Big business, academia and the state team up to launch “Cyber NYC” spy program

Leslie Murtagh
26 July 2019

A “Cyber Boot Camp” headed by computer programming school Fullstack Academy began its first round of courses in June, kicking off a $100M cybersecurity initiative by the New York City Economic Development Corporation (NYCEDC).

The NYCEDC plans to develop New York City as a center of state/corporate internet surveillance. The program, called Cyber NYC, has already opened two large facilities in Manhattan run by Israeli venture capital and innovation companies and established two major educational initiatives intended to “create the next generation of cybersecurity experts.”

While the term cybersecurity is often used to mean protecting corporate databases and computer systems from penetration or attack, it has taken on new meaning since the Democratic Party created the sham of Russian “meddling” in the 2016 US election to explain Donald Trump’s victory, rather than wide-spread disgust at the ruling establishment.

These claims have served to justify massive surveillance and censorship measures across the internet, including Google, Facebook and Twitter, seeking to block the spread of and access to oppositional views under the guise of combating “fake news.”

An examination of the Cyber NYC’s partners and investors exposes a full-on collaboration between academia, major corporations and US and Israeli military-intelligence agencies to step up cyber-surveillance and internet censorship.

The organization behind Cyber NYC, NYCEDC, is a nonprofit that operates between the public and private sectors and functions as the “primary economic development vehicle” for New York City, mainly through real estate investment. It currently controls 60 million square feet of city assets.

The organization’s 27-member Board of Directors is comprised of Wall Street investors, corporate CEOs and lawyers, such as William S. Floyd, head of external affairs for Google New York, Democratic Party public officials, and representatives of big real estate firms. One notable member is Kathryn S. Wylde, a leading advocate of the privatization of public housing in New York and chair of the one of the main employers’ organization in the city, the Partnership for New York City.

Board members are approved by the mayor, who appoints seven directly. The NYCEDC has played a prominent role in making New York City obscenely profitable for real estate investors and unaffordable for millions of working people.

According to a NYCEDC press release, Cyber NYC is set to “create the next billion-dollar opportunity in cybersecurity,” while creating 10,000 new jobs and enrolling 9,000 students in the coming decade. It was funded with $70 million of private investment and $30 million of city financing. Partners include Facebook, Goldman Sachs, Mastercard, City University of New York (CUNY), New York University (NYU), Columbia University, Cornell Tech, LaGuardia Community College, and the NYC Mayor’s Office.

There are four interconnected initiatives established by the Cyber NYC program: a 15,000-square-foot “Global Cyber Center” in the Chelsea neighborhood of Manhattan, seeking to “foster international collaboration and innovation”; a 50,000-square-foot “Hub.NYC” facility in the SoHo area that will work to “breed and develop major cybersecurity companies in New York City”; an “Applied Learning Initiative,” which partners with the New York academic community and Facebook to offer new certifications and degree programs in cybersecurity and the “Cyber Boot Camp” for “industry-specific cybersecurity practices.”

The Global Cyber Center will provide programming for corporations, host industry-specific events, and create virtual testing grounds, all aiming to “facilitate strategic investments, commercialization, and implementation of cyber technologies.” The center is being run by Israeli “corporate innovation expert” company SOSA, which recently worked with leading Israeli defense company Rafael to host a “Drones Startup Challenge Event” in Tel Aviv.

Out of thirteen named investment firms funding the Global

Cyber Center, ten have direct connections to the US or Israeli defense departments, with most firms being founded by individuals formerly in elite US or Israeli military-intelligence forces.

Eric Schmidt’s Innovation Endeavors is also a prominent investor in the Global Cyber Center. Schmidt is Google’s former CEO, who oversaw both the implementation of Google algorithms that censor search results critical of the US government—including the WSWS and other prominent left-wing and anti-war websites—as well as Project Maven, the Pentagon’s AI collaboration with Google for the use in the US drone murder program.

Schmidt currently chairs the Pentagon’s Defense Innovation Advisory Board, which aims to “bring the technological innovation and best practice of Silicon Valley to the US Military.” Another co-founder of Innovation Endeavors, Dror Berman, is a former member of an “elite Special Forces unit of the Intelligence Corps of the Israeli Defense Force.”

Other investors include Glilot Capital Partners, which was founded by Gordon England, former US Deputy Secretary of Defense and US Secretary of the Navy; Team8, which is made up of “former leaders of the Israeli Defense Force’s technology and intelligence Unit 8200”—the equivalent of the US National Security Agency (NSA); and Blumberg Capital, which includes Idan Nurick, who “led computer science R&D teams and the largest cyber operations project in Unit 8200,” as a principal.

The other Cyber NYC facility established, Hub.NYC, is the city’s first international cybersecurity investment hub, seeking to “support growth-stage startups, facilitating access to clients, business support, and investment, with the goal of growing them into major cybersecurity companies in New York City.” Hub.NYC is run by Jerusalem Venture Partners, a top Israeli venture capital firm founded by wealthy businessman and Israeli Labor Party politician, Erel Margalit.

Cyber NYC has close ties with academia. The Applied Learning Initiative works with CUNY, NYU, Columbia, and Cornell Tech, offering new Cybersecurity Studies graduate programs.

The program’s collaboration with Facebook is significant. Facebook, in cooperation with international governments, currently employs an army of 30,000 censors primarily focused on “speech prevention,” working “to identify misinformation and reduce its distribution”—that is, any opinions that differ from mainstream news outlets aligned with the state.

Some graduate programs have already been launched, such as NYU Tandon School of Engineering’s new online Cybersecurity Master’s Degree Program, which is offering a heavily discounted scholarship for US citizens, costing $16,000 for the two-to-three-year program. The master’s program was developed in partnership with NYC Cyber Command, the city’s centralized cyber defense organization created by Mayor de Blasio’s executive order in 2017, as well as with Booz Allen Hamilton, a major contractor with the National Security Agency (NSA). NYU Tandon is designated a Center of Excellence in Information Assurance, Research, and Cyber Operations by the NSA.

Under the Applied Learning Initiative, CUNY has created a citywide Cybersecurity Discipline Council to “connect the academic and private sectors” while Columbia University is connecting “inventors of patented cybersecurity technologies with experienced entrepreneurial talent to launch new cybersecurity startups, accelerating innovation and commercialization,” with an emphasis on doing this “as quickly as possible.”

Fullstack Academy’s Cyber NYC’s Cyber Boot Camp aims to get non-tech savvy, “disadvantaged” New Yorkers—the first class of 24 students all received full-tuition scholarships—up to snuff and ready for industry dispatch in just 19 weeks, flaunting an average entry-level salary of $85,000. The program seeks to place over 1,000 individuals in cybersecurity jobs over the next three years.

Fullstack Academy’s website states that “technology today is more accessible than it’s ever been—but it’s also more of a liability.” As an example, it notes that, “government-sponsored bots disrupted an election”—referring to false claims that Russian social media bots impacted the 2016 US election.

The Cyber NYC program, in short, is seeking to train a new cadre of cyber-spies to work for the intelligence agencies or major companies that work closely with them. The program points to a new standardization of ramped up internet censorship and cyber surveillance that will be implemented and enforced as far and wide as possible on the working class in order to suppress any expression of opposition to war and capitalism.