vulnerability within the election administration system we merge our understanding of system complexity with what we know about how public administration processes work. The central organizing question for emergency preparedness and contingency planning in election operations is: how do organizations attempt to plan for, mitigate, and operate in degraded environments as a consequence of intelligent action or natural disaster? Framed more generally, how do organiza-

METHODS

This article is part of a project that began in January of 2016 with the aim of understanding contingency planning for degraded environments in

³Theories abound and include boundary spanning (Thompson 1967); cooptation (Selznick 1948, 1949); borrowed strength (Manna 2006); resource dependency (Callen, Klein, and Tinkelman 2010; Kreutzer 2009; Miller 2002; Miller-Milleson 2003); information synthesis, or the flow of information between government and nongovernmental actors in trusted relationships (Hale 2011; O'Toole 1997); stakeholder theory (Brown 2002); and contingent governance (Ostrower and Stone 2009).

election administration. However, after executive branch decisions were made about critical infrastructure in January of 2017, our research expanded into the area of cybersecurity. From there we began employing various methods to construct the data presented in this manuscript. We engaged in archival reviews (state, local, and federal government websites, and state and local materials not necessarily included on websites, e.g., COOPs), observational study of election offices and meetings, and unstructured interviews with election officials. This process spanned the period of January 2016 through August 2019. Given the uniqueness of this rapidly evolving environment and the accompanying lack of existing data, we were unable to emulate existing frameworks outlined in previous works. We then engaged in a process of pattern matching of the qualitative data, and mapping processes and relationships in order to characterize the environment. Each of these approaches is consistent for environmental scans of emerging government and policy areas.

DATA

Table 1 displays an array of potential points of vulnerability in the U.S. election system that could arise as a consequence of intelligent or natural disaster.⁴ The first column presents the major components of the election administration system and processes in an order that corresponds generally to the election process, as well as the major categories of actors involved. The second, third, and fourth columns present points of vulnerability by disaster type. Demarcations of check marks denote vulnerability potential and are not evidence that threats have occurred (although clearly some have). There may be some exceptions to what is presented; the purpose is to capture general concerns across states and jurisdictions.

Broadly speaking, we observe that disasters come in two major forms—intelligent and natural—and that responses require some form of coordinated action (see, e.g., Brabant 2000; Quarantelli 1991; Russ 2014). Intelligent disasters can be classified as non-violent, violent, and government interference. Non-violent intelligent disasters usually involve some form of cyber disruption including drone use. Violent intelligent disasters can include drone use, other military or quasi-military operations (gendarme,

TABLE 1. POSSIBLE POINTS OF VULNERABILITY IN THE AMERICAN ELECTION SYSTEM

<i>Election system elements and actors</i>	<i>Intelligent disaster</i>		
	<i>Cyber attack</i>	<i>Physical attack</i>	<i>Natural disaster</i>
Registration			
State gov't	✓		
Local gov't	✓		
Vendors			
Third parties			
GOTV			
Local gov't		✓	✓
Candidates	✓		
Parties	✓		
Media	✓		
Third parties			
Ballot creation			
(State gov't)			
Local gov't	✓	✓	✓
Vendors		✓	✓
Candidates			
Ballot delivery			
Local gov't	✓	✓	✓
USPS		✓	✓
Vendors	✓	✓	✓
Ballot marking			
Voter		✓	✓
Ballot return			
Voter		✓	✓
Local gov't		✓	✓
USPS		✓	✓
Vendors			
Ballot counting			
Local gov't	✓	✓	✓
Vendors	✓	✓	
Reporting			
Local gov't	✓		
State gov't	✓		
Media	✓		
Certification & audit			
Local gov't		✓	
State gov't		✓	

paramilitary, etc.), or terrorism. Government interference that produces disaster conditions is predicated on the use of government power to disrupt normal services or operations in such an extreme way that it produces a humanitarian crisis in the state.

⁴This is an adaptation of the major elements of the electoral system (Hale, Montjoy, Brown 2015, 3) with an overlay of an analysis of areas where risk from degraded environments would be most impactful on the integrity of elections. The result is a synthesis of federal agencies such as CISA and analysis of existing COOPs at the state and local level (Hale and Brown 2020, 166).

Government-sponsored genocide could be one example.

Natural disasters can be grouped as forecasted, unforecasted, and epidemics. Forecasted natural disasters include events that meteorologists can (typically) anticipate; e.g., hurricanes, major snowfall, or ice emergencies. Forecasts allow organizations to prepare and pre-position material or personnel in anticipation of need. Non-forecasted natural disasters are more nuanced. It can be challenging to determine whether, when, and where storms may produce tornadoes or flooding that damage infrastructure or present lethal conditions. Superstorm Sandy and Hurricanes Katrina, Florence, and Michael are examples. Similarly, as the 2020 COVID-19 epidemic demonstrated, predicting the effect of epidemics remains imperfect; epidemiologists have improved understanding of the spread of disease, but cannot predict an initial outbreak. We expect similarities and differences in strategies by types of degradation, notably natural disaster versus cyber warfare, drones, military action, or terrorism (see, e.g., Glaser 2005; Herzog 2011; Kent 2011; Mitchell 2006; Perito 2007). Although not all of the possible degraded environments are anticipated in the U.S. context, we include them in our discussion about election vulnerabilities generally.

No election administration subsystem is independently and fully secure, as Table 1 demonstrates. Vulnerabilities exist across all components of the election subsystems and actors (Defending Digital Democracy Project 2018). In election systems, voter registration and the process of reporting results appear uniquely vulnerable to cyberattack. Although these systems were originally paper-based and static, federal law now requires electronic voter registration databases, and states and vendors have chosen to create various electronic options for collecting and reporting results. These systems are accessible online and centralized at the state level, either in whole or in part, and in some cases, information is stored only electronically. In contrast, ballot marking and ballot return are most vulnerable to physical threats. In these subsystems, components tend to have less internet exposure and are more distributed. This reduces, though does not eliminate, the risk of a large-scale cyber attack. The tangible nature of components in these subsystems makes them among the most vulnerable to physical attack. There also exist existential vulnerabilities across involved parties (e.g., vendors, local offices, state offices, and so on).

Environmental scan of the U.S. election security landscape

For the election community, contingency planning for natural and intelligent disasters is not new. Federal agencies like the Election Assistance Commission (EAC) and national professional associations like the Election Center have long provided materials and training on best practices for planning and positive responses. Since 2016, this focus has shifted from degraded environments generally to security concerns more specifically. During the 2016 presidential election cycle, the DHS and the Federal Bureau of Investigation (FBI) began working with targeted states and localities about possible cybersecurity threats. The unique nature of the election administration environment dictated that initial support would be nascent. In January 2017, the Obama administration designated election operations as critical infrastructure under the auspices of the DHS. This prompted two diametrically opposed reactions from politicians and election administrators: some favored the designation and sought additional support, while others feared national government overreach and the potential for additional problems caused by the designation.

Since that time, the DHS has worked closely with professional associations of election officials, state election directors, and representatives from some local election jurisdictions to better understand and assist the diverse election administration systems across the country. There is no clear threat analysis that can be applied nationally, but national infrastructure has been created to assist election administrators, including (but not limited to) the Information Sharing and Analysis Centers (ISACs), its replication in the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and related Election Infrastructure Subsector Government Coordinating Council (EIS-GCC). Guidance has been developed for activities such as system assessments and defense strategies (Defending Digital Democracy Project 2018). Terms such as network penetration testing, threat vectors, and Certified Information Systems Security Professional (CISSP) have entered the election administration vocabulary. Some state associations and state government entities provide guidance and training in election security, including cyber and other forms of contingency planning. As a consequence of the \$380 million and \$425 million included in the Consolidated Appropriations Acts

of 2018 and 2020, respectively, all of the states will be enhancing their security protocols and training moving forward.

Against this background, we identify the network of organizations and actors engaged in election administration contingency and security initiatives, focusing on the national government and the states. Both government and nongovernmental actors are included, consistent with the cross-sectoral structure of election subsystems and the networked structure of public service provision. We looked for organizational architecture and activities known to enhance public sector capacity such as information exchange, training, and member participation across organizations and in election administration, specifically (Hale 2011; Hale and Brown 2013; Hale and Brown 2016). Information was collected from websites of government offices and nongovernmental organizations, and popular media sources.

First, consistent with previous works (Garnett 2017, 2019; King and Youngblood 2016), we conducted an Internet search to identify relevant federal government and national nongovernmental organizations and examined recent conference programs where election security and cybersecurity were featured. We next explored the website of each organization and summarized their roles in this arena before then searching state election websites for relevant information on what states are doing to guide and train election administrators in their states. We also looked to popular media sources for public statements made by state election officials.⁵ Our coding scheme is reflected in the categories displayed in the tables. Although the categories follow a general order, they provide imperfect ordinal measures. For example, a public statement may also be indicative of other relevant efforts that are not publicly apparent. To capture intergovernmental coordination efforts, we noted the state governments that are represented on the EIS-GCC that examines elections as critical infrastructure. Next, we explored relevant state laws and legislation to learn the role of state legislatures. We looked at broader state government efforts to develop continuity of operations plans (COOPs) and related guidance that may become relevant to election administrators during a crisis. We conducted preliminary bivariate data analyses to determine whether and how these state measures correlate with each other.

Table 2 summarizes a point in time view (August 2018) of the national institutional environment in

election security, including government agencies and nongovernmental organizations providing guidance, training, best practices, and similar integrative information on contingency planning, cybersecurity, and voting system security.⁶ These organizations range across government offices and third-party groups, including nonprofit professional associations and, in the case of the ISACs, collaborations with private sector organizations. The categories of activity are not discrete but suggest areas of relative focus supported by the literature that we can use to understand the efforts underway across the rapidly evolving organizational landscape. The following sections describe more fully the roles of these organizations.

Federal government organizations

Department of Homeland Security. The Department of Homeland Security is the federal executive department tasked with the mission “to secure the nation from the many threats we face.” DHS connects with election emergency management and contingency planning in two ways. Its most well-established role depends upon the work of the Federal Emergency Management Agency (FEMA).⁷ FEMA focuses on disaster planning and relief to provide federal natural disaster assistance to state and local governments in the event of a

⁵One might contend that election offices would not post certain security-related information online in an attempt to further prevent any sort of hacking or disruption. Based on personal communication, we acknowledge that has been one approach (personal communications between authors and election officials at regional and national meetings on February 24–26, April 25–26, and August 19–20 of 2019). However, we still think this approach serves as a useful proxy for understanding a jurisdiction’s security environment. First, practically speaking, we can only measure things we can observe, and other works have effectively relied on a similar strategy (Garnett 2017, 2019; King and Youngblood 2016). Second, announcing something like security training is a relatively costless action that sends a signal that a jurisdiction is likely more prepared for an intrusion and not an ideal target for interference.

⁶Though not necessarily exhaustive, this list is a thorough depiction of many of the largest and most prominent organizations engaged in Education, Support, and/or Research of Contingency Planning, Cybersecurity, and Voting System Security for U.S. Elections. We believe this list, as currently constructed, allows us to effectively assess the state of security and contingency planning and training within U.S. elections.

⁷Other agencies housed under the Department of Homeland Security (DHS) administrative umbrella include U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, the U.S. Secret Service, and the Transportation Security Administration.

TABLE 2. PARTICIPATION IN EDUCATION, SUPPORT, AND/OR RESEARCH OF CONTINGENCY PLANNING, CYBERSECURITY, AND VOTING SYSTEM SECURITY FOR U.S. ELECTIONS BY INSTITUTIONAL SECTOR

<i>Institutional sector</i>	<i>Contingency planning</i>	<i>Cybersecurity</i>	<i>Voting system security</i>
Government	DHS DoD EAC	DHS DoD EAC NIST	EAC NIST
Nongovernmental	Auburn Belfer/D3P Election Center Humphrey iGO NASED NASS NCSL	Auburn Belfer/D3P Brennan CAP CDT CIS/ISACs CNS CSG CTCL Election Center Humphrey ICIT iGO NASCIO NASED NASS NCSL NGA R Street	Election Center iGO NASED NASS NCSL
Auburn	Auburn University Graduate Programs in Election Administration		
Belfer/D3P	Defending Digital Democracy Project of the Belfer Center at Harvard University		
Brennan	Brennan Center for Justice at the New York University School of Law		
CAP	Center for American Progress		
CDT	Center for Democracy & Technology		
CIS	Center for Internet Security		
CNS	Center on National Security at Fordham Law School		
CSG	Council of State Governments		
DHS	Department of Homeland Security		
DoD	Department of Defense		
EAC	Election Assistance Commission		
Humphrey	University of Minnesota's Humphrey School of Public Service		
ICIT	Institute for Critical Infrastructure Technology		
iGO	International Association of Government Officials		
ISAC	Information Sharing and Analysis Centers		
NASCIO	National Association of State Chief Information Officers		
NASED	National Association of State Election Directors		
NASS	National Association of Secretaries of State		
NCSL	National Conference of State Legislatures		
NGA	National Governor's Association		
NIST	National Institute of Standards and Technology		

presidential declaration of emergency. FEMA's assistance is both physical and financial. Election administrators may receive assistance or guidance from FEMA during a disaster which is usually delivered from FEMA through state emergency management agencies to other state and local government organizations including election offices.

Beyond FEMA, DHS has a new and evolving role in election security. DHS coordinates with and provides assistance to private and government entities within the critical infrastructure sectors and subsectors, including those involved in election adminis-

tration. DHS assistance is aimed at reducing both cyber and physical risks to election systems and facilities, and includes cyber and physical security advisement, cybersecurity assessments, detection and prevention services, information sharing and awareness, incident response services, and training and career development. Assistance from DHS is voluntary for state and local election officials.

The 2017 critical infrastructure designation led to the establishment of coordinating councils including the EIS-GCC which is composed of federal, state, and local officials, and the Election Infrastructure

Subsector Coordinating Council (EISCC) which includes private election industry providers and non-profit organizations which support elections. DHS provides operational support for the EIS-GCC and EISCC which are mechanisms for collaboration and information sharing related to securing elections. Currently, many state and local election officials, as well as their organizational representatives, are working closely with DHS and taking advantage of federal cybersecurity services.

Federal Bureau of Investigation. The priorities of the FBI include protecting the U.S. against cyber-based attacks and high technology crimes. The FBI is involved in U.S. election security through investigation, including trying to attribute attacks to their source. As part of this role, the FBI shares information learned through investigation with DHS and other federal agencies so DHS can then share information, as permitted according to classification, with election officials.

U.S. Election Assistance Commission. The EAC was established in 2002 through HAVA as an independent bipartisan commission. Its purpose is to support local and state election officials in the mandated transition to electronic voting systems and the development of statewide voter registration databases, to develop voluntary voting system guidelines (VVSG), and to serve as an information clearinghouse. Through these roles, the EAC interacts regularly with local election administrators and state election offices on the entire array of election operation issues.

The EAC clearinghouse function and its promulgation of VVSG relate directly to the contingency planning and security. Through its clearinghouse, the EAC provides resources to election administrators including checklists, videos, webinars, training materials, white papers, and other literature on both election security and election contingency planning, as well as several subtopics—all aimed at helping election administrators address these challenges, train their employees, and educate voters. Commissioners and staff provide training and assistance through conferences, workshops, and summits, and work closely with election administrators and DHS on the implementation of the critical infrastructure designation. In 2018, the EAC assumed a liaison role between state and local election officials and DHS following the critical infrastructure designation, and DHS helped communicate to the

public and assisted election administrators to understand what the designation did and did not mean, and ensured questions and concerns were heard by DHS.

The VVSG include requirements and specifications for voting system testing to ensure they have necessary functionality, accessibility, and security capabilities.⁸ Although states can choose whether to follow VVSG in full, in part, or not at all, the creation of new election system equipment through the private market is largely dependent on adherence to VVSG (Hale and Brown 2013). Therefore, control over the VVSG gives the EAC significant influence over election security requirements for voting technologies. Related, the EAC works closely with the National Institute of Standards and Technology (NIST) to accredit independent laboratories to test for compliance with VVSG.

National Institute of Standards and Technology. NIST is a federal government agency within the U.S. Department of Commerce, created in 1901 as a physical science laboratory to establish an infrastructure of technology, standards, and measurements to support U.S. industrial growth and competitiveness. NIST works with the EAC on laboratory accreditation for VVSG compliance testing and supports other aspects of VVSG. NIST now provides cybersecurity guidance to U.S. industries and has adapted its resources to be specifically pertinent to U.S. election infrastructure. This includes cybersecurity literature, webcasts, standards, and other resources. In 2018, NIST worked to create an extensive cybersecurity framework for U.S. critical infrastructure as it has for other critical infrastructure sectors.

U.S. Department of Defense. The Department of Defense (DOD) oversees the U.S. military and a civilian force of thousands. As part of its overall mission, the DOD deploys Cyber Mission Force teams to defend its networks, systems, and information; the U.S. homeland and national interests; and to support military operational and contingency plans (Maucione 2019). DOD also trains national guard soldiers in cybersecurity skills (Maucione 2019). Several states called on the National Guard to help

⁸The voluntary voting system guidelines (VVSG) first adopted in 2005 increased security requirements for voting systems; the most recent update occurred in 2015.

protect the 2018 midterm elections through risk assessments and surge support for incident response. DOD also provides public resources related to disaster preparedness, cybersecurity, and contingency planning. Finally, the Federal Voting Assistance Program (FVAP), accessible at the FVAP's website, is a DOD program ensuring that service members, their eligible family members, and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so. FVAP, which is focused on remote voting for U.S. citizens located around the world, has conducted research on electronic voting methods, many of which are at the center of cybersecurity concerns.

Nongovernmental organizations

Government support organizations. The Center for Internet Security (CIS) and the Defending Digital Democracy Project (D3P) administered through the Belfer Center at Harvard University are nongovernmental entities that exist to support U.S. government entities in cybersecurity efforts. U.S. election cybersecurity is a major focus of both CIS and D3P. CIS provides cybersecurity best practices to U.S. election administrators. CIS also operates the EI-ISAC which is geared specifically toward providing cybersecurity resources, training products, alerts, and information sharing for election officials throughout the U.S. D3P conducts research and outreach with election administrators on cybersecurity issues and regularly releases cybersecurity resources. D3P has published several "playbooks" geared toward helping election administrators protect election systems from cyber threats and respond to cyber incidents. Through government partnerships with DHS and state governments, D3P also organizes training exercises for election administrators that provide opportunities to practice and evaluate incident response activities.

Another organization that exists to provide resources to government with a different but related mission to the above organizations is the Center for Technology and Civic Life (CTCL). CTCL provides resources and education to election officials to help them improve communication with voters. Among CTCL's resources is an online education series on cybersecurity for election officials which is provided in partnership with the Center for Democracy and Technology (CDT).

Professional associations and intergovernmental organizations. Several professional associations for government officials and employees related to U.S. elections and other intergovernmental organizations provide support to their members. These associations play an important role in intergovernmental coordination related to election cybersecurity between layers and branches of government as well as relevant nongovernmental actors. Professional associations for state and local election officials include the National Association of Election Officials (otherwise referred to as the Election Center), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and the International Association of Government Officials (iGO). Other intergovernmental organizations active in this space include those which represent government officials who support or otherwise work with state and local election officials, including the National Conference of State Legislatures (NCSL), the Council of State Governments (CSG), the National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO).

The purposes of these professional associations and intergovernmental organizations are related but distinct. The Election Center is the only professional association dedicated solely to the professionalization of election administration; the vast majority of its members are local election administrators and voter registrars. iGO is a professional association for all local government officials, including election officials but also including clerks, recorders, and treasurers. NASS and NASED each represent state-level U.S. election officials. NASS represents secretaries of state, most of whom serve as their state's chief election official, from the 50 U.S. states, the District of Columbia, and the U.S. territories. NASED's membership consists of the state election directors from across the U.S., the District of Columbia, and the territories. The member offices of NASS and NASED overlap significantly. However, NASED focuses directly on the election director, who in most cases reports to the state chief election official (who is typically, but not always, the secretary of state) and in some cases is the state chief election official. Together, the memberships of these four organizations encompass nearly every state election official in the U.S. as well as many local election administrators. Their main roles include coordinating information sharing and activities between each other, the

federal government, election vendors, and other relevant intergovernmental actors, as well as providing resources and training opportunities to members. NASS takes up policy positions on behalf of its membership.

The National Conference of State Legislators (NCSL), the National Governors Association (NGA), the National Association of State Chief Information Officers (NASCIO), and the Council of State Governments (CSG) each represent state-level government actors who are not typically election administrators but play some role in elections through legislation, funding, support, or administrative coordination. These groups represent state legislatures, governors, state chief information officers, and all branches of state government, respectively. Each of these organizations has engaged in research and provided information to its members related to election security. These organizations also coordinate state-level training and activities, and share information with other organizations in the election administration network.

Research organizations. Research about cybersecurity in U.S. election administration has increasingly become the focus of a variety of research organizations. Academic think tanks such as the Belfer Center for Science and International Affairs at Harvard University have developed a sharp focus on election cybersecurity as a dimension of technology policy through the efforts of the Defending Digital Democracy Project. The Brennan Center for Justice at the New York University School of Law has long devoted efforts to identifying inequities in the election process and has added cybersecurity issues to their brief. At the Massachusetts Institution of Technology, the Election Data and Science Lab was formed to focus on the systematic study of election data and election sciences, with advice from election administration scholars and election officials. Graduate programs in election administration have been introduced at Auburn University's Department of Political Science, and at the University of Minnesota's Humphrey School of Public Service. Other think tanks engaged in election security research include the Center for American Progress (CAP), the Center on National Security at Fordham Law School, the Institute for Critical Infrastructure Technology, and R Street.

Advocacy organizations. Several advocacy organizations address security issues in elections.

At least two of these (Verified Voting and the National Election Defense Council) have formed around the goal of securing U.S. elections. Other groups engaged in policy advocacy related to election security include nonpartisan organizations as well as those spanning the full range of the political ideological spectrum in the U.S. and include, but are not limited to, the Brennan Center, CDT, Center for Secure and Modern Elections, Protect Democracy, Common Cause, Freedom Works, Americans for Tax Reform, the Electronic Frontier Foundation, and the Electronic Privacy Information Center. Some of the above organizations are engaged in research and outreach related to election cybersecurity in addition to their advocacy roles.

STATE GOVERNMENT ACTIVITIES SUGGESTING CAPACITY TO RESPOND

To determine how states were addressing election security concerns, we conducted an environmental scan of state election offices and state legislatures from August 2017 through August 2018. In our scan, we searched for various indicators of government capacity to address election contingencies and cybersecurity issues. We conducted a review of state election office websites and looked for evidence of contingency planning including formal planning documents known as continuity of operations plans (COOPs), formal planning documents or policy statements pertaining to cybersecurity, and less formal acknowledgments such as best practices or announcements of training. Data about state election office activities and state legislation were collected systematically by the authors from state election office websites at two-week intervals. Documents and other posted information such as designated website sections, newsletters, topical announcements, and public statements by state officials were observed on these websites. The texts of state election statutes were reviewed to determine the level of specificity and coverage of election security activities. The scan did not consider the volume of information per se; rather, states were grouped by the ordinal measures indicated in each table and coded at the highest level observed. These distinctions are noted in the coding reflected in the tables. The cumulative totals for state activity on cybersecurity were noted in March and August 2018. The particulars of data collection for each analysis and findings are summarized below.

TABLE 3. ELECTION CYBERSECURITY AND CONTINGENCY PLANNING GUIDANCE CONDUCTED BY STATE ELECTION OFFICES

State activity	Election guidance topic			
	Number of states	Cybersecurity	Number of states	Contingency planning
Provides resources	16	CA, CO, CT, IN, KY, MD, MN, NJ, NY, OH, PA, RI, VA, WA, WV, WI	17	CA, CO, CT, FL, ID, KY, LA, MA, MN, MT, NE, NJ, TX, VA, WA, WI
Provides information in broad election administration document(s)	7	AK, AZ, IA, NE, NH, NM, TX	11	AZ, IN, IA, MI, MS, NV, NH, NM, OH, PA, SC
Official public statements by state official related to election security	24	AL, DE, FL, GA, HI, ID, IL, LA, ME, MA, MI, MS, MO, MT, NV, NC, ND, OK, OR, SC, SD, TN, UT, VT	6	AR, HI, KS, NY, NC, WV
Nothing found	4	AR, KS, DC, WY	17	AL, AK, DE, DC, GA, IL, ME, MO, ND, OK, OR, RI, SD, TN, UT, VT, WY

Cybersecurity and contingency planning guidance

State election offices vary in the extent to which they provide broad cybersecurity and/or contingency planning support and guidance to election administrators in their states. Table 3 summarizes this variation; a graphic illustration is presented in Figure 1.

From 16 states, we found documents on state election websites demonstrating that the state election office provides cybersecurity guidance or training to election officials. From seven state election offices, we found information on cybersecurity contained in a broad election administration manual or other document. From 24 states, we found state-

ments from a state election official, which suggests the state election office is addressing cybersecurity in some way, but we did not find any published documents demonstrating their specific efforts. There were four states where nothing related to election cybersecurity was found in either state election websites or a search of public statements. The release of cybersecurity resources or statements by state election offices increased in response to national attention, attempted attacks, and federal funding. The number of election cybersecurity-related documents and statements released by state election officials increased each time. We do not contend that this absence of evidence is evidence of absence

FIG. 1. Comparison of election cybersecurity and contingency planning guidance conducted by state election offices by number of states.

TABLE 4. STATE ACTION ON VOTING SYSTEM SECURITY RULES AND GUIDANCE

<i>State activity</i>	<i>Number of states</i>	<i>Voting system security</i>
Election statute contains voting system requirements	11	AR, CO, DE, GA, HI, IN, ND, OR, RI, UT, WY
Provides resources	18	CA, CT, FL, IL, MD, MI, MN, NE, NV, NH, NJ, NY, OH, PA, TX, VA, WA, WI
Provides information in broad election administration document	5	AK, AZ, NH, NY, SC
Official public statements by state official related to election security	7	IA, ME, LA, NC, OK, VT, WY
Nothing found	11	AL, DC, ID, KS, KY, MA, MS, MO, MT, SD, TN

of state guidance. However, a presence indicates an affirmative attempt to address this issue, which can be used as a proxy for capacity, and that presence indicates a particularly relevant dimension of capacity in this policy area. While some might argue that the presence (or absence) of cyber-readiness information should not be shared because it enhances vulnerability, basic public administration principles of transparency suggest that, at a minimum, the public should be able to know that government is aware of, and addressing, these concerns.

State election offices also vary in their election contingency planning efforts. Contingency planning resources provided by state election offices are also captured in Table 3. In multiple states, new or updated resources were produced, or election contingency planning legislation was introduced following a major natural disaster. We found guidance or training documents related to contingency planning from 17 state election offices. From 11 states, we found information related to contingency planning in a broader election administration document. From six states, we found public statements related to efforts in the area of election contingency planning but did not find actual documents. In 17 states we found no information related to contingency planning through the state election websites or a search for public statements.

Voting system security guidance

State governments also provide guidance on the security of voting technology. This is summarized in Table 4 and presented graphically in Figure 2. In this area of election security, 11 states have also enacted laws that address voting system security in addition to providing training and other resources and publicizing the issues.

A slightly larger number of states (18) provide guidance, separate from legal requirements, to election administrators relating specifically to voting system security. Far fewer (5) states provide information about voting system security in a broad manual. In seven states, election officials are on record

FIG. 2. State actions on voting system security rules and guidance.

TABLE 5. STATE LEGISLATIVE ACTIVITY RELATED TO CYBERSECURITY AND CONTINGENCY PLANNING

State activity	Number of states	Cybersecurity	Number of states	Contingency planning
Election statute contains section related to topic	4	CA, IL, IA, TX	9	CT, FL, LA, MD, MN, NY, NC, OK, WA
Election statute mentions topic	11	AZ, CO, IN, LA, MD, MN, MO, NV, NY, ND, WV	18	CA, DE, GA, HI, IN, IA, KS, ME, MO, MT, ND, OH, PA, SD, TX, UT, VA, WI
Legislation introduced related to topic	n/a	n/a	2	KY, VT
Legislation introduced with mention of topic	3	NC, OH, OR	2	CO, NJ
Nothing found	33	AL, AK, AR, CT, DE, DC, FL, GA, HI, ID, KS, KY, ME, MA, MI, MS, MT, NE, NH, NJ, NM, OK, PA, RI, SC, SD, TN, UT, VT, VA, WA, WI, WY	20	AL, AK, AR, AZ, DC, ID, IL, MA, MI, MS, NE, NV, NH, NM, OR, RI, SC, TN, WA, WY

with public statements about voting system security. In more than 20% of states (11), no information was found that related to voting system security.

State involvement on the EIS-GCC indicates intergovernmental coordination occurring in this area. The EIS-GCC exists as a planning and coordination mechanism between all levels of government. Fifteen states had a state government representative on the election subsector critical infrastructure Government Coordinating Council at the time of this article, while 36 states did not. The number of EIS-GCC members and their selection is prescribed by its charter. Some states may have not had the opportunity to become a member of the EIS-GCC. While the absence of state membership does not indicate a state's lack of desire to

participate in the EIS-GCC or in intergovernmental coordination, the states serving on the EIS-GCC are involved in at least some intergovernmental coordination efforts in which other states are not involved.

Legislative activity and laws

States are also active in legislating on cybersecurity and contingency planning in the election area. Legislative activity through August 2018 is summarized in Table 5 and depicted graphically in Figure 3.

Specific statutory provisions pertaining to cybersecurity appear in four states' election statutes. In 11 states, provisions mention election cybersecurity in a broader section of the election statute. Although no states had legislation pending at the time of this

FIG. 3. Comparison of state legislative activity related to cybersecurity and contingency planning.

TABLE 6. CONTINUITY OF OPERATIONS PLANNING ACTIVITY GUIDANCE BY STATE GOVERNMENTS

State activity	Number of states	COOP guidance
Statewide COOP	10	DC, GA, ID, KY, LA, MA, MI, MN, MS, SC
State provides COOP planning resources	40	AK, AZ, AR, CA, CO, CT, DE, FL, HI, ID, IL, IN, IA, KS, KY, MD, MA, MT, NE, NV, NH, NJ, NM, NY, NC, ND, OH, OK, OR, PA, RI, SD, TN, TX, VT, VA, WA, WV, WI, WY
Nothing found	4	AL, ME, MO, UT

COOP, continuity of operations planning.

examination, in three states, broader legislation addressing election cybersecurity had been introduced but not enacted. In 33 states no election statute or legislation appears to address the issue of cybersecurity for elections at the time of examination.

In contrast, the contingency planning area is more developed in terms of legislation and illustrates a picture of a relatively more established policy agenda. Nine states have election statutes with a section related to contingency planning. From 18 states, we found a provision that mentions contingency planning in a broader section of the election statute. Legislation specific to election contingency plans was introduced but not enacted in two states; legislation that included contingency planning in broader terms was introduced but not enacted. There were 20 states from which we found nothing

in the election statute nor legislation which addresses the issue of contingency planning for elections at the time of examination.

Continuity of operations guidance

State plans and resources for disaster preparedness present yet another dimension of state capacity in the area of disaster preparedness broadly. Statewide COOPs and resources that state governments provide to other government entities are summarized in Table 6. In 10 states, statewide COOPs appear through state government websites, and 40 states provide online guidance on how to create a COOP. These categories are not mutually exclusive as some states provide both on state government websites. In only four states, nothing related to COOPs appeared. Figure 4 presents this information in graphic form.

ANALYSIS OF STATE CAPACITY IN ELECTION EMERGENCY PREPAREDNESS AND SECURITY

To understand the extent to which state election offices have undertaken typical activities that indicate capacity to consider, prepare for, and respond to election emergencies, we analyzed the relationships between provision of resources, guidance, and legislative actions to support contingency planning and cybersecurity. State government responses to contingency planning and cybersecurity are

FIG. 4. State action on voting system security rules and guidance.

TABLE 7. COVARIATES OF CONTINGENCY PLANNING AND CYBERSECURITY GUIDANCE

<i>Covariates</i>	<i>Correlation with type of guidance</i>	
	<i>Contingency planning</i>	<i>Cybersecurity</i>
Cybersecurity guidance	0.527***	—
State COOP	0.317**	−0.045
State Rep on GCC	0.300**	0.504***
Cyber—by March 2018	0.491***	0.828***
Cyber—by August 2018	0.527***	—
Contingency planning law	0.073	0.124
Cybersecurity law	0.151	0.281**

*** $p < .01$ using a one-tailed test; ** $p < .05$ using a one-tailed test; * $p < .10$ using a one-tailed test.

COOP, continuity of operations planning; GCC, Government Coordinating Council.

related, as one might expect. The interorganizational collaborative approach to contingency planning through COOPs and the public/private arrangements established through the ISAC structure would be expected to be a blueprint for the development of new organizational relationships and an institutional structure to support these. To the extent that cybersecurity issues are perceived to be an extension of other contingency planning efforts, we would expect to see correlations between the two. Both require coordination among similar (and some cases the same) groups, and both require coordination among disparate functions and jurisdictions within state government. Frameworks developed in contingency planning should migrate into the cybersecurity arena. Table 7 displays a series of bivariate analyses among these preparation tools.

States with cyber guidance often have other types of contingency planning guidance, and this has only increased after the release of funds from the EAC during the summer of 2018 to support state efforts in these areas. Both contingency planning activity and cybersecurity activity are also related to a state's representation on the GCC. States that issue cyber guidance are also more likely to have COOPs, but having COOPs is not related to issuing cyber guidance. This may be a reflection of the very recent nature of cybersecurity concerns in the election space. The presence of cyber guidance is related to the presence of cyber laws; however, there is no relationship between having contingency planning guidance and contingency planning laws.

DISCUSSION

At the outset, we asked the following questions: What are the emergent policy safeguards and operational contingencies in place in the event of natural or man-made disasters or attacks on election systems? Have states engaged in these and how might responses at the state level vary? In this work, we present multiple and varying points of vulnerabilities in the American election system, and a range of state activities that indicate response capacity. We show that state readiness for different types of degraded environments as measured by legislation, guidance, and plans is related across different policy arenas that touch on election security. In other words, states that are prepared in one aspect of election security policy are largely prepared in others. We also find evidence that multiple strategies of coping with environmental change are in play, given the resultant interorganizational arrangements across multiple sectors (government, nonprofit, and private market) and the expansion of these.

A combination of responses to the problems that emerged from the 2000 election as well as the infrastructure responses to 9/11 created a ready-made infrastructure of national level organizations to support coordinated responses to the emerging threats posed by those seeking to undermine American democracy through the electoral process. For researchers, these emerging threats and intergovernmental responses serve as intriguing subjects. The major question facing researchers interested in contingency planning for degraded environments in elections is, “to what effect is the contingency planning implemented effectively?” There are two major challenges to studying election administration contingency planning and security, especially for academia. First, the nature of the actual risks and problems that require prior planning are not fully clear. Some of this is a consequence of not being able to predict the future. More broadly, it is also a consequence of the proprietary nature of security approaches generally both for vendors and for government offices. Related, with respect to security specifically, public analysis of past attacks and current risks must take place within an unclassified world. We may believe we have mapped the population of attacks and have full knowledge of what is involved, but we cannot know that for certain.

IMPLICATIONS FOR ELECTION LAW IN THE UNITED STATES

Recent years have seen an increased federal interest in getting involved in election law and administration. However, given the tremendous inter-state variance in election law, election administration, and security preparedness, a uniform response from the federal government would likely fall short of whatever objective it sought to achieve. Historically, federal legislation in the election administration arena has focused on questions of equity—not security or integrity—in access and participation (VRA) and preserved state variation in implementation (NVRA, HAVA). Therefore, there is a question of whether election integrity or security supersede the Tenth Amendment and the other constitutional provisions that preserve state authority in election administration.

Knowing this, the federal government made grants available through the EAC so that states could determine how to best spend the money. A majority of the \$380 million allotted through the first round of grants was dedicated to new voting equipment and increased cybersecurity measures. Additionally, as previously discussed, there are many other resources available to localities seeking to secure elections. However, fragmentation not only exists across states, but within states as well. Therefore, a uniform response from the state would have disparate effects across jurisdictions, leaving some localities more or less vulnerable than others. Future attempts at addressing election security will need to consider this additional fragmentation as well.

This fragmentation has long been regarded as a positive aspect of elections for two primary reasons. First, fragmentation is a source of resilience as a successful exploitation of one system does not necessarily mean exploitation of the entire election, even within the same state. Second, this provides states and localities the opportunity to experiment and innovate the best way to protect and administer elections. Given the immense complexity within each jurisdiction, state and federal legislators and administrators will have to carefully consider the consequences and applicability of certain regulations, guidelines, and best practices. In short, preserving fragmentation while simultaneously providing states and localities with sufficient resources (money, information, human resources, training,

and access to the groups previously mentioned, for example) should be the focus of any election-related legislation in order to garner political support.

IMPLICATIONS FOR RESEARCH ON SECURITY AND OPERATIONAL CONTINGENCIES IN U.S. ELECTIONS

An examination of the roles of individual local election administrators related to election security and contingency planning is beyond the scope of this article. However, we realize that the local officials who are ultimately responsible for the administration of U.S. elections play a significant role. We presume all local election administrators—across the more than 8,000 local election jurisdictions across the country—inherently shoulder much of the responsibility for protecting U.S. elections from threats. Their capacity is important at least as much as the institutional infrastructure that now exists. Capacity is associated with resources, and professionalization of the human resources of the election administration community is a significant influence on government capacity generally (Brown and Hale 2018; Hale and Brown 2020). Perhaps this will be the case with security readiness as well.

Moving forward, it will be important to consider the context for research in at least two directions. One is thinking about how the questions we ask align with work being done in the comparative election arena—questions of trust and citizen perception and participation, and demotivating factors like corruption may offer important insights into the questions we ask about election emergency preparedness and management and election security in America. Indeed, the United States presents only one case, but cybersecurity issues are prevalent around the world, and the COVID-19 coronavirus pandemic is global. The mapping of contingency planning and election emergency readiness presented in this article could provide a foundation for replication in other countries and political systems. Identifying potential innovations employed in other countries and exploring how they work in the U.S. context could produce intellectual fruit as well as more concrete policy recommendations.

The role of vendors may also warrant further study. Although vendors are central actors in the

public process of electing public officials to run our government, it is challenging to identify or classify their specific actions related to voting and election system security. Government procurement processes are public and transparent, but some vendors do not release proprietary internal security protocols and procedures for contingency planning during the bidding process for contracts. As the national security infrastructure continues to evolve, additional attention may be directed to procurement requirements. The limited market for voting system hardware, software, and ancillary equipment and the current long-term nature of government contracts have been observed as disincentives to vendor innovation (e.g., Hitt et al. 2016).

Additionally, as these relationships continue to evolve over time and become more (or less) institutionalized across states and localities, we anticipate additional data that will facilitate a more robust analysis. Future work should endeavor to capitalize on this variation in order to provide a better understanding of the election security environment. Future research should also explore how state and local activities reacted to events occurring since the time of our data collection, including injections of federal funds into election administration and a pandemic during a major U.S. election year.

Finally, decisions made about election security are also political decisions with implications under American federalism. The political context for understanding election security therefore includes not only the typical understanding of partisan alignments, but also a sophisticated consideration of the intergovernmental complexities of America's highly decentralized election systems alongside the national role. Therefore, an investigation of the increasingly partisan nature of elections could be highly informative.

REFERENCES

- Agranoff, Robert. 2017. *Crossing Boundaries for Intergovernmental Management*. Washington, DC: Georgetown University Press.
- Atlantic Council. 2020. "The Future of DHS Project: Protecting the Homeland from Coronavirus, Threats to Democracy, and Other Future Threats." Washington, DC: Atlantic Council Scowcroft Center for Strategy and Security. Accessed from <<https://www.atlanticcouncil.org/the-future-of-dhs-project/>> on April 3, 2020.
- Birkland, Thomas A. 2006. *Lessons of Disaster: Policy Change After Catastrophic Events*. Washington, DC: Georgetown University Press.
- Birkland, Thomas A. 2015. *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making*, 4th ed. New York, NY: Routledge. Prior editions published by M. E. Sharpe.
- Brabant, Koenraad van. 2000. *Operational Security Management in Violent Environments: A Field Manual for Aid Agencies*. London, UK: Overseas Development Institute.
- Brown, J. (2002). "Inclusive Governance Practices in Nonprofit Organizations and Implications for Practice." *Nonprofit Management & Leadership* 12(4): 369–385.
- Brown, Mitchell. 2016. "Mobilization Through Third Party Groups." In *Why Don't Americans Vote: Causes and Consequences*, eds. Bridgett King and Kathleen Hale. ABC-CLIO.
- Brown, Mitchell and Kathleen Hale. 2018. "Election Security: How Professionalism and Resources Are Shaping the Future." Paper presented at the 2018 Pre-APSA Workshop, Building Better Elections: New Challenges in Electoral Management. August 29, Boston, MA.
- Callen, J., A. Klein, and D. Tinkelman. 2010. "The Contextual Impact of Nonprofit Board Composition and Structure on Organizational Performance: Agency and Resource Dependency Perspectives." *Voluntas* 21: 101–125.
- Comfort, Louise (ed). 2012. *Journal of Comparative Policy Analysis: Issues 2 and 3, Designing Disaster Resilience and Public Policy*.
- Comfort, Louise, Arjen Boin, and Chris C. Demchak. 2010. *Designing for Resilience: Preparing for Extreme Events*. Pittsburgh, PA: University of Pittsburgh Press.
- Comfort, Louise., W. L. Waugh, and Beverly Cigler. 2012. "Emergency Management Research and Practice in Public Administration: Emergence, Evolution, Expansion, and Future Directions." *Public Administration Review* 72: 35–59.
- Corasaniti, Nick and Stephanie Saul. 2020. "14 States Have Postponed Their Primaries Because of Coronavirus. Here's a List." *New York Times*. March 28.
- Dahl, Robert A. 1961. *Who Governs? Democracy and Power in an American City*. New Haven, CT: Yale University Press.
- Defending Digital Democracy Project. 2018. *The State and Local Election Cybersecurity Playbook*. Cambridge, MA: Harvard Kennedy School and Belfer Center for Science and International Affairs.
- Elazar, Daniel. 1966. *American Federalism: A View from the States*. New York: Crowell.
- Ewald, Alec. 2009. *The Way We Vote: The Local Dimensions of American Suffrage*. Nashville, TN: Vanderbilt University Press.
- Garnett, Holly Ann. 2017. "Open Election Management Bodies." In *Election Watchdogs*, eds. Pippa Norris and Alessandro Nai. New York, NY: Oxford University Press.
- Garnett, Holly Ann. 2019. "Evaluating Election Management Body Capacity." *International Political Science Review* 40(3): 335–353.
- Glaser, Max P. 2005. "Humanitarian Engagement with Non-State Armed Actors: The Parameters of Negotiated Access." Humanitarian Practice Network Policy Group,

- Network Paper No. 51. Accessed from <<http://odihpn.org/wp-content/uploads/2005/06/networkpaper051.pdf>> on July 16, 2016.
- Goggin, Malcolm L., Ann Bowman, James P. Lester, and Laurence J. O'Toole. 1990. *Implementation Theory and Practice: Toward a Third Generation*. Glenview, IL: Scott, Foresman/Little, Brown.
- Hale, Kathleen. 2011. *How Information Matters: Networks and Policy Innovation*. Washington, DC: Georgetown University Press.
- Hale, Kathleen and Mitchell Brown. 2013. "Adopting, Adapting, and Opting Out: State Response to Federal Voting System Guidelines." *Publius: The Journal of Federalism* 43: 428–451.
- Hale, Kathleen and Mitchell Brown. 2016. "Interlocal Diffusion and Difference: How Networks Are Transforming Public Service." In *Transforming Government Organizations: Fresh Ideas and Examples from the Field*, eds. Ronald Sims, William Sauser, Jr., Sheri Bias. Charlotte, NC: Information Age Publishing.
- Hale, Kathleen and Mitchell Brown. 2020. *Measuring Democracy: Innovations and American Elections*. Washington, DC: Georgetown University Press, forthcoming.
- Hale, Kathleen, Robert Montjoy, and Mitchell Brown. 2015. *Administering Elections: How American Elections Work*. New York, NY: Palgrave-MacMillan.
- Hale, Kathleen and Christa Slaton. 2008. "Building Capacity in Election Administration: Responses to Complexity and Interdependence." *Public Administration Review* 68: 839–849.
- Harris, Joseph P. 1928. "The Permanent Registration of Voters." *American Political Science Review* 22: 349–353.
- Harris, Joseph P. 1934. *Election Administration in the United States*. Washington, DC: Brookings Institute Press.
- Headquarters Department of the Army. 2003. *Stability and Support Operations*, Field Manual 3-07 (Washington, D.C.: Headquarters Department of the Army, February 20), A-10.
- Herzog, Stephen. 2011. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4(2): 49–60.
- Hitt, Loren, Simran Ahluwalia, Matthew Caulfield, Leah Davidson, Mary Margaret Diehl, Alina Ispas, and Michael Windle. 2016. *The Business of Voting: Market Structure and Innovation in the Election Technology Industry*. Harrisburg, PA: University of Pennsylvania Penn Wharton Public Policy Initiative.
- International Foundation for Electoral Security. 2020. *Guidelines and Recommendations for Electoral Activities During the COVID-19 Pandemic*. Arlington, VA: International Foundation for Electoral Security. Accessed at <<https://www.ifes.org/publications/guidelines-and-recommendations-electoral-activities-during-covid-19-pandemic>>. April 2.
- James, Toby S. 2020. *Comparative Electoral Management: Performance, Networks and Instruments*. New York, NY: Routledge.
- Kaplan, Thomas. 2013. "Using Hurricane Sandy as a Lesson for Future Elections." *New York Times*. November 12.
- Kent, Randolph. 2011. "Planning from the Future: An Emerging Agenda." *International Review of the Red Cross* 93(884): 939–964.
- Keyssar, Alexander. 2000. *The Right to Vote: The Contestable History of Democracy in the United States*. New York, NY: Basic Books (rev. 2009).
- King, Bridgett A. and Norman E. Youngblood. 2016. "E-government in Alabama: An Analysis of County Voting and Election Website Content, Usability, Accessibility, and Mobile Readiness." *Government Information Quarterly* 33(4): 715–726.
- Kingdon, John. 1984. *Agendas, Alternatives, and Public Policies*. New York, NY: Longman Publishing.
- Kreutzer, K. (2009). "Nonprofit Governance During Organizational Transition in Voluntary Associations." *Nonprofit Management & Leadership* 20(1): 117–133.
- Manna, Paul. 2006. *School's in: Federalism and the National Education Agenda*. Washington, D.C.: Georgetown University Press.
- Maucione, Scott. 2019. "National Guard Cyber Unites Protect Country's Interests, still Face Training Issues." Federal News Network. January 18. Accessed from <<https://federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/>> on April 22, 2019.
- Miller-Millesen, Judith L. 2003. "Understanding the Behavior of Nonprofit Boards of Directors: A Comparative Theory-Based Approach." *Nonprofit and Voluntary Sector Quarterly* 32: 521–547.
- Miller, Judith L. 2002. "The Board as a Monitor of Organizational Activity: The Applicability of Agency Theory to Nonprofit Boards." *Nonprofit Management and Leadership* 12: 429–450.
- Mitchell, Daniel. 2006. *Policy Implications for NGOs and Contractors in Permissive and Non-Permissive Environments*. Carlisle Barracks, PA: Army War College.
- Montjoy, Robert S. and Laurence O'Toole, Jr. 1979. "Toward a Theory of Policy Implementation: An Organizational Perspective." *Public Administration Review* 38: 465–476.
- Nagourney, Adam. 2001. "AFTER THE ATTACKS: THE ELECTION; Primary Rescheduled for Sept. 25, with Run-off, if Necessary, Set for Oct. 11." *New York Times*. September 14.
- Odula, Tom. 2017. "Kenya Election Official Tortured, Killed Days Before Vote." *AP News*. July 31.
- Ostrower, Francie and Melissa Stone. 2009. "Moving Governance Research Forward: A Contingency-based Framework and Data Application." *Nonprofit and Voluntary Sector Quarterly* 39(5): 901–924.
- O'Toole, Lawrence, Jr. 1988. "Strategies for Intergovernmental Management: Implementing Programs in Intergovernmental Management." *International Journal of Public Administration* 11: 417–444.
- O'Toole, Lawrence, Jr. 1997. "Treating Networks Seriously: Practical and Research-based Agendas in Public Administration." *Public Administration Review* 57(1): 45–52.
- Perito, Robert M. 2007. *Guide for Participants in Peace, Stability, and Relief Operations* (web version). Washington, DC: United States Institute of Peace. <<https://www.usip.org/guide-participants-peace-stability-and-relief-operations-0>>.
- Provan, Keith G. and H. Brinton Milward. 1995. "A Preliminary Theory of Interorganizational Network Effectiveness:

- A Comparative Study of Four Community Mental Health Systems." *Administrative Science Quarterly* 40(1): 1–33.
- Quarantelli, E. L. 1991. "Disaster Response: Generic or Agent-specific?" in *Managing Natural Disasters and the Environment*, eds. A. Kreimer and M. Munasinghe. Washington, DC: Environmental Department, World Bank.
- Russ, Catherine. 2014. "The Humanitarian Partnership Broker as Change Agent." *Humanitarian Practice Network*. October 8. Accessed from <<http://odihpn.org/blog/the-humanitarian-partnership-broker-as-change-agent/>> on July 16, 2016.
- Sanger, David E. and Catie Edmondson. 2019. "Russia Targeted Election Systems in All 50 States, Report Finds." *New York Times*. July 25.
- Selznick, Philip. 1948. "Foundations of the Theory of Organization." *American Sociological Review* 13(1): 25–35.
- Selznick, Philip. 1949. *TVA and the Grass Roots: A Study in the Sociology of Formal Organization*. Berkeley, CA: University of California Press.
- Slack, Donovan. 2018. "Midterms: Hurricanes Leaving Election Officials Scrambling to Put Up Polls as Tight Races Hang in the Balance." *USA Today*. October 19.
- Thompson, James D. 1967. *Organizations in Action; Social Science Bases of Administrative Theory*. New York, NY: McGraw-Hill.
- Watkins, Ali. 2017. "Obama Was Warned in 2014 About Russian Interference." *Politico*. August 14.

Address correspondence to:
Mitchell Brown
Department of Political Science
Auburn University
7080 Haley Center
Auburn, AL 36849-5412
USA

E-mail: brown11@auburn.edu

Received for publication February 17, 2020; received in revised form April 6, 2020; accepted April 10, 2020; published online June 12, 2020.