World Socialist Web Site wsws.org

New York University: A center of militarism, mass surveillance and censorship: Part 2

NYU’s role in “cybersecurity” and mass surveillance

The IYSSE at NYU
20 March 2018

PART ONE | PART TWO | PART THREE

This is the second in a three-part series. The first part, “NYU and the preparations of US imperialism for world war” is posted here.

NYU is not only involved in war planning and recruiting agents. It also functions as a center for research and training for the US war machine and state apparatus. Among the most significant areas of NYU’s activities in this respect is its Center for Cybersecurity.

Cybersecurity is broadly defined as ensuring the security of information and data systems. With the digitization of the economy, it is a significant concern for companies and banks as well as states and the military. Cybersecurity has also become a central component of contemporary warfare. It encompasses not only defending the “security” of cyber systems, but also developing technologies to hack into such systems.

The United States has launched several notorious cyber-attacks on Iran as part of its decades-long strategy to encircle and economically undermine the Iranian regime. Moreover, the US military is involved in what it calls a “cyber arms race” in which its principal targets are, at least for now, Russia and China.

The US military, the NSA and the Department of Homeland Security, therefore, have focused many of their resources in academia on collaborating with universities to train a new generation of “cybersecurity” experts. A 2015 report by *Vice News* explained that the most militarized universities in the US now mostly research not “traditional weapons systems” but “intelligence technologies, cyber security, and big data analytics.”

NYU’s Center for Cybersecurity

NYU was one of the first universities in the US to create a “center for cybersecurity.” The center has a team of 19 people who work in both New York City and on NYU’s Abu Dhabi campus. NYU offers a minor as well as a master’s program in cybersecurity that has been officially accredited by the NSA.

In 2014, NYU became a Center of Academic Excellence (CAE) in Cyper Operations for its graduate program in cyper operations. The Department of Homeland Security and the NSA jointly sponsor the program. As of 2016, only 18 other US colleges were CAEs in Cyper Operations.

As part of this program, students at NYU can apply for A Scholarship for Service Partnership for Interdisciplinary Research and Education (ASPIRE). The scholarship completely covers tuition—which at NYU is over $45,000 a year—and provides a stipend of up to $22,500 for undergraduates and $34,000 for master’s degree and doctoral students per academic year.

In exchange for accepting the scholarship, students are required to do a related internship over the summer break, and after graduating must spend two years in government service. According to a 2015 article in the *Guardian*, roughly 29 percent of the students who receive the scholarship are placed in the NSA.

While ASPIRE is largely directed at students at NYU’s Tandon School of Engineering and its Law School, who are focused on technical and legal aspects of hacking and surveillance, it is also available to those studying business at the Stern School of Business; culture, at the Steinhardt School of Culture, Education, and Human Development; public policy and management, at the Robert F. Wagner Graduate School of Public Service; and science, at the Courant Institute of Mathematical Sciences.

On its webpage, the Center for Cybersecurity also prominently advertises the Department of Defense Information Assurance Scholarship Program (IASP), a full scholarship which is aimed at third- and fourth-year undergraduate or graduate and doctoral students. Students who are accepted will serve one year at the DoD, in addition to doing internships specified by the DoD, in order to end up finding permanent or temporary employment with the Pentagon.

The cybersecurity programs at NYU are expanding. In January 2018, it was announced that Tandon partnered with the

New York City Cyber Command (NYC3) to create New York Cyber Fellows, an online cybersecurity master's degree program that is aimed at addressing the "acute shortage of highly trained technical professionals in the city and the nation."

The program was designed jointly by NYU and "elite New York City employers," according to Tandon's press release. Business partners of the program include investment funds and companies like Booz Allen Hamilton, Blackstone, Bridgewater, IBM Security, and banks like Goldman Sachs, Morgan Stanley and the US Bank.

Apart from preparing students to work for the various branches of the US military and state machinery, NYU's "center for cybersecurity" has also been involved in developing surveillance technologies that were used by the right-wing United Arab Emirates government to spy on democracy activists. The spyware, developed by Hacking Team and Cyberpoint, was implanted on the phones of activists, who were subsequently arrested.

According to a report in the *Intercept* from 2015, Paul Kurtz, the chief strategist at Cyberpoint, was at that time also the chair of the privacy and cybersecurity center at NYU-Abu Dhabi. He had earlier worked for the Clinton and Bush administrations. As a member of first the National Security Council and then the White House's Homeland Security Council, Kurtz played a major role in the expansion of the military and surveillance apparatus in the wake of 9/11.

Cyberpoint and Kurtz also maintain various ties to US officials and the Washington-based think tank the Atlantic Council.

Moreover, NYU hosts events like the Cyber Security Awareness Week (CSAW), which is partially funded by the NSA. The CSAW is largely directed at young women who are still in high school. As part of the event, students compete with various hacking challenges and are judged by professionals. Speakers at the event often include figures from the Department of Homeland Security and other government agencies, who try to recruit new talent.

The Center for Cybersecurity also hosted "Women Leaders in Cybersecurity: Closing the Gender Gap" in 2016, to encourage female students to enter into this field—a characteristic combination of the promotion of feminism and militarism. The keynote presentation at the event was given by Renee Forney, the former executive director for the Department of Homeland Security Cyberskills Management Support Initiative.

Other speakers included; Brigadier General Jen Buckner, deputy commander of operations in US Cyber Command's Cyber National Mission Force; Merritt Baer, Senior Cybersecurity Strategist for the Department of Homeland Security; and Kevin Zerrusen, former foreign service officer for the State Department and current managing director for Goldman Sachs Security Incident Response Team. The stated purpose of the event was to "encourage 360-degree mentoring and power-brokering" to bring together "aspiring girls and young women, as well as seasoned professionals" to address the issue of gender inequality within cybersecurity.

Developing technology to break encryption

In 2017, it was revealed, based upon a data leak in early December 2016, that NYU's Institute for Mathematics and Advanced Supercomputing, headed by David and Gregory Chudnovsky, had been involved in developing a new system aimed at breaking complex encryption, at the behest of and in collaboration with the US Department of Defense and IBM.

According to the *Intercept*, this project for a supercomputer, which was described as "WindsorGreen," was "almost certainly intended for use by the Defense Department's signals intelligence wing, the National Security Agency." It was supposed to replace another password-cracking machine that the NSA had previously used, named "WindsorBlue." The details of this latter system had been revealed in documents leaked by Edward Snowden. Both "WindsorGreen" and "WindsorBlue" were to be used by the Pentagon and a few other Western governments, including Canada and Norway.

Experts who spoke to the *Intercept* stated that "WindsorGreen" was "particularly adept at compromising encryption and passwords" due its substantial computing power. Andrew Huang told the *Intercept* that "WindsorGreen" would surpass many of the most powerful code-breaking systems in the world. While the report indicated that Signal and PGP users were probably not at risk, there is little doubt that this is precisely the kind of encryption the US government is seeking to break on a mass scale, and that "WindsorGreen" was a major step in that direction.

To be continued in Part 3: NYU and the efforts to censor the Internet.