POPULAR
SCIENCE

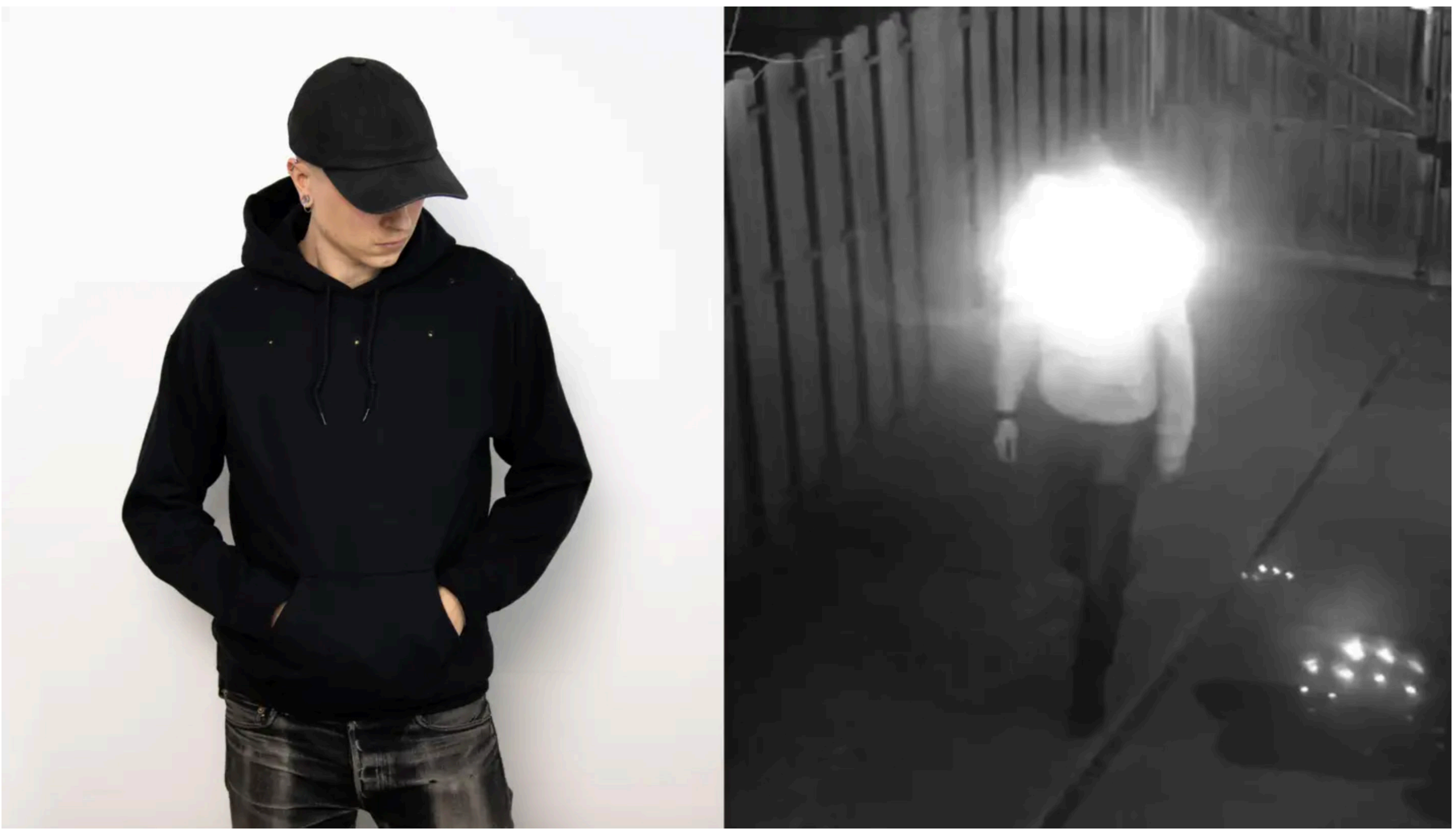
A simple DIY hoodie can fool security cameras

The 'Camera Shy Hoodie' looks innocuous, but keeps your face invisible to surveillance.

BY ANDREW PAUL | PUBLISHED FEB 27, 2023 1:00 PM EST

Despite objections from privacy advocates and many everyday citizens, surveillance technology such as facial recognition AI is appearing more and more in modern life. The market is booming—by 2026, the surveillance tech market will reach over $200 billion, despite being less than half that size in 2020. New products designed to collect personal data and track physical movements will likely keep popping up until meaningful legislation or public pushback causes companies to slow their roll. And that s where people like Mac Pierce enter the picture.

Pierce, an artist whose work critically engages with weaponized emerging technologies, recently unveiled their latest ingenious project—an everyday hoodie retrofitted to include an array of infrared (IR) LEDs that, when activated, blinds any nearby night vision security cameras. Using mostly off-the-shelf components like LumiLED lights, an Adafruit microcontroller, and silicone wire, as well as we software Pierce that made open-source for interested DIYers, the privacy-boosting “Camera Shy Hoodie” is designed to enable citizens to safely engage in civic protests and demonstrations. Or, wearers can just simply opt-out of being tracked by unknown third-parties while walking down the street.



Although unnoticeable to human eyes, the garment s infrared additions wreak havoc on surveillance cameras that utilize the light spectrum to see in evening darkness. Emitting the flashing infrared bursts from the hoodie will force nearby cameras   auto exposure to try correcting for the brightness, thus obscuring a wearers   face in a bright, pulsating light.

Speaking with Motherboard on Monday, Pierce argued, “surveillance technology has gotten to such a point where it s so powerful and so pervasive. And it s only now that we re realizing,   Maybe we don t want this stuff to be as powerful as it is. ” Projects like the Camera Shy Hoodie—alongside Piece s earlier, simplified “Opt Out Cap”—are meant to simultaneously bring attention to the issues of privacy and authority, while also providing creative workarounds to everyday, frequently problematic surveillance tools, he says.

Pierce has made all the designs, plans, and specifications for their hoodie hack available for free on their website. Unfortunately, the project isn t cheap—all told, the work would set makers back around $200—but anyone interested in a Camera Shy Hoodie to call their own can also sign up to be noticed by Pierce when custom kits are available for purchase.

Meanwhile, there are a number of interesting (and cheaper) clothing options in the vein of Piece s Camera Shy Hoodie, including an apparel line meant to confuse license plate scanning traffic cameras, and facial recognition-obscuring makeup techniques.

Andrew Paul

Andrew Paul is Popular Science's staff writer covering tech news. Previously, he was a regular contributor to The A.V. Club and Input, and has had recent work also featured by Rolling Stone, Fangoria, GQ, Slate, NBC, as well as McSweeney's Internet Tendency. He lives outside Indianapolis.

CLTC Announces Winners of Third Annual Cybersecurity Arts Contest

CLTC UC Berkeley Center for Long-Term Cybersecurity

April 4, 2023

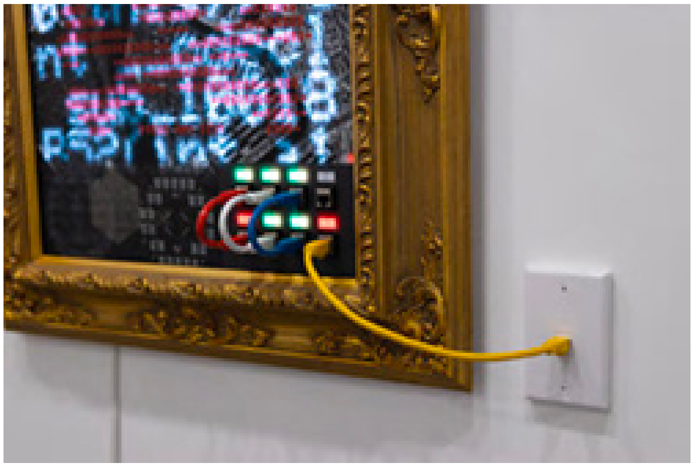
By Rachel Wesen

The Center for Long-Term Cybersecurity (CLTC) is proud to announce the winners of our third-annual Cybersecurity Arts Contest. Following a review by an independent and interdisciplinary panel of judges, three projects were selected based on their artistic merit, relevance, and potential impact.

The primary goal of the Cybersecurity Arts Contest is to expand representations of cybersecurity, broadly defined, through artistic expression and public dialogue.

2nd Prize
Mac Pierce
“Portrait of a Digital Weapon”

Issues of cybersecurity are rarely couched in terms of warfare to the larger public, and are often portrayed



as one-off attacks or the work of stateless cyber criminals. This no longer reflects the reality of the situation, as some of the largest attacks are carried out by national actors for the purposes of achieving state goals, much like traditional armaments of war. As more nations develop cyber-offensive capabilities, more of these attacks will occur. However, unlike conventional warfare, these attacks will never elicit an in-kind declaration of war, as they often remain covert. This cloak-and-dagger approach to cyber warfare allows these attacks to continue and escalate.

Mac Pierce’s Portrait of a Digital Weapon is a series of electronically activated portraits depicting infamous, real-life examples of computer viruses, such as Stuxnet and NotPetya, being used as a tool of geopolitical and financial attack by nation-states. Each piece reads off the decompiled source code of the virus while displaying select elements of how each of the viruses operated and satellite imagery of the attack target. These works lay out the story of the battlefields in which these cyber weapons were used within a traditional painting frame, alluding to the many examples of works of art about war and global conquest throughout history.

The ongoing Portrait of a Digital Weapon series attempts to bring these covert attacks to light and highlight these viruses for what they are — cyber weapons. “When a viewer engages with this work, processing the meaning and the ramifications of the content of the work, I hope that they come away with a sense of unease about the computer viruses depicted,” Pierce said. “Ultimately, the two viruses highlighted so far were covert operations, and greater knowledge of the particulars of their use will only lead more people to question why these viruses existed in the first place. By aestheticizing the elements of each virus, they become far easier to understand.”

hackaday.com

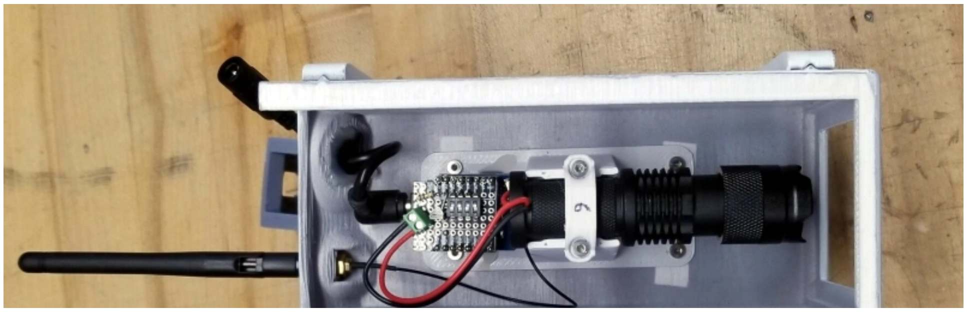
Building An Army Of Faux Cameras In The Name Of Art

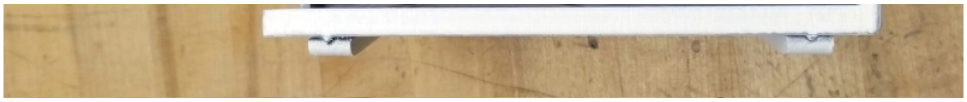
3-4 minutes

Skip to content

After taking mental note of the number of surveillance cameras pointed at him while standing in line at the local Home Depot, [Mac Pierce] was inspired to create *A Scanner Darkly*. The art installation uses beams of light projected by mock security cameras to create a dot-matrix character display on the opposing wall, which slowly blinks out US surveillance laws and regulations.

[Mac] has put together an extensive behind the scenes look at how he created *A Scanner Darkly*, which among other things covers the incredible time and effort that went into producing the fifteen identical cameras used to project the 3×5 grid. Early on he decided on 3D printing each one, as it would give him complete control over the final result. But given their considerable size, it ended up taking 230 hours and 12 kilograms of PLA filament to print out all the parts. It took a further 55 hours to sand and paint the camera housings, to make sure they didn't actually *look* like they'd been 3D printed.

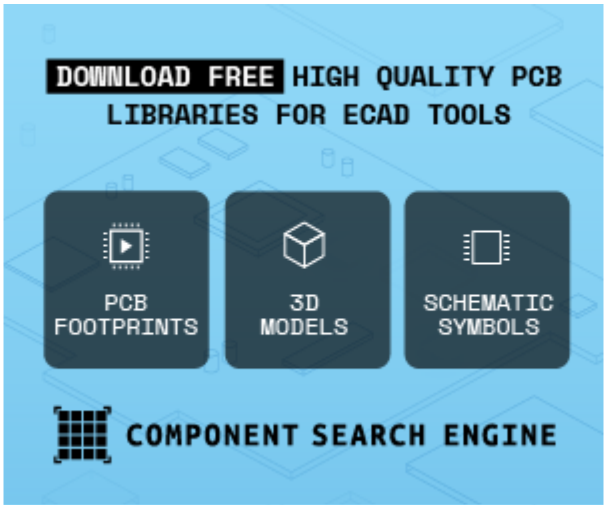




Internally, each camera has an off-the-shelf LED flashlight that's had its power button rigged up to an ESP8266. Once they've been manually pointed to the appropriate spot on the wall, [Mac] can turn each camera's spotlight on and off over WiFi. Rather than rely on the gallery's infrastructure, all of the cameras connect to the ESP32 M5Stack that serves as the central controller via ESP-Now.

From there, it was just a matter of writing some code that would load a text document from the SD card, convert the current character into a 3×5 array, and then command the appropriate cameras to turn their lights on or off. [Mac] has not only provided the STL files for the 3D printed camera, but the client and server Arduino code to control the lights. Combined with his excellent documentation, this makes *A Scanner Darkly* something of a viral art piece; as anyone with the time and appropriate tools can either duplicate the installation or use it as a base for something new.

While some will no doubt argue that [Mac] could have completed this project far faster [had he just modified some commercial dummy cameras](), it's important to remember that as an artist, he had a very specific look in mind for *A Scanner Darkly*. This project is a perfect example of how a creator's passion can take an idea to new heights, and we think the end result proves it's worth the time and sweat to put in the extra effort.



hackaday.com

Portrait Of A Digital Weapon

4-5 minutes

Over the years, artists have been creating art depicting weapons of mass destruction, war and human conflict. But the weapons of war, and the theatres of operation are changing in the 21st century. The outcome of many future conflicts will surely depend on digital warriors, huddled over their computer screens, punching on their keyboards and maneuvering joysticks, or using devious methods to infect computers to disable or destroy infrastructure. How does an artist give physical form to an unseen, virtual digital weapon? That is the question which inspired [Mac Pierce] to create his latest Portrait of a Digital Weapon.

[Mac]'s art piece is a physical depiction of a virtual digital weapon, a nation-state cyber attack. When activated, this piece displays the full code of the Stuxnet virus, a worm that partially disabled Iran's nuclear fuel production facility at Natanz around 2008.

It took a while for [Mac] to finalize the plan for his design. He obtained a high resolution satellite image of the Iranian Natanz facility via the Sentinel Hub satellite imagery service. This was printed on a transparent vinyl and glued to a translucent poly-carbonate sheet. Behind the poly-carbonate layer, he built a large, single digit 16-segment display using WS2812 addressable LED strips, which would be used to display the Stuxnet code. A bulkhead USB socket was added over the centrifuge facility, with a ring of WS2812 LEDs surrounding the main complex. When a USB stick is plugged in, the Stuxnet code is displayed on the 16-segment display, one character at a time. At random intervals, the LED ring around the centrifuge building lights up spinning in a red color to indicate centrifuge failure.

The 16-segment display was built on an aluminum base plate, with 3D printed baffles to hold the LED strips. To hold the rest of the electronics, he built a separate 3D printed frame which could be added to the main art frame. Since this was too large to be printed in one piece on the 3D printer, it was split in parts, which were then joined together using embedded metal stud reinforcement to hold the parts together. Quite a nice trick to make large, rigid parts.

An Adafruit Feather M0 micro-controller board, with micro SD-card slot was the brains of the project. To derive the 5 V logic data signal from the 3.3 V GPIO output of the Feather, [Mac] used two extra WS2812 LEDs as level shifters before sending the data to the LED strips. Driving all the LEDs required almost 20 W, so he powered it using USB-C, adding a power delivery negotiation board to derive the required juice.

The Arduino code is straightforward. It reads the characters stored on the SD-card, and sends them sequentially to the 16-segment display. The circular ring around the USB bulkhead also lights up white, but at random intervals it turns red to simulate the speeding up of the centrifuges. Detecting when the USB stick gets plugged in is another nice hack that [Mac] figured out. When a USB stick is plugged in, the continuity between the shell (shield) and the GND terminal was used to trigger a GPIO input.

Cyber warfare is here to stay. We are already seeing increasing attacks on key infrastructure installations by state as well as non-state actors around the world. Stuxnet was one of the first in this growing category of malicious, weaponized code. Acknowledging its presence using such a physical representation can offer a reminder on how a few lines of software can wreak havoc just as much as any other physical weapon. Check out the brief project video after the break.

boingboing.net

Make: a facial-recognition confounding "Opt Out Cap" | Boing Boing

Cory Doctorow

3-4 minutes

Mac Pierce created a simple wearable to challenge facial recognition: do a little munging to an image of a face, print it on heat transfer paper, iron it onto see-through mosquito netting, slice, and affix to a billed cap — deploy it in the presence of facial recognition cameras and you'll be someone else. It's the kind of "adversarial example" countermeasure that fools computers pretty reliably but wouldn't work on a human. (*via* JWZ)