Challenges and Opportunities in State and Local Cybercrime Enforcement

Maggie Brunner*

Introduction

Cybercrime is a persistent problem that is growing exponentially in the United States, operating in the shadows with significant impunity. It is only expected to continue growing as significant hurdles stand in the way of measuring and combating the phenomenon. To create a robust cybercrime enforcement framework, the United States must consider a whole-of-government approach. Federal law enforcement agencies have restrictive thresholds for investigation and cannot address the bulk of regular cybercrimes that take a significant aggregate toll on the United States economy.[1] To close this gap and create an effective enforcement strategy, *state and local governments* must take a leading role with measurable, effective steps to bring perpetrators to justice and reduce the potential victim pool.

In most areas of crime, state and local governments lead the way in investigating, building, and prosecuting cases. Yet, due to the technical complexity and special nature of cybercrime, state and local governments have been largely hesitant to tackle its enforcement. This article argues that state and local governments should not treat cybercrime differently than other crime—they must create comprehensive frameworks to assess their legal codes, provide law enforcement with the knowledge and resources, and find ways to emphasize prevention.

This article will analyze various ways state and local government can improve their cybercrime enforcement. Section I will discuss the growing threat of cybercrime at the state and local level, including a discussion on the current challenges with even attempting to measure the scope and scale of the problem. Section II will discuss state legal frameworks around cybercrime, detailing how states have differed from the federal approach and providing specific examples of where states have closed legal loopholes on growing cybercrime threats. Finally, Section III will discuss challenges and opportunity to build capacity at the state and local level to enforce cybercrimes. Altogether, this article is designed to provide strategies for state and local governments looking to conduct the challenging work of closing the cybercrime enforcement gap.

---

* Maggie Brunner is a Program Director within the Homeland Security & Public Safety Division at the National Governors Association Center for Best Practices. Brunner also holds a J.D. from the Marshall-Wythe Law School at the College of William & Mary. The author would like to thank Reeve Jacobus, Michael Garcia, James Hillenbrand for their feedback, support, and research assistance.

1. Police Exec. Res. Forum, The Role of Local Law Enforcement Agencies in Preventing and Investigating Cyber Crime 20 (2014), https://perma.cc/AEU6-L4DQ.

I. THE GROWING THREAT OF CYBERCRIME AT THE STATE LEVEL: THE CYBERCRIME ENFORCEMENT GAP

States are increasingly turning their attention to cybercrime. It can be challenging for state officials to understand the severity of the problem, due to a dearth of reliable data on cybercrime. The lead federal agency that tracks cyber and computer-related crime is the Federal Bureau of Investigation's Internet Crimes Complaint Center (IC3). In 2018, IC3 received a total of 351,937 reports of cyber and computer-enabled crime, totaling $2,706.4 million.[2] The FBI estimates that the IC3 only receives reports of approximately ten percent of all cyber and computer-enabled crimes.[3] This is due to a variety of factors, including potential business consequences of disclosing a breach, unfamiliarity with reporting procedures, or a lack of faith in successful investigations.

Another significant issue to identifying the scope of cybercrime is how state and local law enforcement agencies compile statistics on cybercrime. The Uniform Crime Report (UCR), drafted in 1929 and the primary mechanism for standardizing crime data in the U.S., is in the process of being abandoned. Additionally, the upcoming transition to the National Incident Based Reporting System (NIBRS) in January 2021 will categorize many cybercrimes as an underlying traditional offense (e.g., trespass, fraud) while listing cyberspace as the location of the offense.[4] Critics argue that both methods are insufficient to understanding cybercrime because of potential inconsistencies in reporting.[5] There is significant academic effort underway to rethink crime reporting to better account for the challenging nature of cybercrime and modernize the nation's crime statistics.[6]

With a severe underreporting problem and a failure to accurately compile cybercrime statistics, it is impossible to understand with scientific certainty the real toll of cybercrime on the economy or its severity. Policymakers also struggle obtaining the necessary funding to meaningfully address cybercrime. It can be challenging to understand what resources to dedicate to cybercrime enforcement with a lack of reliable data on cybercrimes.

In addition to the dearth of data on the scale of cybercrime in the United States, there also exists a significant enforcement gap. Third Way, a think tank, recently estimated that less than one percent of "malicious cyber incidents" ever face any enforcement action.[7] At every level of government, there exist significant

2. FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME REPORT (2018), https://perma.cc/2TQ9-DT4F.

3. POLICE EXEC. RES. FORUM, THE ROLE OF LOCAL LAW ENFORCEMENT AGENCIES IN PREVENTING AND INVESTIGATING CYBER CRIME 21 (2014), https://perma.cc/AEU6-L4DQ.

4. NAT'L ACAD. OF SCI., ENG'G, & MED., MODERNIZING CRIME STATISTICS—REPORT 1: DEFINING AND CLASSIFYING CRIME 8 (2016), https://perma.cc/UE8P-RFMC.

5. *Id*.

6. *See generally id*.

7. THIRD WAY CYBER ENFORCEMENT INITIATIVE, TO CATCH A HACKER: TOWARD A COMPREHENSIVE STRATEGY TO IDENTIFY, PURSUE, AND PUNISH MALICIOUS CYBER ACTORS 2, 7 (2018), https://perma.cc/65DQ-YNT9 (victims who reported their crimes to the FBI saw an increase in enforcement rates from 0.05 percent to 0.3 percent).

challenges in enforcing cybercrime laws. Federal agencies, such as the FBI, U.S. Secret Service, and Immigration and Customs Enforcement's Homeland Security Investigations, can only lend their resources in the most extreme cases.[8] There are simply not enough federal agents, investigators, or prosecutors to handle a large number of cybercrime cases without surge capacity, and, as a result, federal law enforcement often imposes a monetary threshold to determine when it will open an investigation into a cybercrime. Amongst the nearly 18,000 local law enforcement agencies in the United States, there is an extreme disparity in the training, personnel, and other resources dedicated to cybercrime enforcement, with only a minority of agencies having dedicated cybercrime units. State law enforcement have built robust cybercrime units,[9] but they still require additional enhancement to begin closing the cyber enforcement gap. A whole-of-government approach that weaves together the jurisdictional reach, training, resources, and capacity that all levels of government can contribute is necessary moving forward.

II. STATES APPROACHES TO CYBERCRIME CRIMINAL CODES

The first steps for states looking to improve their cybercrime enforcement is to evaluate whether they have the appropriate legal authority within their criminal statutes. With not only a changing legal environment but a cybersecurity realm where cyber adversaries are constantly innovating, states must conduct frequent assessments to ensure their criminal codes allow state and local enforcement to appropriately provide criminal deterrence and enforcement.

Analyzing state computer crime law first requires understanding relevant federal laws. The most important statute for federal law enforcement in the arena of cybercrime enforcement is the Computer Fraud and Abuse Act (CFAA) of 1984.[10] It reflects a major effort in the 1970s and 1980s to hinge cybercrime alongside corresponding traditional crimes. Importantly, the CFAA faces significant criticism and calls for reform at the national level. The combination of the legal complexities with defining unauthorized access under the statute[11] and the penalty schema has contributed to a critique that the CFAA is overbroad, vague, and too broad in the conduct it criminalizes.[12] Additionally, critics point to the CFAA's provision allowing for civil damages[13] as "mission creep" that threatens to displace other state laws related to contracts or trade secrets.[14]

---

8. *See id*. at 271-72 (considering the FBI currently employs a threshold determining the dollar figure for which it will open an investigation).

9. *See generally* DEP'T OF JUSTICE, THE UTAH MODEL: A PATH FORWARD FOR INVESTIGATING AND BUILDING RESILIENCE TO CYBER CRIME, https://perma.cc/SR57-VUEF.

10. 18 U.S.C. § 1030 (2018).

11. DEP'T OF JUSTICE, *PROSECUTING COMPUTER CRIME* 8-12, https://perma.cc/4PHS-74J2.

12. *See, e.g*., ELEC. FRONTIER FOUND., *Computer Fraud and Abuse Act Reform*, https://perma.cc/L4UW-S5BD.

13. *See id*. (1994 amendment).

14. *See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1389, 1395 (2011).

In the midst of this controversy, states must make the choice of adopting the CFAA or an entirely unique legal framework. There are distinct advantages for states in aligning with the federal government and other states. At a time when the law enforcement community is attempting to close the cybercrime enforcement gap, states under a CFAA model have access to a wide body of case law and legal precedent that can aid their interpretation. As a result, the vast majority of states align their cybercrime codes with federal statutes, including the CFAA. However, it is at the state level where CFAA reform has been successful, with states either adopting entirely new regimes or limiting the more controversial aspects of the statute.

While researchers have conducted comprehensive studies analyzing prosecutions under the CFAA,[15] there is little research examining how computer crime prosecutions have played out at the state level. This may be perhaps due to a lack of data, the "enforcement gap" for cybercrime, and the hesitancy amongst state and local law enforcement to wade into this arena of law in the face of a multitude of competing cases for other criminal offenses.

A. A New Computer Crime Framework: The Washington State Case Study

In 2016, the state of Washington overhauled its computer crime statute and replaced it with a relatively novel framework. The Washington Cybercrime Act[16] passed in 2016 with sweeping bipartisan support from both chambers of the state legislature.[17] The Act frames hacking and network intrusion chiefly as cyber trespass. It creates two separate categories of cyber trespass, however, escalating based on two key factors. Sec. 9A.90.040 provides the crime of cyber trespass in the first degree, which makes hacking a felony if it involves a government database or if the intrusion was committed with the specific intent to commit another crime.[18] Under Washington law, computer trespass in the first degree is a class C felony, providing a maximum penalty of up to five years in prison and a fine of up to $10,000.[19] The Act also has a provision for computer trespass in the second degree (Sec. 9A.90.050), when an offender intentionally gains access to a computer system or electronic database with no specific intent to commit another crime. The penalty for computer trespass in the second degree is a maximum of up to one year in jail and a fine of up to $5,000 as a gross misdemeanor.

The Washington Cybercrime Act also creates a list of enumerated offenses based on the STRIDE cybersecurity threat model.[20] STRIDE is a mechanism for identifying specific cybersecurity threats based on attack properties[21] and allows

15. *See, e.g.*, Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453 (2016).

16. Washington Cybercrime Act, WASH. REV. CODE ANN. § 9A.90 (West 2019).

17. John Stang, *Washington State Lawmakers Pass Tough New Cybercrime Bill*, GEEKWIRE (Mar. 12, 2016, 8:29 AM), https://perma.cc/CKU2-4U4W.

18. WASH. REV. CODE ANN. § 9A.90.040 (West 2019).

19. *Id.*

20. *See* Nataliya Schevchenko et al., *Threat Modeling: A Summary of Available Methods*, CARNEGIE MELLON U. (2018), https://perma.cc/5CFW-2XFA.

21. *See* Sriram Krishnan, *A Hybrid Approach to Threat Modeling* (Feb. 25, 2017), https://perma.cc/DA38-B68E.

security professionals to conduct risk assessments with likely attack vectors. Figure 1 provides a guide to each cybercrime in the Act with associated criminal penalties.

Figure 1:
Enumerated Cybercrimes in the Washington Cybercrime Act and Associated Penalties

Crime	Statute	Selected Requirements	Criminal Penalty
Cyber Trespass – First Degree	9A.90.040	• Intentional access • Without authorization • Government system, or with specific intent to commit another crime	Class C Felony (up to 5 years, $10,000)
Cyber Trespass – Second Degree	9A.90.050	• Intentional access • Without authorization	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Interference	9A.90.060	• Malicious intent	Class C Felony (up to 5 years, $10,000)
Spoofing	9A.90.070	• Intentional act • Without authorization • Specific intent to commit another crime	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Tampering – First Degree	9A.90.080	• Malicious intent • Without authorization • Government system, or with specific intent to commit another crime	Class C Felony (up to 5 years, $10,000)
Electronic Data Tampering – Second Degree	9A.90.090	• Malicious intent • Without authorization	Gross misdemeanor (up to 1 year, $5,000)
Electronic Data Theft	9A.90.100	• Intentional obtainment of data • Without authorization • Specific intent to 1) commit another crime, or 2) wrongfully control/gain access to money, property or electronic data.	Class C Felony (up to 5 years, $10,000)

Under the chapter, Washington law also defines the term "without authorization." Unlike the CFAA, where federal courts have held the term to mean "accessing a protected computer without authorization,"[22] the Washington definition imposes additional criteria.

> Without authorization" means to knowingly circumvent technological access barriers to a data system in order to obtain information without the express or implied permission of the owner, where such technological access measures are specifically designed to exclude or prevent unauthorized individuals from obtaining such information, but does not include white hat security research or circumventing a technological measure that does not effectively control access to a computer. The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an internet service provider, internet web site, or employer. The term "circumvent technological access barriers" may include unauthorized elevation of privileges, such as allowing a normal user to execute code as administrator, or allowing a remote person without any privileges to run code.

In doing so, the Washington Cybercrime Act directly addressed several of the concerns that critics have levied against the federal CFAA. For example, several of the Act's provisions require malicious intent,[23] which is an additional hurdle for the government that several other states have also imposed.[24] Chiefly, the government could not use criminal laws to punish "white hat" security researchers,[25] who can help augment companies' security, and that the Act would not be used to enforce violation of terms of service or contractual disputes.

---

22. United States v. Nosal, 828 F.3d 865, 868 (9th Cir. 2016).

23. Federal courts have held that the intent to commit an offense under the CFAA need only be intentional, not malicious. *See* United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007).

24. *See* NAT'L GOVERNORS ASS'N, *Meet the Threat: States Confront the Cyber Challenge, A review of State Computer Crime Law* 2 (Nov. 1, 2016), https://perma.cc/52NV-TK2P (discussing Virginia's computer crime statute's *mens rea*). Note that some states, however, have second guessed the additional requirements, concerned that it might hinder cybercrime enforcement. *See id.*

25. Note that this is an issue on which the states are split. Roughly half of states use an outside party to conduct penetration testing on their system. *See* Doug Robinson & Srini Subramanian, *2016 Deloitte-NASCIO Cybersecurity Study*, DELOITTE & NAT'L ASSOC. OF STATE CHIEF INFO. OFFICERS 19 (2016), https://perma.cc/65J9-VQYE. Some states—such as Delaware and Missouri—have implemented or are in the process of implementing structured coordinated vulnerability disclosure programs, including the use of "bug bounties." Jeni Bergal, *White-Hat Hackers to the Rescue*, PEW (May 14, 2018), https://perma.cc/JG3B-4BPP. However, this is not universally accepted. In May 2018, then Governor Nathan Deal vetoed a cybercrime bill that had passed the Georgia legislature with a broad understanding of "unauthorized computer access" that would have prohibited "white hat" hacking. *See* S.B. 315-18, Gen. Assemb. (Ga. 2017-2018), https://perma.cc/L57D-BBS6. Governor Deal's veto came after strong opposition from the Information Security community, including a joint letter from Google and Microsoft. *See* Lily Hay Newman, *A Georgia Hacking Bill Gets Cybersecurity All Wrong*, WIRED (May 5, 2018), https://perma.cc/Q99G-XU3Q.

B. Tailored State Action to Close Legal Loopholes for Growing Threats in Cybersecurity and Cybercrime

While there are several state cybercrime statutes that purposefully take a broad approach to give prosecutors flexibility,[26] there is a growing trend in state criminal codes to enact specific cybercrime statutes. While many prohibitions may currently exist under general computer crime laws, states should evaluate their cybercrime laws to ensure there are no gaps in legal authority required for modern cybercrime offenses.

For example, one growing cybersecurity concern is in the arena of denial of service (DoS).[27] In perhaps the most famous DoS attack against a government network, the nation of Estonia had its government networks taken down in 2007 following a political dispute with Russia.[28] DoS attacks have also impacted state networks.[29] With an increasing emphasis on placing essential government services online, state governments must assess whether their current framework would prohibit a DoS attack. For example, the state of Arizona's cybercrime chapter has a specific DoS provision, prohibiting "recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network."[30] The specific statute increases penalties for DoS attacks on critical infrastructure facilities[31] and complements the remainder of the chapter, which diverges from CFAA in its language in a way that would not otherwise cover a disruption.[32]

There have also been several high-profile ransomware attacks on state and local governments in recent years, including attacks on 911 call centers[33] and

---

26. For example, Massachusetts cybercrime law simply prohibits "whoever, without authorization, knowingly accesses a computer system by any means, or . . . knows that such access is not authorized and fails to terminate such access, shall be punished [by imprisonment or fine] . . . " Mass Gen. Laws ch. 266, §120F (2019). *See generally* NAT'L GOVERNORS ASS'N, *supra* note 24.

27. A denial of service attack is one where "legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor." NAT'L CYBERSECURITY & COMM. INTEGRATION CTR., *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* (June 28, 2018), https://perma.cc/AB38-NPS2.

28. *See, e.g.*, Damien McGuinness, *How a cyber attack transformed Estonia*, BBC NEWS (Apr. 27, 2017), http://perma.cc/VUY3-9B56.

29. *See* Dawn Kawamoto, *Rash of Italian Cyberattacks Target State Governments*, GOV'T TECH. (May 16, 2018), https://perma.cc/Q5X4-6MPB.

30. ARIZ. REV. STAT. ANN. § 13-2316 (2019). Most DoS offenses are a Class 4 felony, which carries a maximum penalty of 3.75 years for first time offenders under Arizona law, except any DoS attack that targets critical infrastructure. § 13-702 (2019).

31. Other states also have multi part sentencing provisions for DoS attacks. For example, Connecticut law creates a schema where a sophistication cybercrime like DoS can escalate to a felony offense depending on the monetary damage or whether there was a risk of serious physical injury. CONN. GEN. STAT. § 53a-251 (2019). Florida creates additional criminal penalties for DoS attacks that endanger human life, or disrupt critical infrastructure, transit, or medical devices. FLA. STAT. § 815.06 (2019). Indiana's DoS statute is similarly subject to an increase in penalty based on the target (government-owned or utility), monetary damage, or potential to endanger human life. IND. CODE § 35-43-1-8 (2019).

32. *Compare* 18 U.S.C. § 1030(a)(5) (2018), *with* ARIZ. REV. STAT. ANN. § 13-2316(A)(2) (2019).

33. Jon Schuppe, *Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?*, NBC NEWS (Apr. 3, 2018, 6:36 AM), https://perma.cc/W7SE-VPJY.

coordinated attacks on school districts in Louisiana and Texas.[34] While gathering exact data is difficult due to a lack of standardized disclosure requirements, security experts note that ransomware attacks on state and local governments are increasing.[35] As a result, state legislatures are currently assessing whether they have sufficient legal authority to address the threat in their criminal law.

Several states have enacted specific ransomware statutes as a form of computer-enabled extortion.[36] However, Michigan took a different tactic with its attempt to criminalize the use of ransomware. The statute made the ransomware itself contraband, prohibiting its possession.[37] The Michigan approach was intended to close a legal loophole where state police had been unable to act if a suspected cybercriminal possessed ransomware but had not deployed it yet.[38] The bill's original sponsor cited "numerous cases in the past . . . which effectively protected cybercriminals from law enforcement until after the crime had been committed."[39]

States across the country—including legislatures with the input and advice of key officials in governors' offices—should assess their criminal codes to ensure that no current loopholes exist in their ability to investigate and prosecute cybercrime. Assessments should account for growing trends in the cybersecurity industry that target state and local governments, critical infrastructure, businesses, and citizens within their state.

III. CAPACITY BUILDING CHALLENGES AND OPPORTUNITIES FOR STATE AND LOCAL CYBERCRIME ENFORCEMENT

A. Digital Evidence and Forensics

For state and local law enforcement agencies to more effectively investigate and prosecute cybercrimes, they must first create effective strategies for

34. Sean Gallagher, *A Huge Ransomware Attack Messes with Texas*, WIRED (Aug. 20, 2019, 12:00 PM), https://perma.cc/X7DM-PR7X; Lucas Ropek, *How Louisiana Responded to Its Recent Ransomware Attacks*, GOV'T TECH. (Sept. 20, 2019), https://perma.cc/7R3R-J959.

35. *See* Allan Liska, *Early Findings: Review of State and Local Government Ransomware Attacks*, RECORDED FUTURE (May 10, 2019), https://perma.cc/8C88-HW9W (finding ransomware attacks against 48 states and the District of Columbia); James Sanders, *State and local governments increasingly targeted by ransomware attacks*, TECHREPUBLIC (Aug. 28, 2019, 9:09 AM), https://perma.cc/VC5G-5X8N; Fleming Shi, *Threat Spotlight: Government Ransomware Attacks*, BARACUDA (Aug. 28, 2019), https://perma.cc/8N87-PVSH (finding the majority of public ransomware attacks in 2019 have targeted state and local governments in the United States).

36. *See, e.g.*, *Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES (June 14, 2018), https://perma.cc/RK34-MZHJ; WYO. STAT. ANN. § 6-3-501 (2019).

37. 2018 Mich. Pub. Acts 95, https://perma.cc/F2SQ-X2EL. Michigan law does require the government to demonstrate those who possessed ransomware had a malicious intent to use or employ the ransomware, without authorization. *Id.* The intent requirement was an important aspect of the law to allay any concerns to the security community that the state would prosecute them for possessing ransomware for research purposes. It would also prevent a victim of a ransomware attacks that may have remnants on their computer from criminal penalty. *See* Ryan Johnston, *Possession of ransomware is now a crime in Michigan*, STATESCOOP (Apr. 5, 2018), https://perma.cc/56UE-DU8U.

38. 2018 Mich. Pub. Acts 95, https://perma.cc/F2SQ-X2EL.

39. *Id.*

obtaining, examining, and admitting digital evidence. Digital evidence is the building block of cybercrime investigations, although the proliferation of data created in the commission of traditional crimes is also exponentially growing.[40] Law enforcement leaders must invest significant resources to build their digital forensic capabilities and prioritize cases that pose the most immediate danger to the public.

The technology required for digital evidence examination is costly[41] and can require re-investment as technology advances and manufacturers no longer support older products and services. However, technology and equipment purchases are only one facet of the costs to maintain computer crime laboratories. Salaries for an adequate number of employees or examiners coupled with expensive training requirements can also hinder state and local governments with limited budgets.[42] As a result, many state and local agencies report significant digital evidence backlogs,[43] which can impact the timeliness and quality of investigations, and in some instances preclude prosecution.[44]

Many state and local agencies look to federal resources to augment their digital forensic examination capabilities. A recent survey demonstrated that 95% of law enforcement respondents sought assistance with digital evidence from outside entities.[45] As an example, since 2000, the FBI has operated a series of seventeen Regional Computer Forensics Laboratories (RCFLs)[46] in addition to the FBI's Field Offices and the National Domestic Communications Assistance Center (NDCAC). The RCFLs are spread across the nation to maximize support to state and local investigative entities. RCFLs report metrics on the number of participating state and local agencies, requests received, and forensic examinations performed.[47] State and local governments can also utilize digital forensic capabilities hosted through other federal agencies, such as the Drug Enforcement Administration, U.S. Marshals Service, and Immigration and Customs Enforcement's Homeland Security Investigations. However, periodic reviews of

40. Manhattan District Attorney Cyrus Vance has stated that nearly every investigation in his jurisdiction had a digital evidence component. *See* Joshua Philipp, *Nearly Every NYC Crime Involves Cyber, Says Manhattan DA*, THE EPOCH TIMES (Mar. 2, 2013), https://perma.cc/4FAK-XSPP.

41. For example, in 2015 SC Magazine reported Cellebrite UFED Series—a suite of products popular with law enforcement agencies—cost $15,999. *See Product Information: Cellebrite UFED Series*, SC MAGAZINE (Oct. 1, 2015), https://perma.cc/UT64-TWBV.

42. *See* POLICE EXEC. RESEARCH FORUM, *The Changing Nature of Crime and Criminal Investigations* 59 (Jan. 2018), https://perma.cc/74V6-2EAU (citing that the computer forensic unit is the most expensive unit in one police department).

43. *See* Sean E. Goodison et al., *Priority Criminal Justice Needs Initiative*, DIG. EVIDENCE & THE U.S. CRIM. JUST. SYS. (2015), https://perma.cc/57TY-KR68.

44. *See, e.g.*, Amanda Iacone, *3 More Kids Sexually Exploited as Evidence Sat Waiting in Bell Case; Lack of Manpower Exposed*, WTOP (Aug. 7, 2017, 4:32 AM), https://perma.cc/FC5U-S8JH.

45. William A. Carter & Jennifer C. Daskal, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, CTR. FOR STRATEGIC & INT'L STUD. (July 2018), https://perma.cc/V7WC-MPNP.

46. REG'L COMPUT. FORENSIC LAB., https://perma.cc/PQZ7-DH2N (last visited Sept. 30, 2019).

47. *Rocky Mountain RCFL: Regional Computer Forensics Laboratory* (2013), ROCKY MOUNTAIN RCFL, https://perma.cc/HZ8P-PZUR.

federal digital forensics laboratories[48] still note that digital evidence backlogs may make timely forensic examinations difficult for state and local investigations reliant on federal assistance. Federal facilities have a primary responsibility to aid and support federal investigations, and federal funding is not unlimited. State law enforcement agencies have therefore recognized a need to build their own digital forensic capabilities.[49]

B. Creating Economies of Scale in Digital Forensics

To adequately address the challenges associated with digital evidence, state and local governments must create economies of scale in digital forensics. State and local law enforcement have taken substantial efforts to educate state legislatures on the need for computer forensics labs,[50] as overreliance on federal grants can jeopardize sustainability.[51] For state governments, that often means assisting local agencies within their jurisdiction, [52] despite the existing strain on resources available for state criminal investigations. One promising practice that state governments have implemented is to create digital forensic capabilities at state fusion centers. While some state fusion centers cannot directly support criminal investigations, fusion centers can leverage grants from the U.S. Department of Homeland Security as initial seed money for advanced computer forensic tools.

Moreover, state and local entities recognize the need for regional cooperatives to expand capabilities and leverage technological assets. For example, one sworn officer handling digital forensics shared that his agency was considering piloting a memoranda of understanding (MOUs) to "swap" digital evidence examinations, whereby smaller agencies in the surrounding area might take simple examinations in exchange for his larger agency's handling of a complex or technically complicated case.[53] A local law enforcement entity may not have sufficient resources to stand up a full suite of capabilities at its own computer forensics laboratory, but it could purchase one technology and deconflict with surrounding local agencies to ensure a full suite of capabilities exists across the region.

C. Training

Within state and local law enforcement, there is a growing need to enhance cybercrime training opportunities. However, training is multi-faceted and must be implemented at multiple layers within an agency:

---

48. *See, e.g.*, DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S NEW JERSEY REGIONAL COMPUTER FORENSIC LABORATORY HAMILTON, NEW JERSEY (Mar. 2016), https://perma.cc/JBQ3-2ML8.

49. *See* ATT'Y GEN. OF WASH. & WASH. STATE PATROL, THE EMERGENCE, EVOLUTION AND NECESSITY OF DIGITAL FORENSIC CRIME LABS, SB 5184 (2009-10), (Oct. 30, 2009), https://perma.cc/U9AZ-X7KU (presenting results of a law enforcement needs survey to the Washington state legislature to demonstrate the need for state funding).

50. *See id.*

51. *See* Goodison et al., *supra* note 43.

52. Carter & Daskal, *supra* note 45.

53. Interview (not for attribution) (Jan. 14, 2018).

1. Digital Evidence for First Responders

All frontline officers in state and local agencies must have a preliminary understanding of how to recognize and properly seize relevant digital evidence. Agencies should train all sworn officers both at the academy and through refreshed in-service training. Digital evidence has the potential to significantly impact cases and recognition of its capabilities for aiding investigations must be understood. The content of training may also include questions necessary for enhancing investigations (e.g., soliciting authorized users of devices), procedures for effective collection of digital evidence and devices, and practical tips for enhancing investigations—such as asking suspects for their consent to share passwords.[54] Careful training can help officers prioritize digital examination requests and potentially reduce the backlog of digital evidence, allowing officers to also eliminate digital evidence that is clearly not relevant to the crime.[55]

2. Digital Evidence Forensics Training

Digital evidence examiners must have specialized training in digital extraction methods to create a robust cybercrime capability within an agency. While their skills will be required for many other criminal investigations, computer forensics are the foundation of all cybercrime investigation. Digital forensic examiners must also learn important triaging skills to adequately prioritize requests and establish effective workflows.[56]

State and local law enforcement have different models for *who* should be a digital forensic examiner—some agencies prefer sworn officers, while others rely heavily on civilian support.[57] Regardless of which model an agency selects, the demands of training compared with the demand of existing caseloads can be difficult to balance. One police chief shared that he invests heavily in recommended training for his examiners, which results in each examiner's absence from the office for two months out of the year.[58]

3. Cybercrime Investigations

Specialized investigators within cybercrime units must obtain the skills for building effective cases for computer-enabled (computer as a tool) and high-tech (computer as a target) crimes. Seasoned cybercrime investigators note that it can take approximately six months for them to be fully trained on cybercrime investigations and approximately one year to feel truly comfortable and sufficiently

54. *See, e.g.*, MASS. DIGITAL EVIDENCE CONSORTIUM, DIGITAL EVIDENCE GUIDE FOR FIRST RESPONDERS (May 2015), https://perma.cc/8S6F-BFX3.

55. *See* POLICE EXEC. RESEARCH FORUM, THE CHANGING NATURE OF CRIME AND CRIMINAL INVESTIGATIONS 61 (Jan. 2018), https://perma.cc/H5QZ-4S6Q ("For example, if detectives are at a crime scene, they might seize an old laptop with an inch of dust on it [if not properly trained].").

56. *See* Goodison et al., *supra* note 43.

57. POLICE EXEC. RESEARCH FORUM, *supra* note 55, at 56-58.

58. *Id.* at 59.

experienced in handling cybercrime cases.[59] Like many types of investigations, hands-on training is a crucial source of expertise for investigators to gain experience. As a result, participation in federal task forces is a crucial mechanism for giving state and local investigators firsthand expertise, technical assistance, and training opportunities in cybercrime investigations.[60]

There are several providers available for cybercrime investigators. One important resource is the U.S. Secret Service's National Computer Forensics Institute (NCFI), which trains law enforcement on high-tech investigative techniques at no cost.[61] However, the NCFI only trains approximately 1,200 state and local law enforcement officers per year and demand exceeds that number.[62] There are also private companies that provide discounts to state and local law enforcement through partnerships with the Multi-State Information Sharing and Analysis Center (MS-ISAC).[63] Nonprofit organizations like the National White Collar Crime Center (NW3C)[64] and SEARCH[65] also provide state and local law enforcement with important training in cybercrime investigations. To accommodate the difficulty in taking officers out of their agencies, these nonprofit providers are increasingly creating virtual training modules that are accessible online in shorter blocks of time.

Like digital evidence examination, state governments are increasingly partnering with local agencies within their jurisdiction to enhance their capabilities. Recognizing that state cybercrime units must prioritize their investigations and triage complaints, state law enforcement leaders see building capability at the local level as an essential step for enhancing cybercrime enforcement.[66] State cybercrime units look to the number of technical assistance requests and training conduct for local agencies as an important metric to measure their effectiveness.[67]

Much of the work involved with cybercrime investigations involves requests from technology or software companies, carriers, and internet service providers (ISPs),[68] either through exigent circumstances or subpoenas. As a result, it is important for state and local cybercrime detectives to liaise with their counterparts across the country to share best practices for languages in subpoenas and utilize appropriate channels from private companies' engagement with law enforcement.[69]

---

59. DEP'T OF JUSTICE, *supra* note 9, at 35.

60. DEP'T OF JUSTICE, *supra* note 9, at 37-44.

61. *See* NAT'L COMPUT. FORENSICS CTR., https://perma.cc/6JHN-TDPL.

62. Carter & Daskal, *supra* note 45.

63. For example, the SANS Institute offers reduced training for state and local governments through a bulk contract with the MS-ISAC. *See Training*, CTR. FOR INTERNET SECURITY, https://perma.cc/ZVU7-9K3Z.

64. NW3C, https://perma.cc/A3T9-QFM6 (last visited Sept. 30, 2019).

65. SEARCH, https://perma.cc/W3TQ-MPTD (last visited Sept. 30, 2019).

66. DEP'T OF JUSTICE, *supra* note 9, at 35.

67. *Id*.

68. Carter & Daskal, *supra* note 45.

69. Note that SEARCH has a robust directory of ISP providers points of contact along with subpoena requirements available at https://www.search.org/resources/isp-list/.

4. Daubert[70] Experts for Digital Evidence

Agencies must also have experts who understand the underlying basis of the technology used in a digital examination for testimony. A forensic examiner who simply utilizes technology without understanding its scientific basis will be insufficient to meet legal requirements. While forensic technology companies can provide some experts for testimony, many state and local agencies should also have a roster of experts certified in investigative techniques from their cybercrime units, fusion center personnel, or federal partners while admitting digital evidence.

D. Personnel and Management Challenges in Local and State Law Enforcement Agencies

Cybercrime investigations also present unique challenges to state and local law enforcement agencies within the confines of traditional agency policies and culture. One key issue is professional development for law enforcement officers. Traditional policing agencies require sworn officers ascending through the ranks to move to different departments and units in order to gain a broader understanding of the profession. While there are notable examples of cybercrime investigators staying within the unit following a promotion,[71] many skilled investigators will rotate to another job function following two years of service and eligibility for a promotion. These policies can severely hamper institutional knowledge, limit capabilities for cybercrime units, and raise operational costs of training particularly given the extraordinary length of time it takes for state and local cybercrime investigators to gain competency and hands-on experience throughout often lengthy computer crime investigations.

To address these challenges, some police agencies ask their investigators to commit to a minimum term while serving within the cybercrime unit.[72] Law enforcement leaders should consider instating departmental policies that allow for officers' professional development and promotion while continuing their specialized cybercrime investigative function. In the words of one local agency police chief, "We need to be recruiting for different skill sets and educational experiences than a typical boots-on-the-ground guy. We need to develop the future leaders of our department into this specialty."[73]

Aside from this key professional development challenge, there are also key strategic considerations that state and local agencies must contemplate. Several state public safety agencies have asked their legislature for additional monetary support to enhance cybercrime capabilities.[74] However, legislators must weigh a

70. The federal standard whereby an expert witness's scientific testimony is properly based on scientifically valid methodology. *See* Daubert v. Merrell Dow Pharm. Inc., 509 U.S. 579 (1993).

71. *ISP's Cohen becomes captain*, HERALD TIMES ONLINE (Nov. 21, 2015), https://perma.cc/YH9L-59EP.

72. DEP'T OF JUSTICE, *supra* note 9, at 35.

73. POLICE EXEC. RESEARCH FORUM, *supra* note 55, at 6.

74. DEP'T OF JUSTICE, *supra* note 9 at 7, 20, 44.

competing variety of public safety priorities. It is therefore important to report back progress and assess the effectiveness of state and local cybercrime units.

Defining success in cybercrime enforcement is a challenging area for state and local agencies. Unlike patrol areas that may look at crime statistics like Compstat, or homicide units that measure their clearance rate, cybercrime units must wrestle with the issue that many of their investigations may not lead to arrest or quantifiable metrics demonstrating crime reduction. As a result, state and local cybercrime units should look to other benchmarks. One state police captain shared that his unit's highest value came from intelligence it produced for the state fusion center.[75]

Recent cybersecurity incidents demonstrate this value. For example, in July 2019, Louisiana experienced a series of coordinated ransomware attacks targeting local school parish districts in the state, prompting Governor John Bel Edwards to declare a state of emergency.[76] The Louisiana State Police's cybercrime unit analyzed the malware and was able to provide crucial context behind the threat. The state credits the LSP's forensic examination of the virus[77] with preventing the spread of the Ryuk ransomware to seven additional school districts that had also been targeted.[78] As a result, state and local law enforcement not only have evidence of cybercrime units' generation of intelligence, but *actionable* intelligence that can reduce cybercrime.

In addition to intelligence value that minimizes the impact of cybercrime, there are other benchmarks that state and local agencies also employ. Agencies collect metrics on the number of cybercrime tips investigated and cases opened, monetary losses prevented and/or recovered, technical assistance and training requests fulfilled for outside agencies, and investigative hours.[79]

E. The Judicial System

Building capacity, however, is not only important for state and local law enforcement agencies. For cybercrime cases that do make it to trial, litigators and judicial officials must have a working knowledge of the basic technical components of a cybercrime to inform good outcomes. The U.S. Secret Service's National Computer Forensics Institute (NCFI) offers specific courses for prosecutors and judges free of charge on topics like digital evidence.[80] However, training opportunities are still limited for state prosecutors and judges, particularly with the demands of tight judicial calendars. Furthermore, achieving good outcomes in cybercrime cases requires not only educating

75. Interview (not for attribution) (June 19, 2019).

76. LA. EXEC. DEP'T, PROCLAMATION NO. 115 JBE 2019, STATE OF EMERGENCY – CYBERSECURITY (2019), https://perma.cc/U6BG-L9Y7.

77. James Waskom, Director, La. Governor's Office of Homeland Security and Emergency Preparedness, Remarks at the CISA Cybersecurity Summit: State Cyber Emergency Declarations (Sept. 19, 2019).

78. Ropek, *supra* note 34.

79. DEP'T OF JUSTICE, *supra* note 9, at 34-35.

80. NAT'L COMPUT. FORENSICS CTR., *supra* note 61.

prosecutors, but also the defense attorneys responsible for zealously advocating on behalf of criminal defendants.[81]

In addition to substantive computer crime law, there are procedural issues at the state level that state governments must also address. One such example is the authentication of digital evidence. Recognizing the need to reform evidentiary rules to account for the proliferation of digital evidence, amendments to Federal Rules of Evidence 902(13) & (14)[82] passed in December of 2018. Several states have followed suit in creating standard procedures for authenticating digital evidence,[83] but most states generally lag behind the federal rules. State courts should consider adopting the federal framework to make authentication smoother. Litigators must also prepare strategies following admittance for convincing juries of the trustworthiness of digital evidence to enhance cybercrime cases.[84]

F. Task Forces

On the state and local level, there is a common misperception that federal law enforcement will actively investigate and lead the bulk of cybercrime investigations.[85] This distinguishes cybercrime from most other types of crime in the United States, where the 18,000 state and local agencies handle the majority of investigations in a bottom-up approach. Federal agencies can only focus investigative resources in the most serious of cases, despite the aggregate impact of routine cybercrime on the economy.[86] For example, the FBI will only open an investigation into computer-enabled theft or fraud if it exceeds a specific threshold of monetary losses.[87] To begin to see a substantial closure of the cybercrime enforcement gap, state and local agencies must build their capacity to handle cybercrime investigations and prosecutions so that every level of government is leveraging all available capabilities and resources.

Limitations on federal resources notwithstanding, state and local law cybercrime units cite partnerships with federal agencies as one of the most effective force multipliers for their enforcement efforts.[88] Common cyber-related task forces with state and local participation are FBI Cyber Task Forces, USSS Electronic Crimes Task Forces, Internet Crimes Against Children (ICAC) for child exploitation, and HIDTA task forces for dark web investigations, involving not only the Drug Enforcement Administration, but additional federal agencies

81. *See* Goodison et al., *supra* note 43.

82. FED. R. EVID. 902(13)-(14).

83. *See*, *e.g.*, ARIZ. R. EVID. 902; ILL. R. EVID. 803; N.D. R. EVID. 902.

84. For example, some litigators have debated over the effectiveness of using "hash values," or algorithm-based digital identifiers, with juries. *See, e.g.*, Don L. Lewis, *The Hash Algorithm Dilemma – Hash Value Collisions*, FORENSIC MAG. (Dec. 1, 2008), https://perma.cc/Q5E2-FBY5.

85. DEP'T OF JUSTICE, *supra* note 9, at 21.

86. *See generally* Michael Garcia et al., *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*, 96 NEB. L. REV. 252 (2017).

87. DEP'T OF JUSTICE, *supra* note 9, at 17.

88. *Id*. at 37-38.

like Immigration and Customs Enforcement's Homeland Security Investigations or the United States Postal Inspection Service.

The task force model for cybercrime can unlock important benefits for state and local agencies, including:

- Assistance with multi-jurisdictional cases, both for legal processes such as mutual legal assistance treaties (MLAT) and relationship-building through federal field offices;
- Hands-on, experiential cybercrime investigations training;
- Deconfliction of cases where multiple agencies may be investigating a lead;
- State and local access to sensitive federal databases, including clearances; and
- Aggregation of cases, tips, or leads through intelligence fusion.[89]

Task forces can provide a direct solution to cases where federal agencies do not have the manhours or the mandate to open a case due to stringent investigative thresholds. As an example, in 2013, the FBI launched Operation Wellspring as a pilot program to create a referral process between Cyber Task Forces and the IC3.[90] During the pilot program with the Utah Department of Public Safety (DPS), IC3 provided the DPS's Cyber Crimes Unit with approximately twenty-five "incident packets" for review, aggregating incidents from 900 victims and $2.5 million total in losses.[91] After initial investigation, the Utah DPS Cyber Crimes Unit opened nine cases with the assistance of the FBI.[92] The pilot program has since expanded to a total of thirteen field offices across the county.[93] Through Wellspring, the IC3 provided a total of 123 referrals to thirteen Cyber Task Forces in 2018, involving a total of 1,192 victims and aggregate financial losses of $28.1 million.[94]

G. Multi-Jurisdictional Investigations

Another challenge associated with state and local cybercrime enforcement is its multi-jurisdictional nature. Internet-based crimes cross geographic borders, or exist in cyberspace,[95] making already-complex and technical investigations all

89. *Id.*

90. FED. BUREAU OF INVESTIGATION, *supra* note 2, at 9.

91. UTAH DEP'T OF PUBLIC SAFETY, ESTABLISHING A CYBER CRIMES UNIT WHITE PAPER (2014), http://docplayer.net/10626312-Establishing-a-state-cyber-crimes-unit-white-paper.html.

92. *Id.*

93. FED. BUREAU OF INVESTIGATION, *supra* note 2.

94. *Id.*

95. KRISTIN M. FINKLEA, CONG. RESEARCH CTR., THE INTERPLAY OF BORDERS, TURF, CYBERSPACE, AND JURISDICTION: ISSUES CONFRONTING U.S. LAW ENFORCEMENT (2013), https://perma.cc/XB7T-B6LL.

the more difficult for state and local law enforcement agencies. Complications are both legal and practical in nature. For example, the primary legal vehicle for overseas data requests, mutual legal assistance (MLA) requests, takes an average of ten months to fulfill.[96] Cybercrime cases that require in-person witness testimony mean that state and local agencies may have to expend significant resources on travel funding with limited budgets. Additionally, defendants who are foreign nationals may walk free from criminal liability if their country of origin does not want to extradite them to the United States or prosecute them, especially if federal law enforcement—such as the U.S. Secret Service—is unable to lure them to a third party country.

Despite associated issues, state and local law enforcement agencies have started developing complex, cross-jurisdictional investigations with other local, state, federal, and international counterparts. These notable cases demonstrate that cases can move forward even though key evidence, witnesses, or suspects reside out of the state's geographic boundaries. One such case involved a computer-enabled scheme to defraud the Hawaii government involving twenty-four New Jersey defendants.[97] New Jersey brought charges following a joint investigation between the New Jersey Division of Criminal Justice, New Jersey State Police Cyber Crimes Unit, New Jersey Division of Taxation, and State of Hawaii Department of Taxation.[98]

State and local investigations can also reach across international borders. For example, in 2015, a detective sergeant in the Johns Creek, Georgia Police Department investigated a swatting case where the perpetrator was responsible for over 40 additional swatting calls outside his jurisdiction.[99] Working with the FBI's Atlanta Field Office and the DOJ's legal attaché in Canada, he was able to turn over sufficient evidence that allowed Canadian police to charge 46 counts of criminal harassment, resulting in the juvenile perpetrator pleading to 26 counts and serving 16 months in jail.[100]

State and local agencies must continue to expend their resources on multi-jurisdictional cybercrime cases, even if it means expending additional resources, assisting victims outside their primary area of responsibility or turning over evidence for foreign law enforcement agencies for prosecution.

---

96. RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227 (2013), https://perma.cc/TFX9-9ZVP.

97. *See* Press Release from the State of Hawaii, *Release: Indictment Charges 24 New Jersey Residents in Tax Fraud Scheme in which they Allegedly Stole Nearly $250,000 from the State of Hawaii* (July 24, 2018), https://perma.cc/ZZ5V-G3ZM ("'Just as we aggressively prosecute those who steal from the State of New Jersey and its taxpayers, we stand ready to investigate and charge those who engage in tax fraud that crosses jurisdictional lines,' said Director Veronica Allende of the [New Jersey] Division of Criminal Justice.").

98. *Id.*

99. Jason Fagone, *The Serial Swatter*, N.Y. TIMES (Nov. 24, 2015), https://perma.cc/F5N9-F72K.

100. *Id.*

H. Reducing the Victim Pool Through Prevention

State governments also recognize the need to emphasize cybercrime prevention. Law enforcement agencies across the United States have long recognized the crucial role in educating the community for crime prevention and public safety purposes, but preventative training and awareness programs for businesses and communities are just in their infancy. Of course, the technical sophistication of many cybercrime actors—individuals, criminal organizations, and nation states—makes it virtually impossible for any computer to be impenetrable. However, by some estimates roughly 80% of cyber incidents could be prevented with basic cyber hygiene.[101] State and local executives have recognized the importance of changing the culture surrounding cybercrime and fighting complacency in small businesses and private individuals.

As a result, governors, as the chief executives of their states, are playing a key role in enhancing community awareness. In 2018, at least eighteen governors proclaimed October to be cybersecurity awareness month in their respective states, leveraging the power of the bully pulpit.[102] Mayors and city councils have also

101. DEP'T OF HOMELAND SECURITY, HOMELAND SECURITY ADVISORY COUNCIL, INTERIM REPORT OF THE STATE, LOCAL, TRIBAL AND TERRITORIAL CYBERSECURITY COMMITTEE 20 (2019), https://perma.cc/DAZ6-SGWY.

102. *See* Press Release from Governor Ivey, *Gov. Ivey Proclaims October As Cybersecurity Awareness Month* (Sept. 26, 2018), https://perma.cc/XL2N-DDWP; Press Release from Governor Doug Ducey, *Brief: October is Cybersecurity Awareness Month* (Oct. 19, 2018), https://perma.cc/5K67-W99T; Proclamation from Governor Asa Hutchinson (Sept. 20, 2018), https://perma.cc/YJT6-5RF4; Proclamation from the State of Delaware Office of the Governor, *Proclamation in Observance of Cyber Security Awareness Month* (2018), https://perma.cc/7WXU-XFJH; Proclamation from Governor David Y. Ige, *Cyber Security Awareness Month* (Sept. 19, 2018), https://perma.cc/79J9-M3SN; *see October is Cybersecurity Awareness Month*, OFFICE OF THE GOVERNOR OF IOWA KIM REYNOLDS, https://governor.iowa.gov/2018/10/october-is-cybersecurity-awareness-month; Proclamation from Governor Rick Snyder, *October 2018: Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/WGP6-VBZY; *Governor Mark Dayton Proclaims "Cybersecurity Awareness Month" in Minnesota, Creating Awareness Around the Critical Issue of Cybersecurity*, MINN. IT SERVS. (Oct. 16, 2018), https://perma.cc/Z7H7-RB27; Proclamation from Governor Phil Bryant, *National Cyber Security Awareness Month* (Sept. 4, 2018), https://perma.cc/N82C-8HS6; Press Release from Governor Michael L. Parson, *Governor Parson and Secretary Aschroft Highlight Missouri's Readiness to Defend Against Cyber Threats* (Nov. 1, 2018), https://perma.cc/2J7A-AMSP; *Governor Steve Bullock Acknowledges October as National Cybersecurity Awareness Month*, MONT. STATE INFO. TECH. SERVS. DIV. (Oct. 11, 2019), https://perma.cc/4YKQ-DRYZ; Proclamation from Governor Christopher T. Sununu, *Cybersecurity Awareness Month* (Oct. 3, 2018), https://perma.cc/XN6G-YMHD; Press Release from the N.J. Office of Homeland Security & Preparedness, *Governor Phil Murphy Signs Proclamation Declaring October As Cybersecurity Awareness Month in New Jersey* (Sept. 2019), https://www.njhomelandsecurity.gov/media/governor-phil-murphy-signs-proclamation-declaring-october-as-cybersecurity-awareness-month-in-new-jersey; Proclamation from Governor Andrew Cuomo, *Cyber Security Awareness Month* (Oct. 1, 2018), https://perma.cc/798Q-G43C; Proclamation from Governor Roy Cooper, *National Cybersecurity Awareness Month* (Sept. 28, 2018), https://perma.cc/84PA-L4EP; Proclamation from Governor Doug Burgum, *Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/L6HP-3YSJ; Proclamation from Governor Kate Brown, *Cyber Security Awareness Month* (Oct. 19, 2018), https://perma.cc/4QYQ-DHNJ; Proclamation from Governor Ralph S. Northam, *Cybersecurity Awareness Month* (Oct. 1, 2019), https://perma.cc/LRY8-BXKM.

issued similar proclamations.[103] However, cybersecurity awareness must be incorporated into larger statewide cybersecurity strategies. Recent data demonstrates that nine out of ten governors have established cybersecurity governance bodies,[104] many of which have labelled greater community awareness a key tenet of their statewide cybersecurity strategy.[105] For example, Governor Doug Ducey's Arizona Cybersecurity Team (ACT) is establishing a proactive cybersecurity awareness campaign, including training events for citizens and businesses in Arizona, with the assistance of private sector cybersecurity subject matter experts and marketing specialists.[106]

State governments have also incorporated private citizens into their cybersecurity information sharing activities. In New Jersey, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)—housed under the New Jersey Office of Homeland Security & Emergency Preparedness—provides bulletins, alerts, and advisories on cybersecurity threats.[107] Private citizens and business can all sign up to become members, regardless of their residency or affiliation with the state of New Jersey, and the NJCCIC also provides practical cybersecurity tips for community members.[108]

Cybercrime experts also recognize the need for proactive programming to reduce revictimization in cybercrime. Victims can experience frustration or embarrassment when they make the effort to report cybercrime but law enforcement does not open an investigation.[109] So it is critical for governments to take a victim-centered approach in connecting cybercrime victims to services and educating them on better cyber hygiene. This is particularly true of elderly cybercrime victims, who may be unfamiliar with existing technology and potential vulnerabilities. As a result, organizations like the American Association of Retired Persons (AARP) have stood up resource centers along with hotlines for elderly victims of computer-enabled crime and fraud.[110] One promising program which is rapidly expanding is the Cybercrime Support Network's 211 pilot program[111] that leverages existing helpline infrastructure to connect cybercrime and online fraud victims to resources, support, and training and to encourage reporting to law enforcement. The mission of the 211 program is to reduce revictimization among the growing population of cybercrime victims. At this juncture, the

103. *See, e.g.*, Proclamation from the City of Boston, *Cyber Security Awareness Month* (Oct. 1, 2018), https://perma.cc/599K-QUT8; Proclamation from the City of San Jose, *Cyber Security Awareness Month* (Oct. 2018), https://perma.cc/S6QP-B8WG.

104. Doug Robinson & Srini Subramanian, *supra* note 25, at 16.

105. *Louisiana Cybersecurity Awareness Month*, LA. CYBERSECURITY COMM'N (Oct. 2019), https://perma.cc/AK68-VKJC.

106. *Arizona Cybersecurity Team*, OFFICE OF THE GOVERNOR DOUG DUCEY, https://perma.cc/GQP2-K9QT (last visited Oct. 1, 2019).

107. N.J. CYBERSECURITY & COMMC'N INTEGRATION CELL, https://www.cyber.nj.gov/ (last visited Oct. 1, 2019).

108. *Id.*

109. DEP'T OF JUSTICE, *supra* note 9, at 20.

110. *Scams & Fraud*, AARP, https://perma.cc/E9KY-XHTE (last visited Nov. 6, 2019).

111. *Id.*

Cybercrime Support Network has partnered with several local regions and has piloted statewide in the state of Rhode Island.

CONCLUSION

State and local governments are at the forefront of both traditional criminal enforcement and bearing the brunt of novel cyber threats on their government networks, critical infrastructure, businesses, and citizens. Despite this unique role, states have been slow to develop capabilities towards meaningfully enforcing cybercrimes. The federal government cannot address cybercrime alone and must partner with state and local agencies to enhance their investigation and prosecution of cybercrime, as with all other types of crime.

This paper outlines the challenges and opportunities for state and local governments looking to enhance their cybercrime enforcement. It provides a detailed discussion of the legal framework at the state level—exploring how states have created computer crime codes that mostly model federal legislation, but tailor them in significant ways. State governments should look at their computer crime acts to determine the best approach and to ensure that there are no gaps in their authorities for growing cybercrime threats.

But, perhaps mostly importantly, this article also recognizes that capacity-building is the much more challenging work. States need concrete strategies to handle digital evidence throughout the justice system. They must also equip state and local law enforcement with the training, executive management, and partnerships required for effective enforcement. States must also pilot initiatives to emphasize prevention and reduce the pool of cybercrime victims. Altogether, cybercrime should be treated no differently than any other crime in the United States. State and local governments must increase their authority and capacity to combat this growing threat and close the cybercrime enforcement gap.