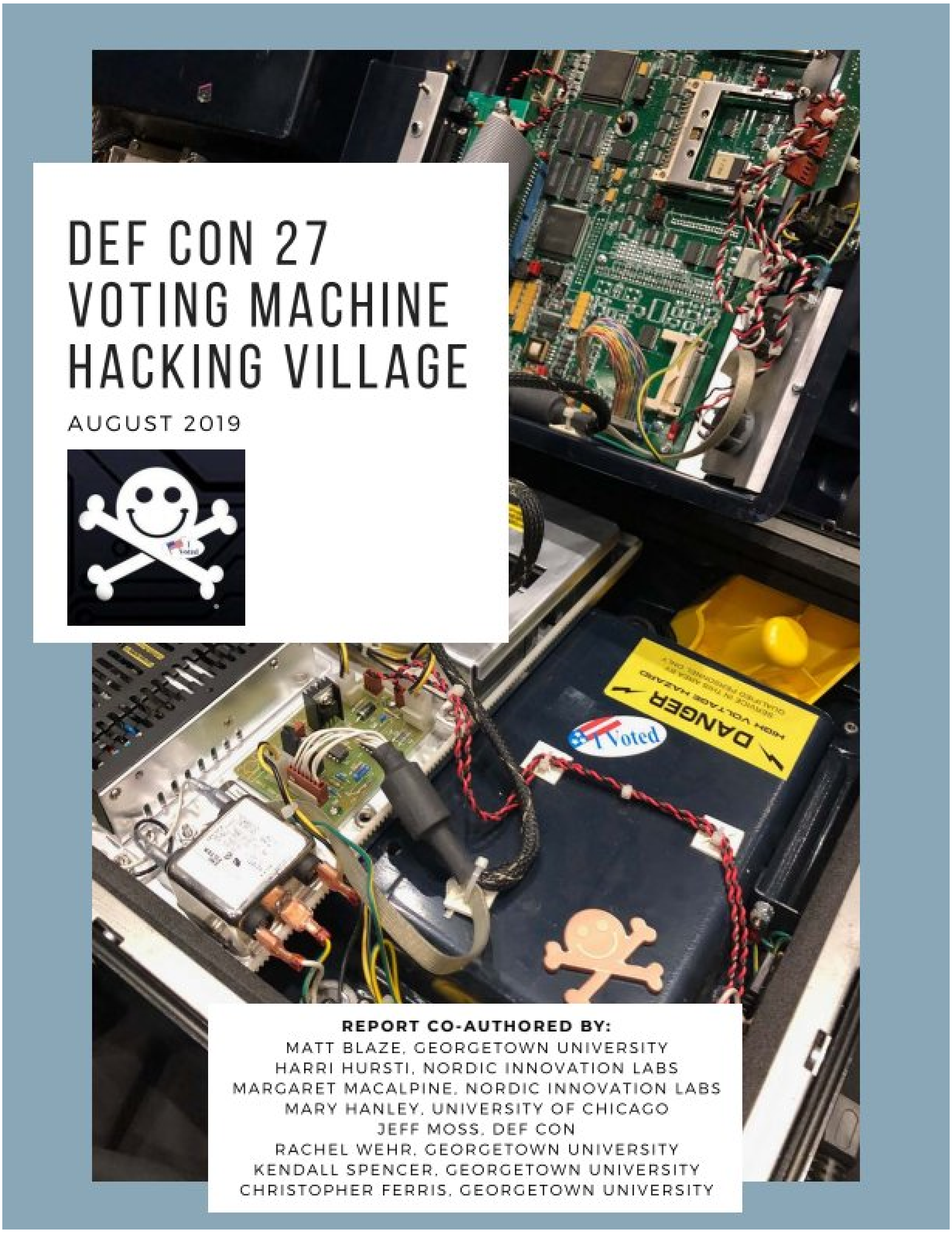
BUZZ CHRONICLES > TRUMP
Saved by @Alex1Powell
See On Twitter

Twitter Thread by [redacted]

[redacted]
@EffisforFUn

@CodeMonkeyZ @RudyGiuliani @realDonaldTrump :X



DEF CON 27 VOTING MACHINE HACKING VILLAGE

AUGUST 2019

REPORT CO-AUTHORED BY:

MATT BLAZE, GEORGETOWN UNIVERSITY
HARRI HURSTI, NORDIC INNOVATION LABS
MARGARET MACALPINE, NORDIC INNOVATION LABS
MARY HANLEY, UNIVERSITY OF CHICAGO
JEFF MOSS, DEF CON
RACHEL WEHR, GEORGETOWN UNIVERSITY
KENDALL SPENCER, GEORGETOWN UNIVERSITY
CHRISTOPHER FERRIS, GEORGETOWN UNIVERSITY

https://t.co/suwxo2PH0d

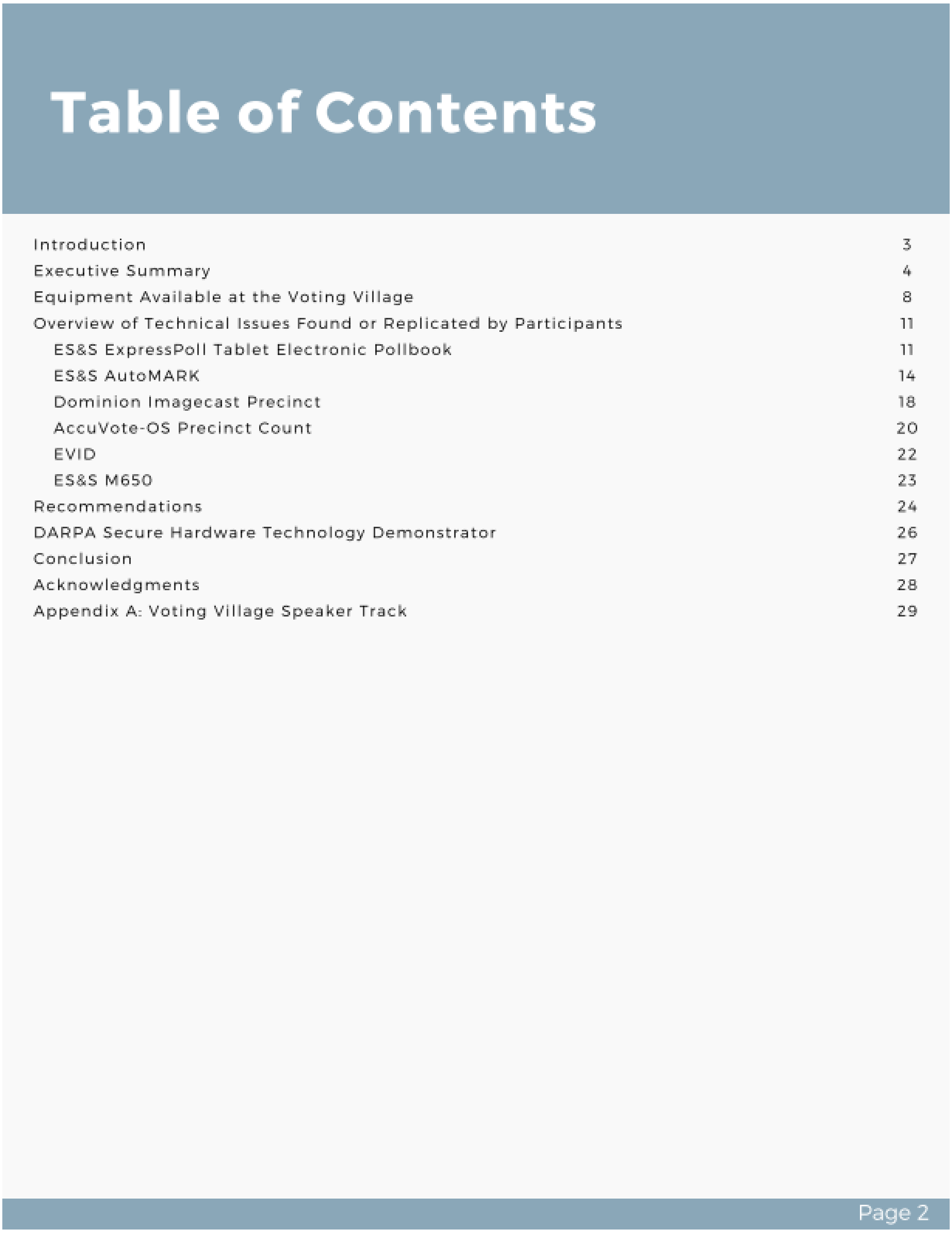
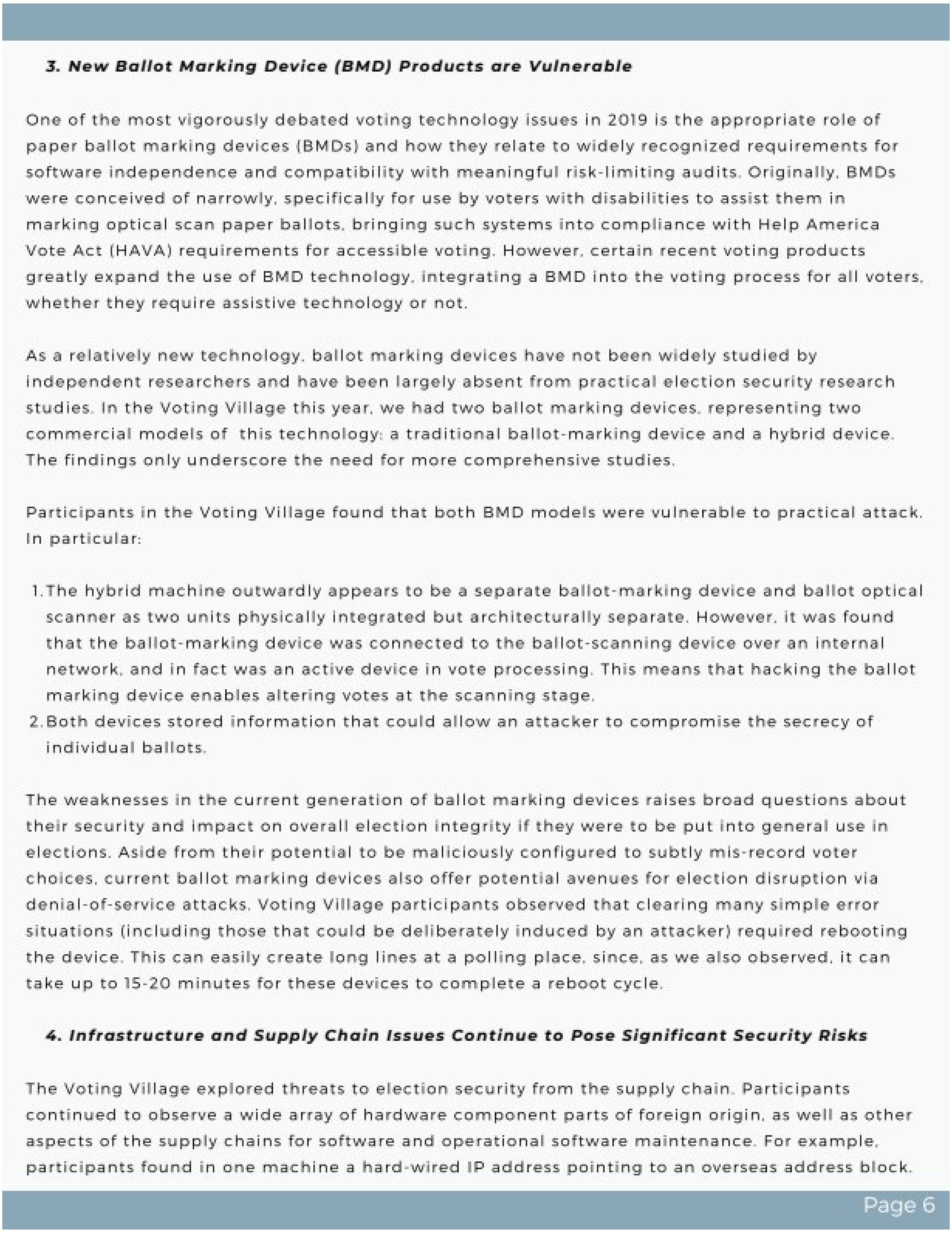


Table of Contents

https://t.co/U3q1FP0Cwl



3. New Ballot Marking Device (BMD) Products are Vulnerable

One of the most vigorously debated voting technology issues in 2019 is the appropriate role of paper ballot marking devices (BMDs) and how they relate to widely recognized requirements for software independence and compatibility with meaningful risk-limiting audits. Originally, BMDs were conceived of narrowly, specifically for use by voters with disabilities to assist them in marking optical scan paper ballots, bringing such systems into compliance with Help America Vote Act (HAVA) requirements for accessible voting. However, certain recent voting products greatly expand the use of BMD technology, integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

As a relatively new technology, ballot marking devices have not been widely studied by independent researchers and have been largely absent from practical election security research studies. In the Voting Village this year, we had two ballot marking devices, representing two commercial models of this technology: a traditional ballot-marking device and a hybrid device. The findings only underscore the need for more comprehensive studies.

Participants in the Voting Village found that both BMD models were vulnerable to practical attack. In particular:

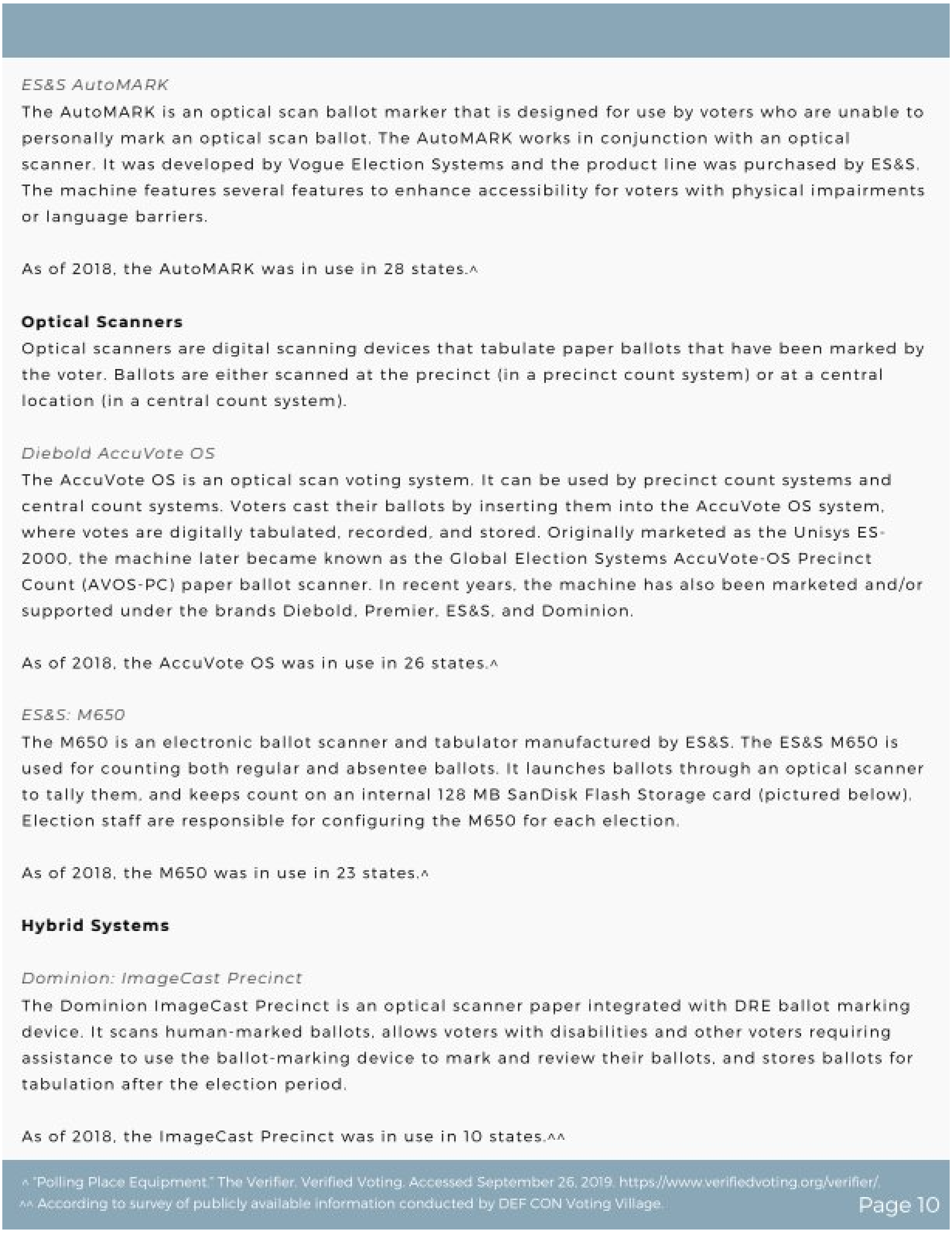
1. The hybrid machine outwardly appears to be a separate ballot-marking device and ballot optical scanner as two units physically integrated but architecturally separate. However, it was found that the ballot-marking device was connected to the ballot-scanning device over an internal network, and in fact was an active device in vote processing. This means that hacking the ballot marking device enables altering votes at the scanning stage.
2. Both devices stored information that could allow an attacker to compromise the secrecy of individual ballots.

The weaknesses in the current generation of ballot marking devices raises broad questions about their security and impact on overall election integrity if they were to be put into general use in elections. Aside from their potential to be maliciously configured to subtly mis-record voter choices, current ballot marking devices also offer potential avenues for election disruption via denial-of-service attacks. Voting Village participants observed that clearing many simple error situations (including those that could be deliberately induced by an attacker) required rebooting the device. This can easily create long lines at a polling place, since, as we also observed, it can take up to 15-20 minutes for these devices to complete a reboot cycle.

4. Infrastructure and Supply Chain Issues Continue to Pose Significant Security Risks

The Voting Village explored threats to election security from the supply chain. Participants continued to observe a wide array of hardware component parts of foreign origin, as well as other aspects of the supply chains for software and operational software maintenance. For example, participants found in one machine a hard-wired IP address pointing to an overseas address block.

https://t.co/3BZpGrHDNA



ES&S AutoMARK

The AutoMARK is an optical scan ballot marker that is designed for use by voters who are unable to personally mark an optical scan ballot. The AutoMARK works in conjunction with an optical scanner. It was developed by Vogue Election Systems and the product line was purchased by ES&S. The machine features several features to enhance accessibility for voters with physical impairments or language barriers.

As of 2018, the AutoMARK was in use in 28 states.^

Optical Scanners

Optical scanners are digital scanning devices that tabulate paper ballots that have been marked by the voter. Ballots are either scanned at the precinct (in a precinct count system) or at a central location (in a central count system).

Diebold AccuVote OS

The AccuVote OS is an optical scan voting system. It can be used by precinct count systems and central count systems. Voters cast their ballots by inserting them into the AccuVote OS system, where votes are digitally tabulated, recorded, and stored. Originally marketed as the Unisys ES-2000, the machine later became known as the Global Election Systems AccuVote-OS Precinct Count (AVOS-PC) paper ballot scanner. In recent years, the machine has also been marketed and/or supported under the brands Diebold, Premier, ES&S, and Dominion.

As of 2018, the AccuVote OS was in use in 26 states.^

ES&S: M650

The M650 is an electronic ballot scanner and tabulator manufactured by ES&S. The ES&S M650 is used for counting both regular and absentee ballots. It launches ballots through an optical scanner to tally them, and keeps count on an internal 128 MB SanDisk Flash Storage card (pictured below). Election staff are responsible for configuring the M650 for each election.

As of 2018, the M650 was in use in 23 states.^

Hybrid Systems

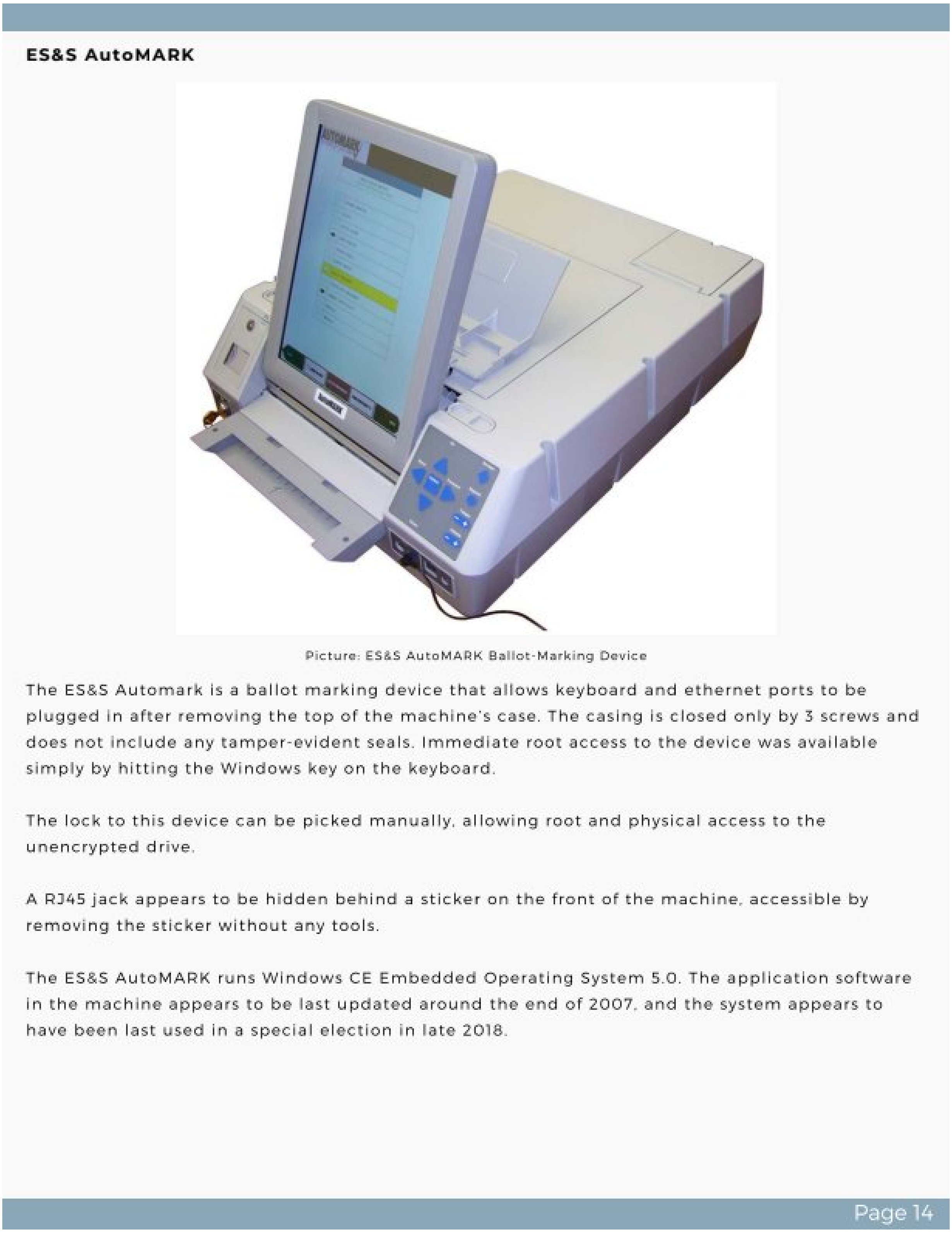
Dominion: ImageCast Precinct

The Dominion ImageCast Precinct is an optical scanner paper integrated with DRE ballot marking device. It scans human-marked ballots, allows voters with disabilities and other voters requiring assistance to use the ballot-marking device to mark and review their ballots, and stores ballots for tabulation after the election period.

As of 2018, the ImageCast Precinct was in use in 10 states.^^

^ "Polling Place Equipment." The Verifier. Verified Voting. Accessed September 26, 2019. https://www.verifiedvoting.org/verifier/.
^^ According to survey of publicly available information conducted by DEF CON Voting Village.

Six sided shape ?



ES&S AutoMARK

Picture: ES&S AutoMARK Ballot-Marking Device

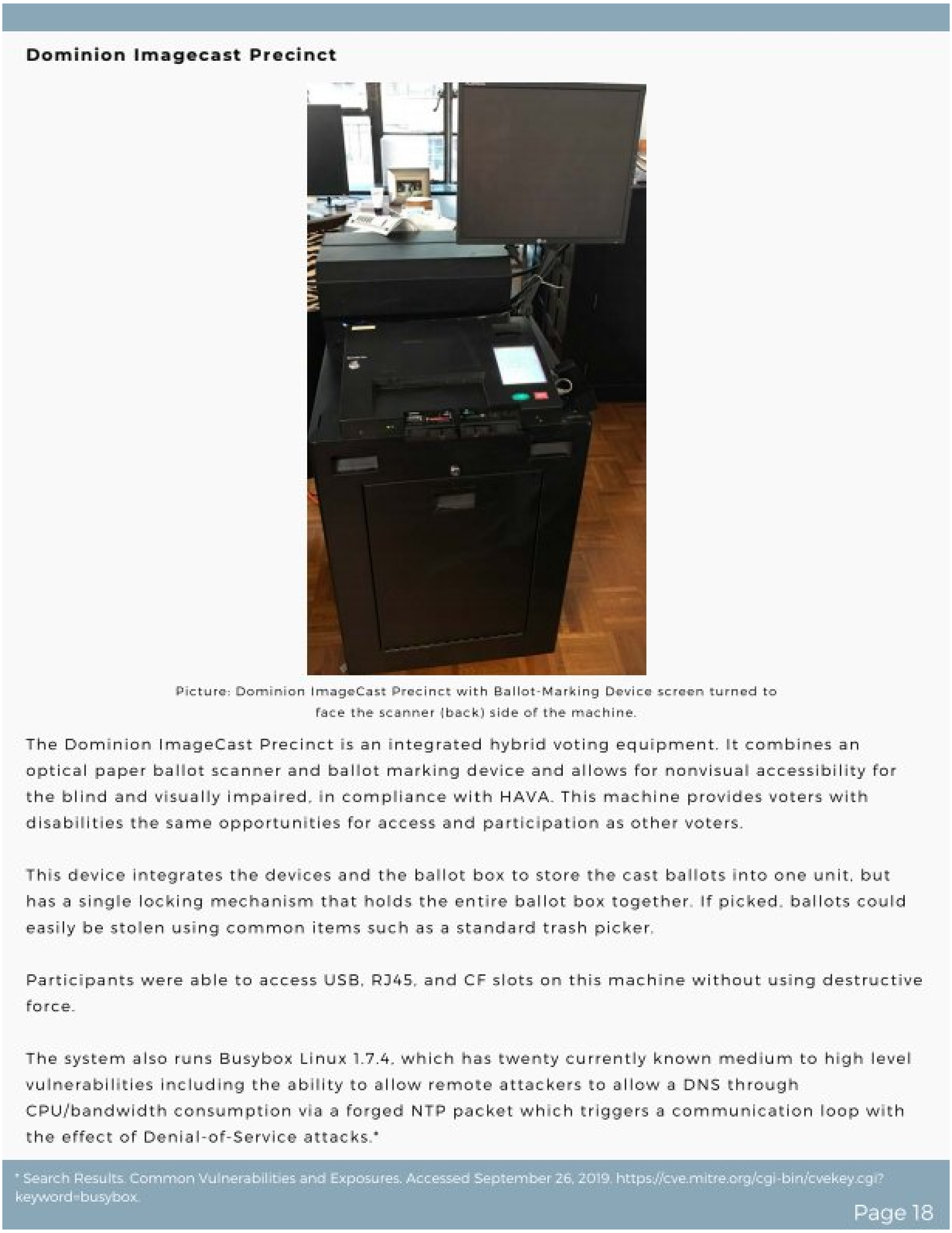
The ES&S Automark is a ballot marking device that allows keyboard and ethernet ports to be plugged in after removing the top of the machine's case. The casing is closed only by 3 screws and does not include any tamper-evident seals. Immediate root access to the device was available simply by hitting the Windows key on the keyboard.

The lock to this device can be picked manually, allowing root and physical access to the unencrypted drive.

A RJ45 jack appears to be hidden behind a sticker on the front of the machine, accessible by removing the sticker without any tools.

The ES&S AutoMARK runs Windows CE Embedded Operating System 5.0. The application software in the machine appears to be last updated around the end of 2007, and the system appears to have been last used in a special election in late 2018.

https://t.co/b3sAYl3FpQ



Dominion Imagecast Precinct

Picture: Dominion ImageCast Precinct with Ballot-Marking Device screen turned to face the scanner (back) side of the machine.

The Dominion ImageCast Precinct is an integrated hybrid voting equipment. It combines an optical paper ballot scanner and ballot marking device and allows for nonvisual accessibility for the blind and visually impaired, in compliance with HAVA. This machine provides voters with disabilities the same opportunities for access and participation as other voters.

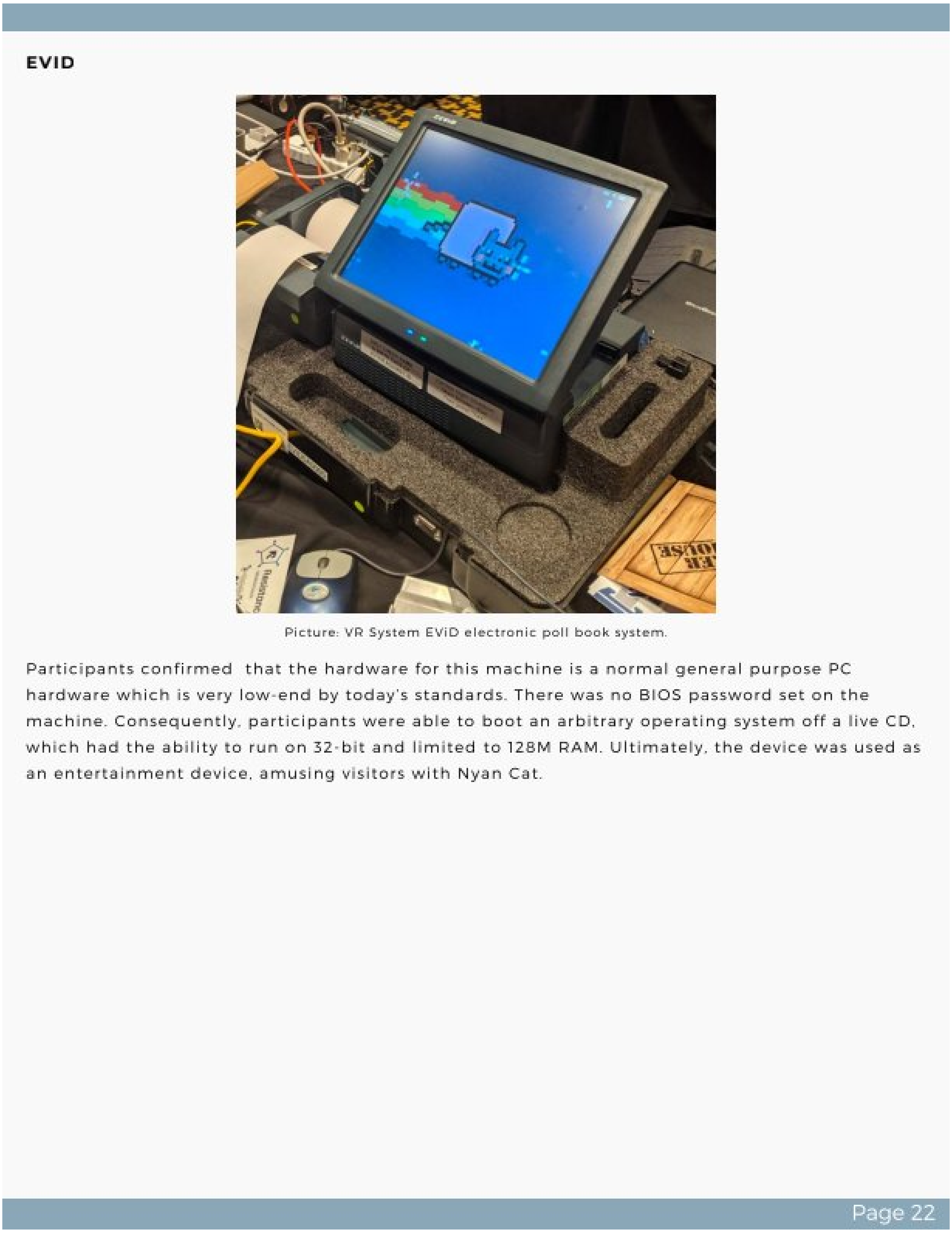
This device integrates the devices and the ballot box to store the cast ballots into one unit, but has a single locking mechanism that holds the entire ballot box together. If picked, ballots could easily be stolen using common items such as a standard trash picker.

Participants were able to access USB, RJ45, and CF slots on this machine without using destructive force.

The system also runs Busybox Linux 1.7.4, which has twenty currently known medium to high level vulnerabilities including the ability to allow remote attackers to allow a DNS through CPU/bandwidth consumption via a forged NTP packet which triggers a communication loop with the effect of Denial-of-Service attacks.*

* Search Results. Common Vulnerabilities and Exposures. Accessed September 26, 2019. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=busybox.

20 20 68 74 74 70 73 3A 2F 2F 67 69 74 68 75 62 2E 63 6F 6D 2F 73 65 63 75 72 69 74 79 76 6F 69 64 2F 64 6F 6D 69 6E 69 6F 6E 2D 76 6F 74 69 6E 67 2F 69 73 73 75 65 73 2F 31

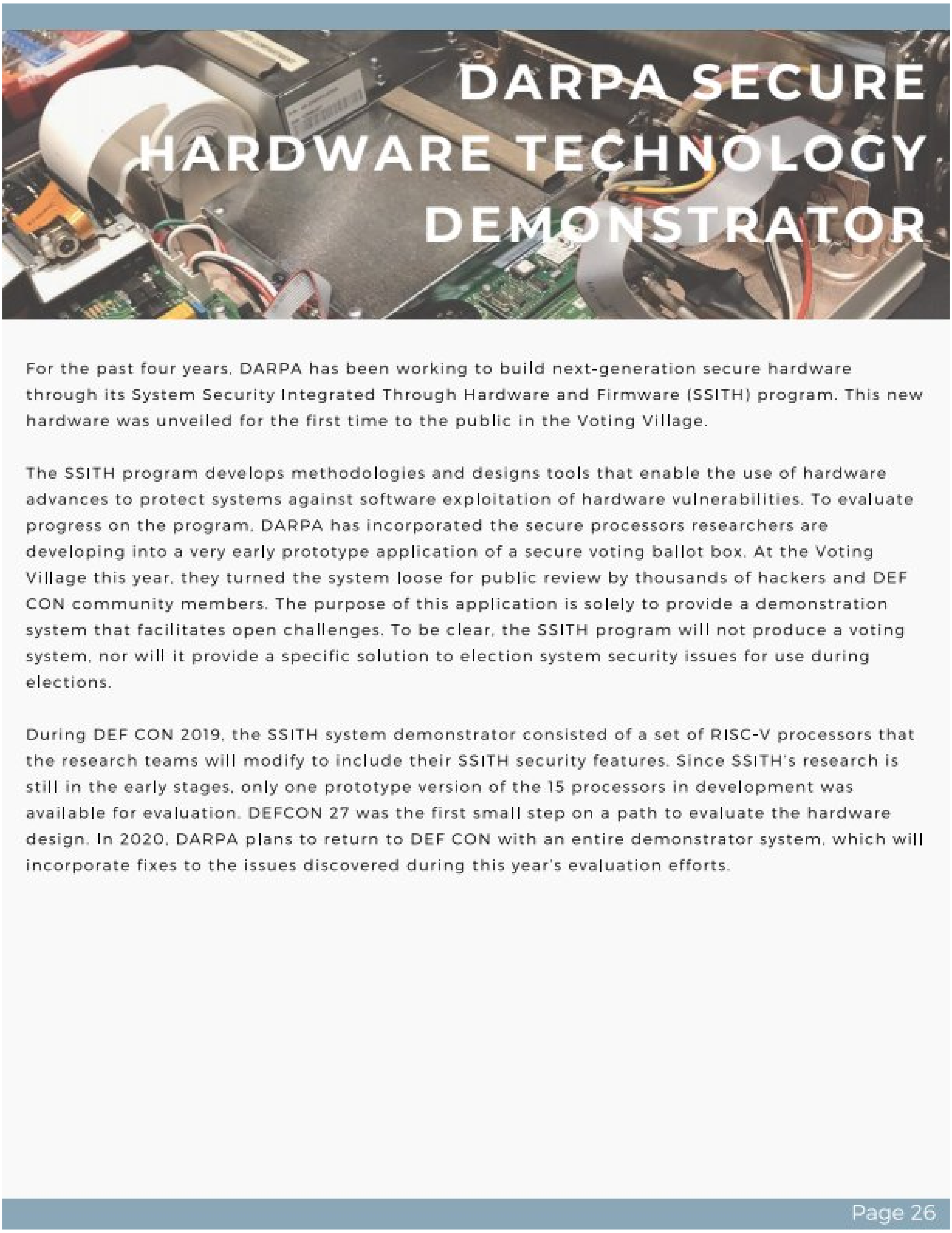


EVID

Picture: VR System EViD electronic poll book system.

Participants confirmed that the hardware for this machine is a normal general purpose PC hardware which is very low-end by today's standards. There was no BIOS password set on the machine. Consequently, participants were able to boot an arbitrary operating system off a live CD, which had the ability to run on 32-bit and limited to 128M RAM. Ultimately, the device was used as an entertainment device, amusing visitors with Nyan Cat.

https://t.co/d9gDpDnmoX



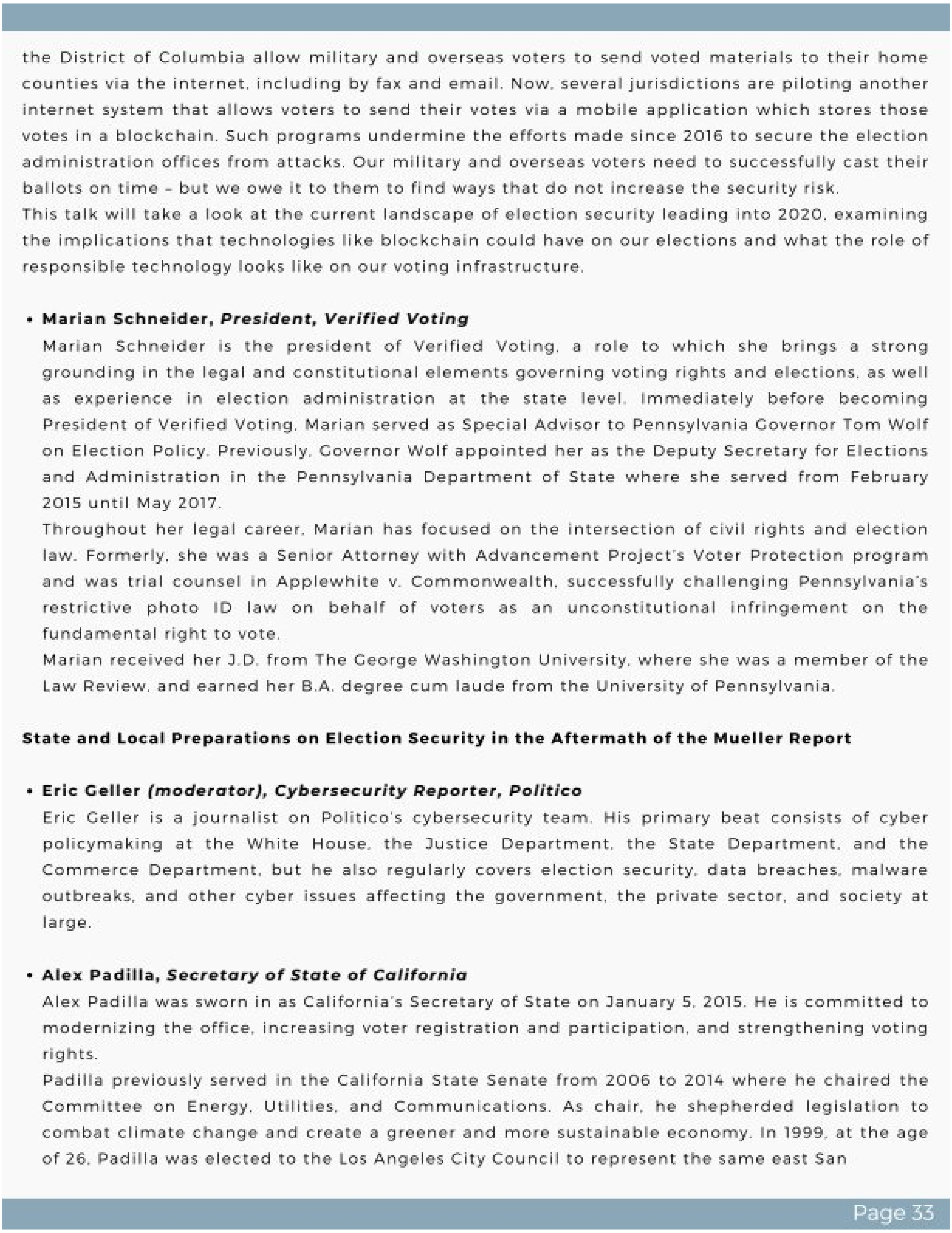
DARPA SECURE HARDWARE TECHNOLOGY DEMONSTRATOR

For the past four years, DARPA has been working to build next-generation secure hardware through its System Security Integrated Through Hardware and Firmware (SSITH) program. This new hardware was unveiled for the first time to the public in the Voting Village.

The SSITH program develops methodologies and designs tools that enable the use of hardware advances to protect systems against software exploitation of hardware vulnerabilities. To evaluate progress on the program, DARPA has incorporated the secure processors researchers are developing into a very early prototype application of a secure voting ballot box. At the Voting Village this year, they turned the system loose for public review by thousands of hackers and DEF CON community members. The purpose of this application is solely to provide a demonstration system that facilitates open challenges. To be clear, the SSITH program will not produce a voting system, nor will it provide a specific solution to election system security issues for use during elections.

During DEF CON 2019, the SSITH system demonstrator consisted of a set of RISC-V processors that the research teams will modify to include their SSITH security features. Since SSITH's research is still in the early stages, only one prototype version of the 15 processors in development was available for evaluation. DEFCON 27 was the first small step on a path to evaluate the hardware design. In 2020, DARPA plans to return to DEF CON with an entire demonstrator system, which will incorporate fixes to the issues discovered during this year's evaluation efforts.

68 74 74 70 73 3A 2F 2F 67 69 74 68 75 62 2E 63 6F 6D 2F 73 74 65 76 65 63 68 65 63 6B 6F 77 61 79 2F 66 72 6F 6E 74 69 65 72 2D 65 6C 65 63 74 69 6F 6E 2D 73 79 73 74 65 6D



the District of Columbia allow military and overseas voters to send voted materials to their home counties via the internet, including by fax and email. Now, several jurisdictions are piloting another internet system that allows voters to send their votes via a mobile application which stores those votes in a blockchain. Such programs undermine the efforts made since 2016 to secure the election administration offices from attacks. Our military and overseas voters need to successfully cast their ballots on time – but we owe it to them to find ways that do not increase the security risk.
This talk will take a look at the current landscape of election security leading into 2020, examining the implications that technologies like blockchain could have on our elections and what the role of responsible technology looks like on our voting infrastructure.

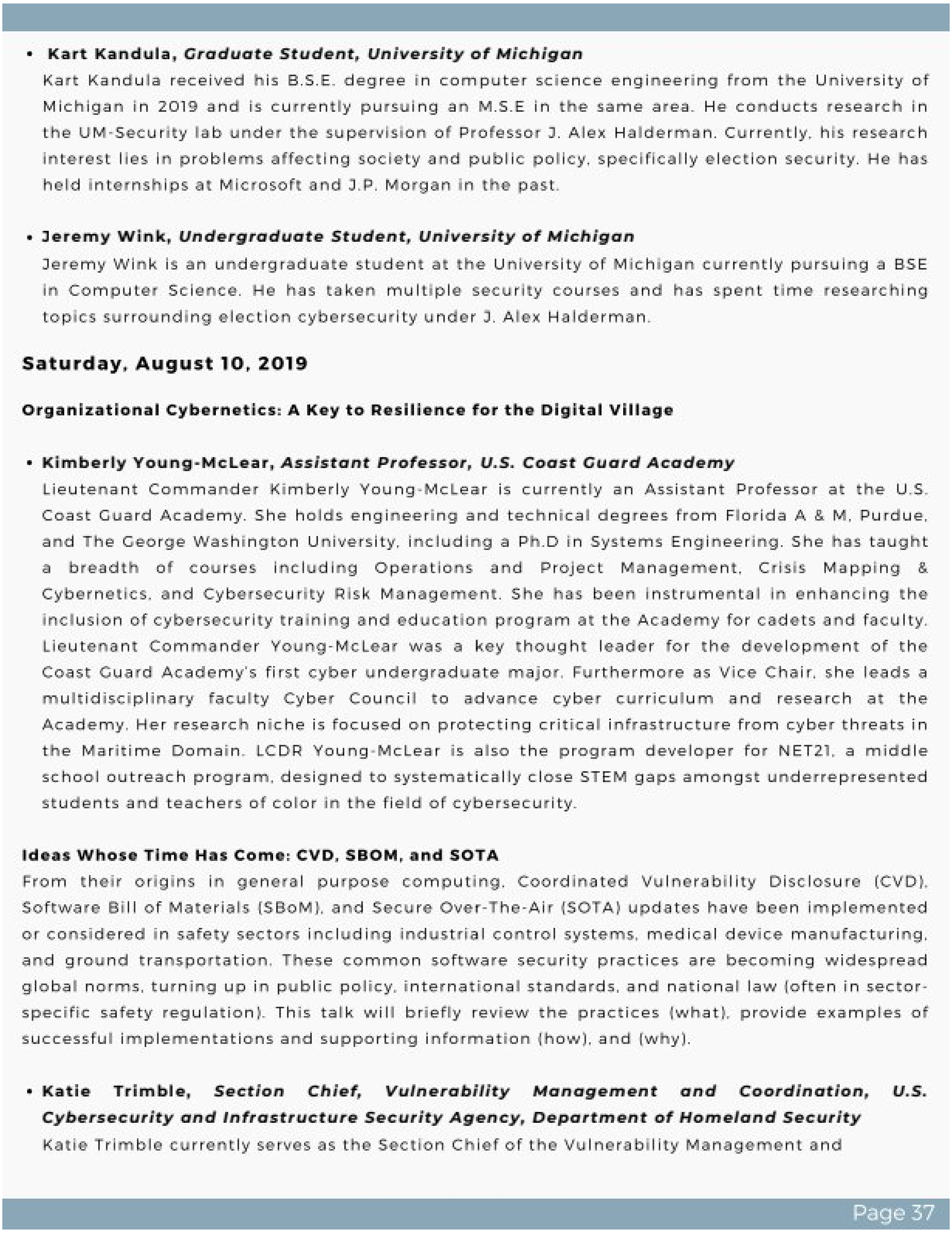
- **Marian Schneider, *President, Verified Voting***
  Marian Schneider is the president of Verified Voting, a role to which she brings a strong grounding in the legal and constitutional elements governing voting rights and elections, as well as experience in election administration at the state level. Immediately before becoming President of Verified Voting, Marian served as Special Advisor to Pennsylvania Governor Tom Wolf on Election Policy. Previously, Governor Wolf appointed her as the Deputy Secretary for Elections and Administration in the Pennsylvania Department of State where she served from February 2015 until May 2017.
  Throughout her legal career, Marian has focused on the intersection of civil rights and election law. Formerly, she was a Senior Attorney with Advancement Project's Voter Protection program and was trial counsel in Applewhite v. Commonwealth, successfully challenging Pennsylvania's restrictive photo ID law on behalf of voters as an unconstitutional infringement on the fundamental right to vote.
  Marian received her J.D. from The George Washington University, where she was a member of the Law Review, and earned her B.A. degree cum laude from the University of Pennsylvania.

State and Local Preparations on Election Security in the Aftermath of the Mueller Report

- **Eric Geller *(moderator), Cybersecurity Reporter, Politico***
  Eric Geller is a journalist on Politico's cybersecurity team. His primary beat consists of cyber policymaking at the White House, the Justice Department, the State Department, and the Commerce Department, but he also regularly covers election security, data breaches, malware outbreaks, and other cyber issues affecting the government, the private sector, and society at large.

- **Alex Padilla, *Secretary of State of California***
  Alex Padilla was sworn in as California's Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.
  Padilla previously served in the California State Senate from 2006 to 2014 where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San

https://t.co/GJVgQa2lY0



- **Kart Kandula, *Graduate Student, University of Michigan***
  Kart Kandula received his B.S.E. degree in computer science engineering from the University of Michigan in 2019 and is currently pursuing an M.S.E in the same area. He conducts research in the UM-Security lab under the supervision of Professor J. Alex Halderman. Currently, his research interest lies in problems affecting society and public policy, specifically election security. He has held internships at Microsoft and J.P. Morgan in the past.

- **Jeremy Wink, *Undergraduate Student, University of Michigan***
  Jeremy Wink is an undergraduate student at the University of Michigan currently pursuing a BSE in Computer Science. He has taken multiple security courses and has spent time researching topics surrounding election cybersecurity under J. Alex Halderman.

Saturday, August 10, 2019

Organizational Cybernetics: A Key to Resilience for the Digital Village

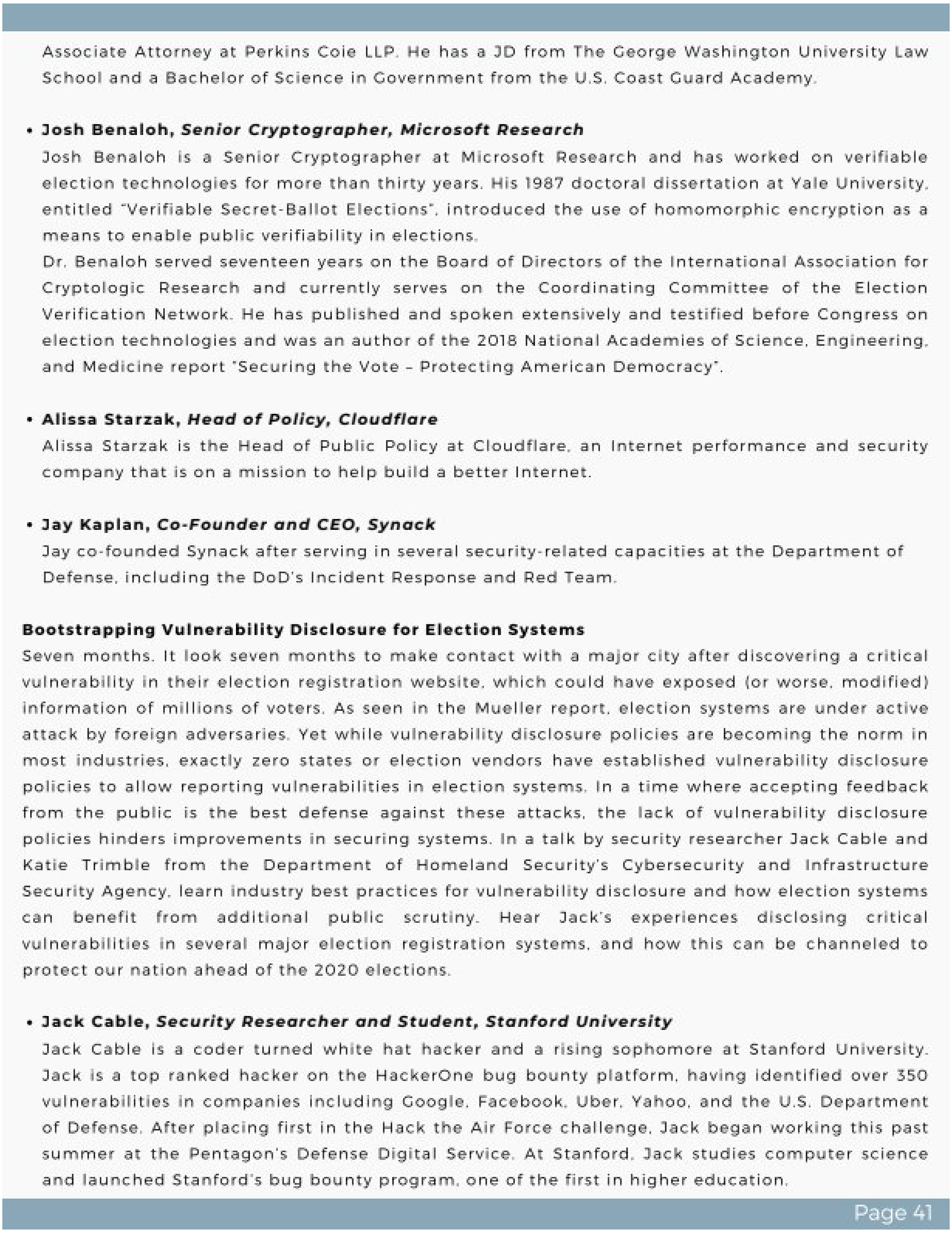
- **Kimberly Young-McLear, *Assistant Professor, U.S. Coast Guard Academy***
  Lieutenant Commander Kimberly Young-McLear is currently an Assistant Professor at the U.S. Coast Guard Academy. She holds engineering and technical degrees from Florida A & M, Purdue, and The George Washington University, including a Ph.D in Systems Engineering. She has taught a breadth of courses including Operations and Project Management, Crisis Mapping & Cybernetics, and Cybersecurity Risk Management. She has been instrumental in enhancing the inclusion of cybersecurity training and education program at the Academy for cadets and faculty. Lieutenant Commander Young-McLear was a key thought leader for the development of the Coast Guard Academy's first cyber undergraduate major. Furthermore as Vice Chair, she leads a multidisciplinary faculty Cyber Council to advance cyber curriculum and research at the Academy. Her research niche is focused on protecting critical infrastructure from cyber threats in the Maritime Domain. LCDR Young-McLear is also the program developer for NET21, a middle school outreach program, designed to systematically close STEM gaps amongst underrepresented students and teachers of color in the field of cybersecurity.

Ideas Whose Time Has Come: CVD, SBOM, and SOTA

From their origins in general purpose computing, Coordinated Vulnerability Disclosure (CVD), Software Bill of Materials (SBoM), and Secure Over-The-Air (SOTA) updates have been implemented or considered in safety sectors including industrial control systems, medical device manufacturing, and ground transportation. These common software security practices are becoming widespread global norms, turning up in public policy, international standards, and national law (often in sector-specific safety regulation). This talk will briefly review the practices (what), provide examples of successful implementations and supporting information (how), and (why).

- **Katie Trimble, *Section Chief, Vulnerability Management and Coordination, U.S. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security***
  Katie Trimble currently serves as the Section Chief of the Vulnerability Management and

https://t.co/JUZTp6dJvP



Associate Attorney at Perkins Coie LLP. He has a JD from The George Washington University Law School and a Bachelor of Science in Government from the U.S. Coast Guard Academy.

- **Josh Benaloh, *Senior Cryptographer, Microsoft Research***

  Josh Benaloh is a Senior Cryptographer at Microsoft Research and has worked on verifiable election technologies for more than thirty years. His 1987 doctoral dissertation at Yale University, entitled "Verifiable Secret-Ballot Elections", introduced the use of homomorphic encryption as a means to enable public verifiability in elections.

  Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has published and spoken extensively and testified before Congress on election technologies and was an author of the 2018 National Academies of Science, Engineering, and Medicine report "Securing the Vote – Protecting American Democracy".

- **Alissa Starzak, *Head of Policy, Cloudflare***

  Alissa Starzak is the Head of Public Policy at Cloudflare, an Internet performance and security company that is on a mission to help build a better Internet.

- **Jay Kaplan, *Co-Founder and CEO, Synack***

  Jay co-founded Synack after serving in several security-related capacities at the Department of Defense, including the DoD's Incident Response and Red Team.

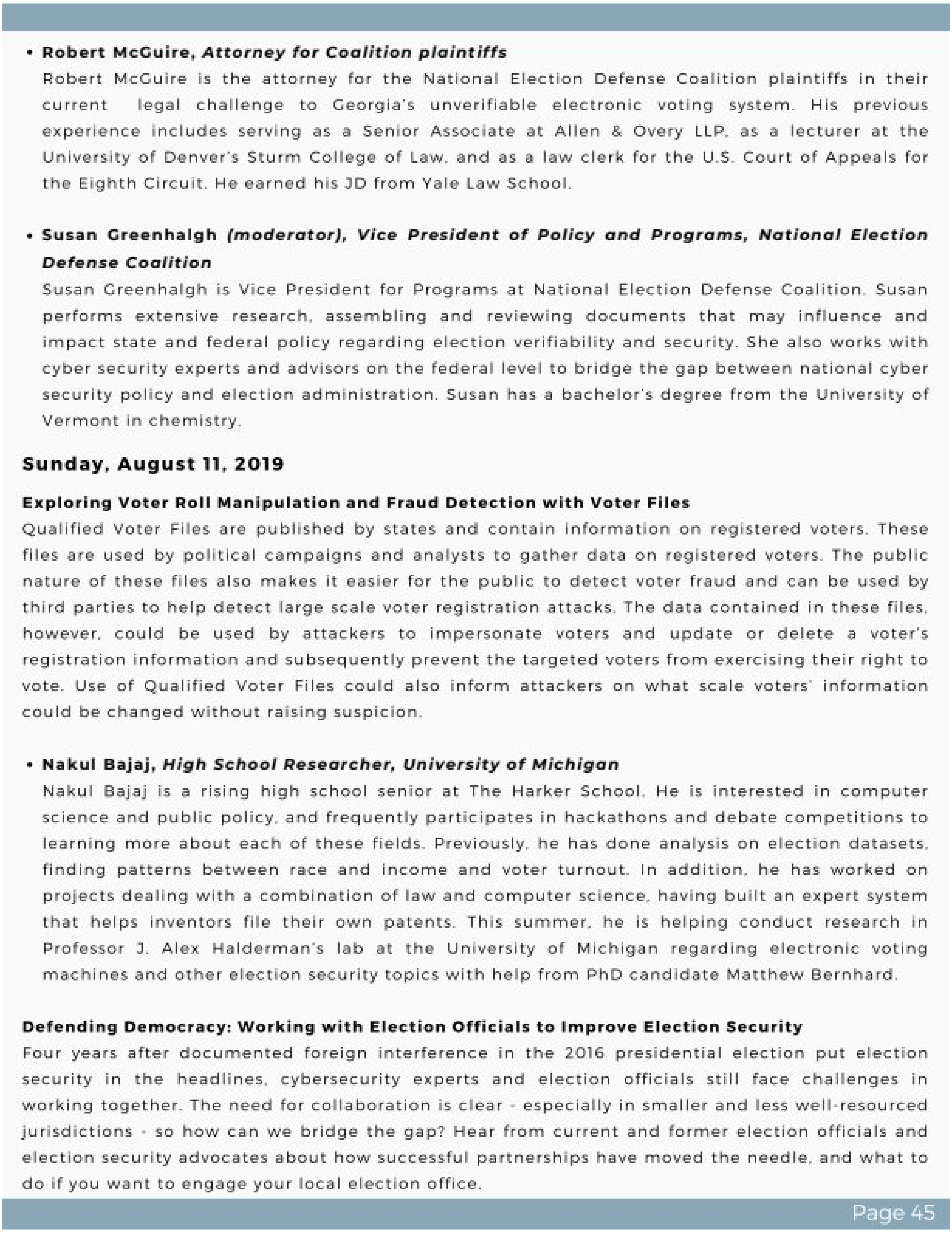
Bootstrapping Vulnerability Disclosure for Election Systems

Seven months. It look seven months to make contact with a major city after discovering a critical vulnerability in their election registration website, which could have exposed (or worse, modified) information of millions of voters. As seen in the Mueller report, election systems are under active attack by foreign adversaries. Yet while vulnerability disclosure policies are becoming the norm in most industries, exactly zero states or election vendors have established vulnerability disclosure policies to allow reporting vulnerabilities in election systems. In a time where accepting feedback from the public is the best defense against these attacks, the lack of vulnerability disclosure policies hinders improvements in securing systems. In a talk by security researcher Jack Cable and Katie Trimble from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, learn industry best practices for vulnerability disclosure and how election systems can benefit from additional public scrutiny. Hear Jack's experiences disclosing critical vulnerabilities in several major election registration systems, and how this can be channeled to protect our nation ahead of the 2020 elections.

- **Jack Cable, *Security Researcher and Student, Stanford University***

  Jack Cable is a coder turned white hat hacker and a rising sophomore at Stanford University. Jack is a top ranked hacker on the HackerOne bug bounty platform, having identified over 350 vulnerabilities in companies including Google, Facebook, Uber, Yahoo, and the U.S. Department of Defense. After placing first in the Hack the Air Force challenge, Jack began working this past summer at the Pentagon's Defense Digital Service. At Stanford, Jack studies computer science and launched Stanford's bug bounty program, one of the first in higher education.

https://t.co/XtbFjGIIEI



- **Robert McGuire, *Attorney for Coalition plaintiffs***
  Robert McGuire is the attorney for the National Election Defense Coalition plaintiffs in their current legal challenge to Georgia's unverifiable electronic voting system. His previous experience includes serving as a Senior Associate at Allen & Overy LLP, as a lecturer at the University of Denver's Sturm College of Law, and as a law clerk for the U.S. Court of Appeals for the Eighth Circuit. He earned his JD from Yale Law School.

- **Susan Greenhalgh *(moderator), Vice President of Policy and Programs, National Election Defense Coalition***
  Susan Greenhalgh is Vice President for Programs at National Election Defense Coalition. Susan performs extensive research, assembling and reviewing documents that may influence and impact state and federal policy regarding election verifiability and security. She also works with cyber security experts and advisors on the federal level to bridge the gap between national cyber security policy and election administration. Susan has a bachelor's degree from the University of Vermont in chemistry.

Sunday, August 11, 2019

Exploring Voter Roll Manipulation and Fraud Detection with Voter Files

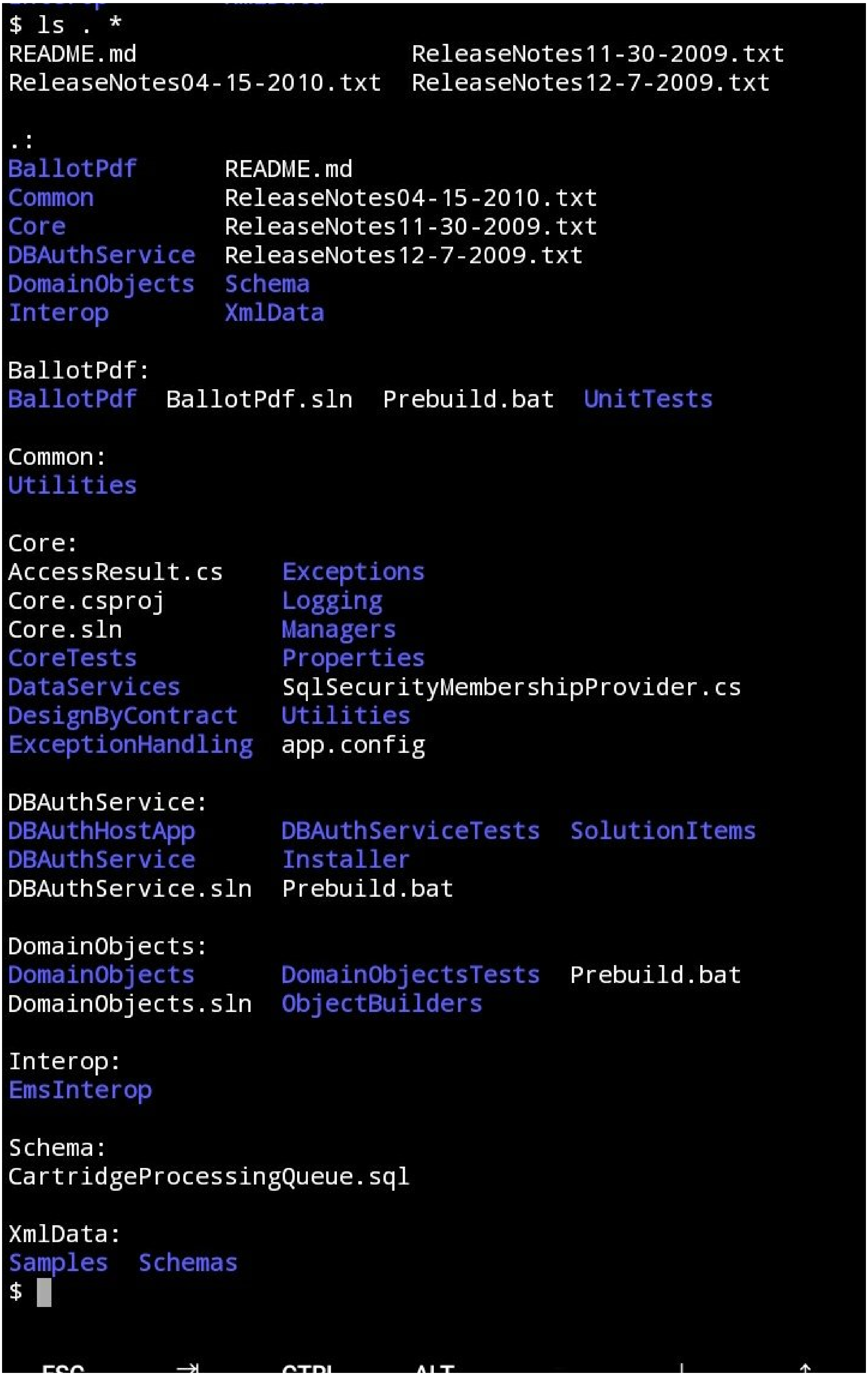
Qualified Voter Files are published by states and contain information on registered voters. These files are used by political campaigns and analysts to gather data on registered voters. The public nature of these files also makes it easier for the public to detect voter fraud and can be used by third parties to help detect large scale voter registration attacks. The data contained in these files, however, could be used by attackers to impersonate voters and update or delete a voter's registration information and subsequently prevent the targeted voters from exercising their right to vote. Use of Qualified Voter Files could also inform attackers on what scale voters' information could be changed without raising suspicion.

- **Nakul Bajaj, *High School Researcher, University of Michigan***
  Nakul Bajaj is a rising high school senior at The Harker School. He is interested in computer science and public policy, and frequently participates in hackathons and debate competitions to learning more about each of these fields. Previously, he has done analysis on election datasets, finding patterns between race and income and voter turnout. In addition, he has worked on projects dealing with a combination of law and computer science, having built an expert system that helps inventors file their own patents. This summer, he is helping conduct research in Professor J. Alex Halderman's lab at the University of Michigan regarding electronic voting machines and other election security topics with help from PhD candidate Matthew Bernhard.

Defending Democracy: Working with Election Officials to Improve Election Security

Four years after documented foreign interference in the 2016 presidential election put election security in the headlines, cybersecurity experts and election officials still face challenges in working together. The need for collaboration is clear - especially in smaller and less well-resourced jurisdictions - so how can we bridge the gap? Hear from current and former election officials and election security advocates about how successful partnerships have moved the needle, and what to do if you want to engage your local election office.

@grimmemer2 @stephanie_co239 @CodeMonkeyZ use HEX to decrypt both comments. They will lead you to a dominion source code. Here's proof of I got it saved on my phone



```
Interop          XmlData
$ ls . *
README.md                          ReleaseNotes11-30-2009.txt
ReleaseNotes04-15-2010.txt   ReleaseNotes12-7-2009.txt

.:
BallotPdf         README.md
Common            ReleaseNotes04-15-2010.txt
Core              ReleaseNotes11-30-2009.txt
DBAuthService   ReleaseNotes12-7-2009.txt
DomainObjects   Schema
Interop           XmlData

BallotPdf:
BallotPdf  BallotPdf.sln  Prebuild.bat  UnitTests

Common:
Utilities

Core:
AccessResult.cs     Exceptions
Core.csproj          Logging
Core.sln              Managers
CoreTests            Properties
DataServices        SqlSecurityMembershipProvider.cs
DesignByContract   Utilities
ExceptionHandling  app.config

DBAuthService:
DBAuthHostApp       DBAuthServiceTests  SolutionItems
DBAuthService       Installer
DBAuthService.sln  Prebuild.bat

DomainObjects:
DomainObjects       DomainObjectsTests  Prebuild.bat
DomainObjects.sln  ObjectBuilders

Interop:
EmsInterop

Schema:
CartridgeProcessingQueue.sql

XmlData:
Samples  Schemas
$ 
```