Staff: Committee on Technology

Irene Byhovsky, Legislative Counsel

Charles Kim, Legislative Policy Analyst

Florentine Kabore, Finance Analyst



##### THE COUNCIL

##### COMMITTEE REPORT OF THE INFRASTRUCTURE DIVISION

*Jeffrey Baker, Legislative Director*

*Terzah Nasser, Deputy Director, Infrastructure*

**COMMITTEE ON TECHNOLOGY**

*Hon. Robert Holden, Chairperson*

**August 27, 2020**

**INT. NO. 1297-A:** By Council Members Torres, Koo, Brannan, Holden, Cornegy and Gibson

**TITLE:** A Local Law to amend the New York city charter, in relation to the creation of an office of cyber command

**CHARTER:** Adds section 20-j

1. **INTRODUCTION**

On Thursday, August 27, 2020, the Committee on Technology, chaired by Council Member Robert Holden, held a hearing to consider Int. No. 1297-A. The committee previously heard the original version of the bill, Int. No. 1297, on December 13, 2018. More information on Int. No. 1297-A and materials from the previous hearing can be accessed online at <https://go.usa.gov/xGcKh>.

1. **BACKGROUND**

As cybersecurity becomes the new arms race between hacker and system, or illegitimate versus legitimate user, governments and private entities alike must develop resilient policies to address an insufficiency of laws and regulations.[[1]](#footnote-1) Cyber threats can result in data breaches and can significantly affect critical infrastructure.

The centrality of digital technology in all facets of modern life coupled with the vulnerability of the technologies and infrastructures to threats and damage necessitates close attention to cybersecurity. Cyber attacks[[2]](#footnote-2) are increasing at an alarming pace and could disrupt the supply of essential services people take for granted, including water, healthcare, electricity or mobile services.[[3]](#footnote-3) Threats are diverse and can have different origins including criminal, politically motivated, terrorist or state-sponsored attacks, as well as unintentional mistakes.

Cyber threats can result in data breaches or significantly affect critical infrastructure. In a recent hacking event, hackers compromised the confidential information of 145 million Equifax records in the United States, including 8,447,840[[4]](#footnote-4) in New York[[5]](#footnote-5), 500 million Marriott records,[[6]](#footnote-6) 145 million eBay records; 130 million Heartland records; 76 million JPMorgan Chase client records; 80 million Anthem records; 77 million Sony records; 70 million Target records; and 56 million Home Depot records.[[7]](#footnote-7)

As our physical infrastructure becomes increasingly digitalized, it also becomes increasingly vulnerable to potential cyber attacks.[[8]](#footnote-8) Hackers, for example, have been trying to compromise the electrical infrastructure of the United States (U.S.). Other hackers successfully cut off power to hundreds of thousands of people throughout the Ukraine in 2015, and again in 2016. [[9]](#footnote-9)  In the Ukraine, a power distribution station near Kiev unexpectedly switched off, leaving the northern part of the capital without electricity.[[10]](#footnote-10)

Beyond our energy infrastructure, traffic signals are generally susceptible to being hijacked, as numerous demonstrations have proven.[[11]](#footnote-11) Therefore, the City needs to ensure its systems continue to operate as intended and to meet the standards and best practices of cybersecurity.

1. **The Office of New York City Cyber Command**

The Office of New York Cyber Command (“NYC Cyber Command”) was established in 2017 pursuant to Executive Order 28 by Mayor Bill de Blasio. NYC Cyber Command is considered a center for cyber defense strategies in New York City. NYC Cyber Command works across more than 100 agencies and offices to prevent, detect, respond, and recover from cyber threats. NYC Cyber Command is committed to protecting NYC infrastructure and critical systems from malicious attacks through the use of the latest technologies, public-private partnerships, and regular training and exercises for City employees. In signing the executive order, Mayor de Blasio highlighted the need for the city to have centralized cyber defense and accountability to protect the City information infrastructure and City residents from cyber attacks.

The legislation before the Committee would codify New York Cyber Command to ensure that this centralized cyber defensecenter survives successive mayoralties and continues to protect the critical infrastructure of the City, defend from cyber-attacks and promote prosperity by nurturing a secure, thriving digital economy.

1. **ANALYSIS OF INT. NO. 1297-A**

Int. No. 1297-A would codify NYC Cyber Command into the Charter. This bill would provide NYC Cyber Command with the power and duty to establish cyber-security policies and standards for the city agencies, train appropriate city officers and employees on cybersecurity policies and standards, and direct cybersecurity defense and responses to cyber-attacks.

The bill would take effect immediately.

**Update**

On Thursday, August 27, 2020, the Committee adopted Int. No. 1297-A by a vote of six in the affirmative, zero in the negative, and zero abstentions.

[This page intentionally left blank.]

Int. No. 1297-A

By Council Members Torres, Koo, Brannan, Holden, Cornegy and Gibson

..Title

A Local Law to amend the New York city charter, in relation to the creation of an office of cyber command

..Body

Be it enacted by the Council as follows:

Section 1. Chapter 1 of the New York city charter is amended by adding a new section 20-j to read as follows:

§ 20-j Office of cyber command. a. The mayor shall establish an office of cyber command. Such office may be established in the executive office of the mayor or as a separate office or within any department the head of which is appointed by the mayor. Such office shall be headed by a director who shall be appointed by the mayor or the head of such department and who shall serve as the chief information security officer of the city.

b. Powers and duties. The director, in coordination with the commissioner of information technology and telecommunications as appropriate, shall have the power and duty to:

1. establish and regularly update cybersecurity policies and standards for city agencies;

2. regularly train appropriate city officers and employees on cybersecurity policies and standards;

3. review, at the request of the mayor, the budget priorities of all agencies for programs related to cybersecurity, and recommend to the mayor budget priorities among such programs;

4. at the direction of the deputy mayor for operations or another designee of the mayor, require any city agency to furnish data and information that is necessary to ensure the compliance of city agencies with cybersecurity policies and standards;

5. direct cybersecurity defense and response, in coordination with the department of emergency management as appropriate; and

6. perform such other responsibilities with respect to cybersecurity, including responsibilities delegated elsewhere by the charter, as the mayor shall direct.

c. Agency cooperation. All city agencies shall cooperate with the office so as to ensure the efficient performance of its duties.

§ 2. This local law takes effect immediately.

IB

LS 7962

8/19/20 11 pm

1. John P. Dever, Captain James A. Dever, *A Democracy of Users*, 6 JL & Cyber Warfare 8, 9 [2017]. [↑](#footnote-ref-1)
2. Cyber attacks come in many forms: denials of service, malware, phishing, infected thumb drives, and unauthorized access to computer systems by third parties. The means of attack are only limited by the imaginations of the attackers. The consequences of cyber attacks are also myriad: stolen intellectual property, stolen credit card information, stolen social security numbers, paralyzed computer systems, and tarnished brands due to the ensuing lack of public trust in the hacked entity.Christopher C. French, *Insuring Against Cyber Risk: The Evolution of an Industry Introduction*, 122 Penn St L Rev 607, 607-08 [2018]. [↑](#footnote-ref-2)
3. *See* John P. Dever, Captain James A. Dever, *A Democracy of Users*, 6 JL & Cyber Warfare 8, 27-28 [2017]. [↑](#footnote-ref-3)
4. 2017 Data Breaches Reported to the New York Attorney General’s Office, p.1, <https://ag.ny.gov/sites/default/files/data_breach_report_2017.pdf>. [↑](#footnote-ref-4)
5. In 2017, companies and other entities reported a record-breaking 1,583 breaches to the New York State Office of the Attorney General. The breaches exposed the personal records of 9.2 million New Yorkers; *see* 2017 Data Breaches Reported to the New York Attorney General’s Office, p.1, <https://ag.ny.gov/sites/default/files/data_breach_report_2017.pdf>. [↑](#footnote-ref-5)
6. # David Sanger, *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing, NYTimes, December 11, 2018,* [*https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html*](https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html)*.*

   [↑](#footnote-ref-6)
7. Marian K. Riedy & Bartlomiej Hanus, [Yes, Your Personal Data Is at Risk: Get over It!, 19 SMU SCI. & TECH. L. REV. 3, 12 (2016)](https://1.next.westlaw.com/Link/Document/FullText?findType=Y&serNum=0449220372&pubNum=0205071&originatingDoc=Ibc600bdaa00911e79bef99c0ee06c731&refType=LR&fi=co_pp_sp_205071_12&originationContext=document&transitionType=DocumentItem&contextData=(sc.Search)#co_pp_sp_205071_12). [↑](#footnote-ref-7)
8. # Ellis Talton, *A Lack of Cybersecurity Funding and Expertise Threatens U.S. Infrastructure*, Forbes, April 23, 2018, <https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#10e8ce7f49e0>.

   [↑](#footnote-ref-8)
9. *Id.* [↑](#footnote-ref-9)
10. # The outage amounted to 200 megawatts of capacity, equivalent to about a fifth of the capital’s energy consumption at night Pavel Poliuyk, *Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid*, Reuters, December 20, 2016, <https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks/ukraine-investigates-suspected-cyber-attack-on-kiev-power-grid-idUSKBN1491ZF>.

    [↑](#footnote-ref-10)
11. # Ellis Talton, *A Lack of Cybersecurity Funding and Expertise Threatens U.S. Infrastructure*, Forbes, April 23, 2018, <https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#10e8ce7f49e0>.

    [↑](#footnote-ref-11)