The Masked Avengers

How Anonymous incited online vigilantism from Tunisia to Ferguson.

BY DAVID KUSHNER

Anyone can join Anonymous simply by claiming affiliation. An anthropologist says that participants “remain subordinate to a focus on the epic win—and, especially, the lulz.”

In the mid-nineteen-seventies, when Christopher Doyon was a child in rural Maine, he spent hours chatting with strangers on CB radio. His handle was Big Red, for his hair. Transmitters lined the walls of his bedroom, and he persuaded his father to attach two directional antennas to the roof of their house. CB radio was associated primarily with truck drivers, but Doyon and others used it to form the sort of virtual community that later appeared on the Internet, with self-selected nicknames, inside jokes, and an earnest desire to effect change.

Doyon’s mother died when he was a child, and he and his younger sister were reared by their father, who they both say was physically abusive. Doyon found solace, and a sense of purpose, in the CB-radio community. He and his friends took turns monitoring the local emergency channel. One friend’s father bought a bubble light and affixed it to the roof of his car; when the boys heard a distress call from a stranded motorist, he’d drive them to the side of the highway. There wasn’t much they could do beyond offering to call 911, but the adventure made them feel heroic.

Small and wiry, with a thick New England accent, Doyon was fascinated by “Star Trek” and Isaac Asimov novels. When he saw an ad in Popular Mechanics for a build-your-own personal-computer kit, he asked his grandmother to buy it for him, and he spent months figuring out how to put it together and hook it up to the Internet. Compared with the sparsely populated CB airwaves, online chat rooms were a revelation. “I just click a button, hit this guy’s name, and I’m talking to him,” Doyon recalled recently. “It was just breathtaking.”

At the age of fourteen, he ran away from home, and two years later he moved to Cambridge, Massachusetts, a hub of the emerging computer counterculture. The Tech Model Railroad Club, which had been founded thirty-four years earlier by train hobbyists at M.I.T., had evolved into “hackers”—the first group to popularize the term. Richard Stallman, a computer scientist who worked in M.I.T.’s Artificial Intelligence Laboratory at the time, says that these early hackers were more likely to pass around copies of “Gödel, Escher, Bach” than to incite technological warfare. “We didn’t have tenets,” Stallman said. “It wasn’t a movement. It was just a thing that people did to impress each other.” Some of their “hacks” were fun (coding video games); others
were functional (improving computer-processing speeds); and some were pranks that took place in the real world (placing mock street signs near campus). Michael Patton, who helped run the T.M.R.C. in the seventies, told me that the original hackers had unwritten rules and that the first one was “Do no damage.”

In Cambridge, Doyon supported himself through odd jobs and panhandling, preferring the freedom of sleeping on park benches to the monotony of a regular job. In 1985, he and a half-dozen other activists formed an electronic “militia.” Echoing the Animal Liberation Front, they called themselves the Peoples Liberation Front. They adopted aliases: the founder, a towering middle-aged man who claimed to be a military veteran, called himself Commander Adama; Doyon went by Commander X. Inspired by the Merry Pranksters, they sold LSD at Grateful Dead shows and used some of the cash to outfit an old school bus with bullhorns, cameras, and battery chargers. They also rented a basement apartment in Cambridge, where Doyon occasionally slept.

Doyon was drawn to computers, but he was not an expert coder. In a series of conversations over the past year, he told me that he saw himself as an activist, in the radical tradition of Abbie Hoffman and Eldridge Cleaver; technology was merely his medium of dissent. In the eighties, students at Harvard and M.I.T. held rallies urging their schools to divest from South Africa. To help the protesters communicate over a secure channel, the P.L.F. built radio kits: mobile FM transmitters, retractable antennas, and microphones, all stuffed inside backpacks. Willard Johnson, an activist and a political scientist at M.I.T., said that hackers were not a transformative presence at rallies. “Most of our work was still done using a bullhorn,” he said.

In 1992, at a Grateful Dead concert in Indiana, Doyon sold three hundred hits of acid to an undercover narcotics agent. He was sentenced to twelve years in Pendleton Correctional Facility, of which he served five. While there, he developed an interest in religion and philosophy and took classes from Ball State University.

Netscape Navigator, the first commercial Web browser, was released in 1994, while Doyon was incarcerated. When he returned to Cambridge, the P.L.F. was still active, and their tools had a much wider reach. The change, Doyon recalls, “was gigantic—it was the difference between sending up smoke signals and being able to telegraph someone.” Hackers defaced an Indian military Web site with the words “Save Kashmir.” In Serbia, hackers took down an Albanian site. Stefan Wray, an early online activist, defended such tactics at an “anti-Columbus Day” rally in New York. “We see this as a form of electronic civil disobedience,” he told the crowd.

In 1999, the Recording Industry Association of America sued Napster, the file-sharing service, for copyright infringement. As a result, Napster was shut down in 2001. Doyon and other hackers disabled the R.I.A.A. site for a weekend, using a Distributed Denial of Service, or DDoS, attack, which floods a site with so much data that it slows down or crashes. Doyon defended his actions, employing the heightened rhetoric of other “hacktivists.” “We quickly came to understand that the battle to defend Napster was symbolic of the battle to preserve a free internet,” he later wrote.

One day in 2008, Doyon and Commander Adama met at the P.L.F.’s basement apartment in Cambridge. Adama showed Doyon the Web site of the Epilepsy Foundation, on which a link,
instead of leading to a discussion forum, triggered a series of flashing colored lights. Some epileptics are sensitive to strobes; out of sheer malice, someone was trying to induce seizures in innocent people. There had been at least one victim already.

Doyon was incensed. He asked Adama who would do such a thing.

“Ever hear of a group called Anonymous?” Adama said.

In 2003, Christopher Poole, a fifteen-year-old insomniac from New York City, launched 4chan, a discussion board where fans of anime could post photographs and snarky comments. The focus quickly widened to include many of the Internet’s earliest memes: LOLcats, Chocolate Rain, RickRolls. Users who did not enter a screen name were given the default handle Anonymous.

Poole hoped that anonymity would keep things irreverent. “We have no intention of partaking in intelligent discussions concerning foreign affairs,” he wrote on the site. One of the highest values within the 4chan community was the pursuit of “lulz,” a term derived from the acronym LOL. Lulz were often achieved by sharing puerile jokes or images, many of them pornographic or scatological. The most shocking of these were posted on a part of the site labelled /b/, whose users called themselves /b/tards. Doyon was aware of 4chan, but considered its users “a bunch of stupid little pranksters.” Around 2004, some people on /b/ started referring to “Anonymous” as an independent entity.

It was a new kind of hacker collective. “It’s not a group,” Mikko Hypponen, a leading computer-security researcher, told me—rather, it could be thought of as a shape-shifting subculture. Barrett Brown, a Texas journalist and a well-known champion of Anonymous, has described it as “a series of relationships.” There was no membership fee or initiation. Anyone who wanted to be a part of Anonymous—an Anon—could simply claim allegiance.

Despite 4chan’s focus on trivial topics, many Anons considered themselves crusaders for justice. They launched vigilante campaigns that were purposeful, if sometimes misguided. More than once, they posed as underage girls in order to entrap pedophiles, whose personal information they sent to the police. Other Anons were apolitical and sowed chaos for the lulz. One of them posted images on /b/ of what looked like pipe bombs; another threatened to blow up several football stadiums and was arrested by the F.B.I. In 2007, a local news affiliate in Los Angeles called Anonymous “an Internet hate machine.”

In January, 2008, Gawker Media posted a video in which Tom Cruise enthusiastically touted the benefits of Scientology. The video was copyright-protected, and the Church of Scientology sent a cease-and-desist letter to Gawker, asking that the video be removed. Anonymous viewed the church’s demands as attempts at censorship. “I think it’s time for /b/ to do something big,” someone posted on 4chan. “I’m talking about ‘hacking’ or ‘taking down’ the official Scientology Web site.” An Anon used YouTube to issue a “press release,” which included stock footage of storm clouds and a computerized voice-over. “We shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form,” the voice said. “You have nowhere to hide.” Within a few weeks, the YouTube video had been viewed more than two million times.
Anonymous had outgrown 4chan. The hackers met in dedicated Internet Relay Chat channels, or I.R.C.s, to coordinate tactics. Using DDoS attacks, they caused the main Scientology Web site to crash intermittently for several days. Anons created a “Google bomb,” so that a search for “dangerous cult” would yield the main Scientology site at the top of the results page. Others sent hundreds of pizzas to Scientology centers in Europe, and overwhelmed the church’s Los Angeles headquarters with all-black faxes, draining the machines of ink. The Church of Scientology, an organization that reportedly has more than a billion dollars in assets, could withstand the depletion of its ink cartridges. But its leaders, who had also received death threats, contacted the F.B.I. to request an investigation into Anonymous.

On March 15, 2008, several thousand Anons marched past Scientology churches in more than a hundred cities, from London to Sydney. In keeping with the theme of anonymity, the organizers decided that all the protesters should wear versions of the same mask. After considering Batman, they settled on the Guy Fawkes mask worn in “V for Vendetta,” a dystopian movie from 2005. “It was available in every major city, in large quantities, for cheap,” Gregg Housh, one of the organizers of the protests and a well-known Anon, told me. The mask was a caricature of a man with rosy cheeks, a handlebar mustache, and a wide grin.

Anonymous did not “dismantle” the Church of Scientology. Still, the Tom Cruise video remained online. Anonymous had proved its tenacity. The collective adopted a bombastic slogan: “We are Legion. We do not forgive. We do not forget. Expect us.”

In 2010, Doyon moved to Santa Cruz, California, to join a local movement called Peace Camp. Using wood that he stole from a lumberyard, he built a shack in the mountains. He borrowed WiFi from a nearby mansion, drew power from salvaged solar panels, and harvested marijuana, which he sold for cash.

At the time, the Peace Camp activists were sleeping on city property as a protest against a Santa Cruz anti-homelessness law that they considered extreme. Doyon appeared at Peace Camp meetings and offered to promote their cause online. He had an unkempt red beard and wore a floppy beige hat and quasi-military fatigues. Some of the activists called him Curbhugger Chris.

Kelley Landaker, a member of Peace Camp, spoke with Doyon several times about hacking. Doyon sometimes bragged about his technical aptitude, but Landaker, an expert programmer, was unimpressed. “He was more of a spokesman than a hands-on-the-keyboard type of person,” Landaker told me. But the movement needed a passionate leader more than it needed a coder. “He was very enthusiastic and very outspoken,” Robert Norse, also a member of Peace Camp, told me. “He created more media attention for the issue than anyone I’ve seen, and I’ve been doing this for twenty years.”

Commander Adama, Doyon’s superior in the P.L.F., who still lived in Cambridge and communicated with him via e-mail, had ordered Doyon to monitor Anonymous. Doyon’s brief was to observe their methods and to recruit members to the P.L.F. Recalling his revulsion at the Epilepsy Foundation hack, Doyon initially balked. Adama argued that the malicious hackers were a minority within Anonymous, and that the collective might inspire powerful new forms of activism. Doyon was skeptical. “The biggest movement in the world is going to come from 4chan?” he said. But, out of loyalty to the P.L.F., he obeyed Adama.
Doyon spent much of his time at the Santa Cruz Coffee Roasting Company, a café downtown, hunched over an Acer laptop. The main Anonymous I.R.C. did not require a password. Doyon logged in using the name PLF and followed along. Over time, he discovered back channels where smaller, more dedicated groups of Anons had dozens of overlapping conversations. To participate, you had to know the names of the back channels, which could be changed to deflect intruders. It was not a highly secure system, but it was adaptable. “These simultaneous cabals keep centralization from happening,” Gabriella Coleman, an anthropologist at McGill University, told me.

Some Anons proposed an action called Operation Payback. As the journalist Parmy Olson wrote in a 2012 book, “We Are Anonymous,” Operation Payback started as another campaign in support of file-sharing sites like the Pirate Bay, a successor to Napster, but the focus soon broadened to include political speech. In late 2010, at the behest of the State Department, several companies, including MasterCard, Visa, and PayPal, stopped facilitating donations to WikiLeaks, the vigilante organization that had released hundreds of thousands of diplomatic cables. In an online video, Anonymous called for revenge, promising to lash out at the companies that had impeded WikiLeaks. Doyon, attracted by the anti-corporate spirit of the project, decided to participate.

During Operation Payback, in early December, Anonymous directed new recruits, or noobs, to a flyer headed “How to Join the Fucking Hive,” in which participants were instructed to “FIX YOUR GODDAMN INTERNET. THIS IS VERY FUCKING IMPORTANT.” They were also asked to download Low Orbit Ion Cannon, an easy-to-use tool that is publicly available. Doyon downloaded the software and watched the chat rooms, waiting for a cue. When the signal came, thousands of Anons fired at once. Doyon entered a target URL—say, www.visa.com—and, in the upper-right corner, clicked a button that said “IMMA CHARGIN MAH LAZER.” (The operation also relied on more sophisticated hacking.) Over several days, Operation Payback disabled the home pages of Visa, MasterCard, and PayPal. In court filings, PayPal claimed that the attack had cost the company five and a half million dollars.

To Doyon, this was activism made tangible. In Cambridge, protesting against apartheid, he could not see immediate results; now, with the tap of a button, he could help sabotage a major corporation’s site. A banner headline on the Huffington Post read “MasterCard DOWN.” One gloating Anon tweeted, “There are some things WikiLeaks can’t do. For everything else, there’s Operation Payback.”

In the fall of 2010, the Peace Camp protests ended. With slight concessions, the anti-homelessness law remained in effect. Doyon hoped to use the tactics of Anonymous to reinvigorate the movement. He recalls thinking, “I could wield Anonymous against this tiny little city government and they would just be fucking wrecked. Plan was we were finally going to solve this homelessness problem, once and for all.”

Joshua Covelli, a twenty-five-year-old Anon who went by the nickname Absolem, admired Doyon’s decisiveness. “Anonymous had been this clusterfuck of chaos,” Covelli told me. With Commander X, “there seemed to be a structure set up.” Covelli worked as a receptionist at a college in Fairborn, Ohio, and knew nothing about Santa Cruz politics. But when Doyon asked
for help with Operation Peace Camp, Covelli e-mailed back immediately: “I’ve been waiting to
join something like that my entire life.”

Doyon, under the name PLF, invited Covelli into a private I.R.C.:

Absolem: Sorry to be so rude . . . Is PLF part of Anonymous or separate?

Absolem: I was just asking because you all seem very organized in chat.

PLF: You are not in the least rude. I am pleased to meet you. PLF is 22 year old hacker
group originally from Boston. I started hacking in 81, not with computers but PBX
(telephones).

PLF: We are all older 40 or over. Some of us are former military or intelligence. One of
us, Commander Adama is currently sought by an alphabet soup of cops and spooks and in
hiding.

Absolem: Wow that’s legit. I am really interested in helping this out in some way and
Anonymous just seems too chaotic. I have some computer skills but very noob in
hacking. I have some tools but no Idea how to use them.

With ritual solemnity, Doyon accepted Covelli’s request to join the P.L.F.:

PLF: Encrypt the fuck out of all sensitive material that might incriminate you.

PLF: Yep, work with any PLFer to get a message to me. Call me . . . Commander X for
now.

In 2012, the Associated Press called Anonymous “a group of expert hackers”; Quinn Norton, in
*Wired*, wrote that “Anonymous had figured out how to infiltrate anything,” resulting in “a wild
string of brilliant hacks.” In fact some Anons are gifted coders, but the vast majority possess
little technical skill. Coleman, the anthropologist, told me that only a fifth of Anons are
hackers—the rest are “geeks and protesters.”

On December 16, 2010, Doyon, as Commander X, sent an e-mail to several reporters. “At
exactly noon local time tomorrow, the Peoples Liberation Front and Anonymous will remove
from the Internet the Web site of the Santa Cruz County government,” he wrote. “And exactly 30
minutes later, we will return it to normal function.”

The data-center staff for Santa Cruz County saw the warning and scrambled to prepare for the
attack. They ran security scans on the servers and contacted A.T. & T., the county’s Internet
provider, which suggested that they alert the F.B.I.

The next day, Doyon entered a Starbucks and booted up his laptop. Even for a surfing town, he
was notably eccentric: a homeless-looking man wearing fatigues and typing furiously. Covelli
met him in a private chat room.
PLF: Go to Forum, sign in—and look at top right menu bar “chat.” Thats Ops for today. Thank you for standing with us.

Absolem: Anything for PLF, sir.

They both opened DDoS software. Though only a handful of people were participating in Operation Peace Camp, Doyon gave orders as if he were addressing legions of troops:

PLF: ATTENTION: Everyone who supports the PLF or considers us their friend—or who cares about defeating evil and protecting the innocent: Operation Peace Camp is LIVE and an action is underway. TARGET: www.co.santa-cruz.ca.us. Fire At Will. Repeat: FIRE!

Absolem: got it, sir.

The data-center staff watched their servers, which showed a flurry of denial-of-service requests. Despite their best efforts, the site crashed. Twenty-five minutes later, Doyon decided that he had made his point. He typed “CEASE FIRE,” and the county’s site flickered back to life. (Despite the attack, the city’s anti-homelessness law did not change.)

Doyon hardly had time to celebrate before he grew anxious. “I got to leave,” he typed to Covelli. He fled to his shack in the mountains. Doyon was right to be wary: an F.B.I. agent had been snooping in the I.R.C. The F.B.I. obtained a warrant to search Doyon’s laptop.

A few weeks later, Doyon’s food ran out, and he returned to town. While he was at the Santa Cruz Coffee Roasting Company, two federal agents entered the shop. They brought him to the county police station. Doyon called Ed Frey, a lawyer and the founder of Peace Camp, who met him at the station. Doyon told Frey about his alter ego as Commander X.

Doyon was released, but the F.B.I. kept his laptop, which was full of incriminating evidence. Frey, a civil-rights lawyer who knew little about cybersecurity, drove Doyon back to his hillside encampment. “What are you going to do?” Frey asked.

He spoke in cinematic terms. “Run like hell,” he said. “I will go underground, try to stay free as long as I can, and keep fighting the bastards any way possible.” Frey gave him two twenty-dollar bills and wished him luck.

Doyon hitchhiked to San Francisco and stayed there for three months. He spent his days at Coffee to the People, a quirky café in the Haight-Ashbury district, where he would sit for hours in front of his computer, interrupted only by outdoor cigarette breaks.

In January, 2011, Doyon contacted Barrett Brown, the journalist and Anon. “What are we going to do next?” Doyon asked.

“Tunisia,” Brown said.

“Yeah, it’s a country in the Middle East,” Doyon said. “What about it?”
“We’re gonna take down its dictator,” Brown said.

“Oh, they have a dictator?” Doyon said.

A couple of days later, Operation Tunisia began. Doyon volunteered to spam Tunisian government e-mail addresses in an attempt to clog their servers. “I would take the text of the press release for that op and just keep sending it over and over again,” he said. “Sometimes, I was so busy that I would just put ‘fuck you’ and send it.” In one day, the Anons brought down the Web sites of the Tunisian Stock Exchange, the Ministry of Industry, the President, and the Prime Minister. They replaced the Web page of the President’s office with an image of a pirate ship and the message “Payback is a bitch, isn’t it?”

Doyon often spoke of his online battles as if he had just crawled out of a foxhole. “Dude, I turned black from doing it,” he told me. “My face, from all the smoke—it would cling to me. I would look up and I would literally be like a raccoon.” Most nights, he camped out in Golden Gate Park. “I would look at myself in the mirror and I’d be like, O.K., it’s been four days—maybe I should eat, bathe.”

Anonymous-affiliated operations continued to be announced on YouTube: Operation Libya, Operation Bahrain, Operation Morocco. As protesters filled Tahrir Square, Doyon participated in Operation Egypt. A Facebook page disseminated information, including links to a “care package” for protesters on the ground. The package, distributed through the file-sharing site Megaupload, contained encryption software and a primer on defending against tear gas. Later, when the Egyptian government disabled Internet and cellular networks within the country, Anonymous helped the protesters find alternative ways to get online.

In the summer of 2011, Doyon succeeded Adama as Supreme Commander of the P.L.F. Doyon recruited roughly half a dozen new members and attempted to position the P.L.F. as an élite squad within Anonymous. Covelli became one of his technical advisers. Another hacker, Crypt0nymous, made YouTube videos; others did research or assembled electronic care packages. Unlike Anonymous, the P.L.F. had a strict command structure. “X always called the shots on everything,” Covelli said. “It was his way or no way.” A hacker who founded a blog called AnonInsiders told me over encrypted chat that Doyon was willing to act unilaterally—a rare thing within Anonymous. “When we wanted to start an op, he didn’t mind if anyone would agree or not,” he said. “He would just write the press release by himself, list all the targets, open the I.R.C. channel, tell everyone to go in there, and start the DDoSing.”

Some Anons viewed the P.L.F. as a vanity project and Doyon as a laughingstock. “He’s known for his exaggeration,” Mustafa Al-Bassam, an Anon who went by Tflow, told me. Others, even those who disapproved of Doyon’s egotism, grudgingly acknowledged his importance to the Anonymous movement. “He walks that tough line of sometimes being effective and sometimes being in the way,” Gregg Housh said, adding that he and other prominent Anons had faced similar challenges.

Publicly, Anonymous persists in claiming to be non-hierarchical. In “We Are Legion,” a 2012 documentary about Anonymous by Brian Knappenberger, one activist uses the metaphor of a flock of birds, with various individuals taking turns drifting toward the front. Gabriella Coleman
told me that, despite such claims, something resembling an informal leadership class did emerge within Anonymous. “The organizer is really important,” she said. “There are four or five individuals who are really good at it.” She counted Doyon among them. Still, Anons tend to rebel against institutional structure. In a forthcoming book about Anonymous, “Hacker, Hoaxer, Whistleblower, Spy,” Coleman writes that, among Anons, “personal identity and the individual remain subordinate to a focus on the epic win—and, especially, the lulz.”

Anons who seek individual attention are often dismissed as “egofags” or “namefags.” (Many Anons have yet to outgrow their penchant for offensive epithets.) “There are surprisingly few people who violate the rule” against attention-seeking, Coleman says. “Those who do, like X, are marginalized.” Last year, in an online discussion forum, a commenter wrote, “I stopped reading his BS when he started comparing himself to Batman.”

Peter Fein, an online activist known by the nickname n0pants, was among the many Anons who were put off by Doyon’s self-aggrandizing rhetoric. Fein browsed the P.L.F. Web site, which featured a coat of arms and a manifesto about the group’s “epic battle for the very soul of humanity.” Fein was dismayed to find that Doyon had registered the site using his real name, leaving himself and possibly other Anons vulnerable to prosecution. “I’m basically okay with people DDoSing,” Fein recalls telling Doyon over private chat. “But if you’re going to do it, you’ve got to cover your ass.”

On February 5, 2011, the Financial Times reported that Aaron Barr, the C.E.O. of a cybersecurity firm called HBGary Federal, had identified the “most senior” members of Anonymous. Barr’s research suggested that one of the top three was Commander X, a hacker based in California, who could “manage some significant firepower.” Barr contacted the F.B.I. and offered to share his work with them.

Like Fein, Barr had seen that the P.L.F. site was registered to Christopher Doyon at an address on Haight Street. Based on Facebook and I.R.C. activity, Barr concluded that Commander X was Benjamin Spock de Vries, an online activist who had lived near the Haight Street address. Barr approached de Vries on Facebook. “Please tell the folks there that I am not out to get you guys,” Barr wrote. “Just want the ‘leadership’ to know what my intent is.”

“‘Leadership’ lmao,” de Vries responded.

Days after the Financial Times story appeared, Anonymous struck back. HBGary Federal’s Web site was defaced. Barr’s personal Twitter account was hijacked, thousands of his e-mails were leaked online, and Anons released his address and other personal information—a punishment known as doxing. Barr resigned from HBGary Federal within the month.

In April, 2011, Doyon left San Francisco and hitchhiked around the West, camping in parks at night and spending his days at Starbucks outlets. In his backpack he kept his laptop, his Guy Fawkes mask, and several packs of Pall Malls.

He followed internal Anonymous news. That spring, six élite Anons, all of whom had been instrumental in deflecting Barr’s investigation, formed a group called Lulz Security, or LulzSec. As their name indicated, they felt that Anonymous had become too self-serious; they aimed to bring the lulz back. While Anonymous continued supporting Arab Spring protesters, LulzSec
hacked the Web site of PBS and posted a fake story claiming that the late rapper Tupac Shakur was alive in New Zealand.

Anons often share text through the Web site Pastebin.com. On the site, LulzSec issued a statement that read, “It has come to our unfortunate attention that NATO and our good friend Barrack Osama-Llama 24th-century Obama have recently upped the stakes with regard to hacking. They now treat hacking as an act of war.” The loftier the target, the greater the lulz. On June 15th, LulzSec took credit for crashing the C.I.A.’s Web site, tweeting, “Tango down—cia.gov—for the lulz.”

On June 20, 2011, Ryan Cleary, a nineteen-year-old member of LulzSec, was arrested for the DDoS attacks on the C.I.A. site. The next month, F.B.I. agents arrested fourteen other hackers for DDoS attacks on PayPal seven months earlier. Each of the PayPal Fourteen, as they became known, faced fifteen years in prison and a five-hundred-thousand-dollar fine. They were charged with conspiracy and intentional damage to protected computers under the Computer Fraud and Abuse Act. (The law allows for wide prosecutorial discretion and was widely criticized after Aaron Swartz, an Internet activist who was facing thirty-five years in prison, committed suicide last year.)

A petition was circulated on behalf of Jake (Topiary) Davis, a member of LulzSec, who needed help paying his legal fees. Doyon entered an I.R.C. to promote Davis’s cause:

CommanderX: Please sign the petition and help Topiary…

toad: you are an attention whore
toad: so you get attention

CommanderX: Toad your an asshole.

katanon: sigh

Doyon had grown increasingly brazen. He DDoS’ed the Web site of the Chamber of Commerce of Orlando, Florida, after activists there were arrested for feeding the homeless. He launched the attacks from public WiFi networks, using his personal laptop, without making much effort to cover his tracks. “That’s brave but stupid,” a senior member of the P.L.F. who asked to be called Kalli told me. “He didn’t seem to care if he was caught. He was a suicide hacker.”

Two months later, Doyon participated in a DDoS strike against San Francisco’s Bay Area Rapid Transit, protesting an incident in which a BART police officer had killed a homeless man named Charles Hill. Doyon appeared on the “CBS Evening News” to defend the action, his voice disguised and his face obscured by a bandanna. He compared DDoS attacks to civil disobedience. “It’s no different, really, than taking up seats at the Woolworth lunch counters,” he said. Bob Schieffer, the CBS anchor, snickered and said, “It’s not quite the civil-rights movement, as I see it.”

On September 22, 2011, in a coffee shop in Mountain View, California, Doyon was arrested and charged with causing intentional damage to a protected computer. He was detained for a week
and released on bond. Two days later, against his lawyer’s advice, he called a press conference on the steps of the Santa Cruz County Courthouse. His hair in a ponytail, he wore dark sunglasses, a black pirate hat, and a camouflage bandanna around his neck.

In characteristically melodramatic fashion, Doyon revealed his identity. “I am Commander X,” he told reporters. He raised his fist. “I am immensely proud, and humbled to the core, to be a part of the idea called Anonymous.” He told a journalist, “All you need to be a world-class hacker is a computer and a cool pair of sunglasses. And the computer is optional.”

Kalli worried that Doyon was placing his ego above the safety of other Anons. “It’s the weakest link in the chain that ends up taking everyone down,” he told me. Josh Covelli, the Anon who had been eager to help Doyon with Operation Peace Camp, told me that his “jaw dropped” when he saw a video of Doyon’s press conference online. “The way he presented himself and the way he acted had become more unhinged,” Covelli said.

Three months later, Doyon’s pro-bono lawyer, Jay Leiderman, was in a federal court in San Jose. Leiderman had not heard from Doyon in a couple of weeks. “I’m inquiring as to whether there’s a reason for that,” the judge said. Leiderman had no answer. Doyon was absent from another hearing two weeks later. The prosecutor stated the obvious: “It appears as though the defendant has fled.”

Operation Xport was the first Anonymous operation of its kind. The goal was to smuggle Doyon, now a fugitive wanted for two felonies, out of the country. The coördinators were Kalli and a veteran Anon who had met Doyon at an acid party in Cambridge during the eighties. A retired software executive, he was widely respected within Anonymous.

Doyon’s ultimate destination was the software executive’s house, deep in rural Canada. In December, 2011, he hitchhiked to San Francisco and made his way to an Occupy encampment downtown. He found his designated contact, who helped him get to a pizzeria in Oakland. At 2 A.M., Doyon, using the pizzeria’s WiFi, received a message on encrypted chat.

“Are you near a window?” the message read.

“Yeah,” Doyon typed.

“Look across the street. Do you see the green mailbox? In exactly fifteen minutes, go and stand next to that mailbox and set your backpack down, and lay your mask on top of it.”

For a few weeks, Doyon shuttled among safe houses in the Bay Area, following instructions through encrypted chat. Eventually, he took a Greyhound bus to Seattle, where he stayed with a friend of the software executive. The friend, a wealthy retiree, spent hours using Google Earth to help Doyon plot a route to Canada. They went to a camping-supplies store, and the friend spent fifteen hundred dollars on gear for Doyon, including hiking boots and a new backpack. Then he drove Doyon two hours north and dropped him off in a remote area, several hundred miles from the border, where Doyon met up with Amber Lyon.

Months earlier, Lyon, a broadcast journalist, had interviewed Doyon for a CNN segment about Anonymous. He liked her report, and they stayed in touch. Lyon asked to join Doyon on his
escape, to shoot footage for a possible documentary. The software executive thought that it was “nuts” to take the risk, but Doyon invited her anyway. “I think he wanted to make himself a face of the movement,” Lyon told me. For four days, she filmed him as he hiked north, camping in the woods. “It wasn’t very organized,” Lyon recalls. “He was functionally homeless, so he just kind of wandered out of the country.”

On February 11, 2012, a press release appeared on Pastebin. “The PLF is delighted to announce that Commander X, aka Christopher Mark Doyon, has fled the jurisdiction of the USA and entered the relative safety of the nation of Canada,” it read. “The PLF calls upon the government of the USA to come to its senses and cease the harassment, surveillance—and arrest of not only Anonymous, but all activists.”

In Canada, Doyon spent a few days with the software executive in a small house in the woods. In a chat with Barrett Brown, Doyon was effusive.

BarrettBrown: you have enough safe houses, etc? . . .

CommanderX: Yes I am good here, money and houses a plenty in Canada.

CommanderX: Amber Lyon asked me on camera about you.

CommanderX: I think you will like my reply, and fuck the trolls Barrett. I have always loved you and always will.

CommanderX: :-)

CommanderX: I told her you were a hero.

BarrettBrown: you’re a hero . . .

BarrettBrown: glad you’re safe for now

BarrettBrown: let me know if you need anything

CommanderX: I am, and if this works we can get others out to . . . .

BarrettBrown: good, we’re going to need that

Ten days after Doyon’s escape, the Wall Street Journal reported that Keith Alexander, then the N.S.A. and U.S. Cyber Command director, had held classified meetings in the White House and elsewhere during which he expressed concern about Anonymous. Within two years, Alexander warned, the group might be capable of destabilizing national power grids. General Martin Dempsey, the chairman of the Joint Chiefs of Staff, told the Journal that an enemy of the U.S. “could give cyber malware capability to some fringe group,” adding, “We have to get after this.”

On March 8th, a briefing on cybersecurity was held for members of Congress at a Sensitive Compartmented Information Facility near the Capitol Building. Many of the country’s top security officials attended the briefing, including Alexander, Dempsey, Robert Mueller, the head
of the F.B.I., and Janet Napolitano, the Secretary of Homeland Security. Attendees were shown a
computer simulation of what a cyberattack on the Eastern Seaboard’s electrical supply might
look like. Anonymous was not yet capable of mounting an attack on this scale, but security
officials worried that they might join forces with other, more sophisticated groups. “As we were
dealing with this ever-increasing presence on the Net and ever-increasing risk, the government
nuts and bolts were still being worked out,” Napolitano told me. When discussing potential
cybersecurity threats, she added, “We often used Anonymous as Exhibit A.”

Anonymous might be the most powerful nongovernmental hacking collective in the world. Even
so, it has never demonstrated an ability or desire to damage any key elements of public
infrastructure. To some cybersecurity experts, the dire warnings about Anonymous sounded like
fearmongering. “There’s a big gap between declaring war on Orlando and pulling off a Stuxnet
attack,” James Andrew Lewis, a senior fellow at the Center for Strategic and International
Studies, told me, referring to the elaborate cyberstrike carried out by the U.S. and Israel against
Iranian nuclear sites in 2007. Yochai Benkler, a professor at Harvard Law School, told me,
“What we’ve seen is the use of drumbeating as justification for major defense spending of a form
that would otherwise be hard to justify.”

Keith Alexander, who recently retired from the government, declined to comment for this story,
as did representatives from the N.S.A., the F.B.I., the C.I.A., and the D.H.S. Although Anons
have never seriously compromised government computer networks, they have a record of
seeking revenge against individuals who anger them. Andy Purdy, the former head of the
national-cybersecurity division of the D.H.S., told me that “a fear of retaliation,” both
institutional and personal, prevents government representatives from speaking out against
Anonymous. “Everyone is vulnerable,” he said.

On March 6, 2012, Hector Xavier Monsegur, a key member of LulzSec with the screen name
Sabu, was revealed to be an F.B.I. informant. In exchange for a reduced sentence, Monsegur
had spent several months undercover, helping to gather evidence against other LulzSec members.
The same day, five leading Anons were arrested and charged with several crimes, including
computer conspiracy. An F.B.I. official told Fox News, “This is devastating to the organization.
We’re chopping off the head of LulzSec.” Over the next ten months, Barrett Brown was indicted
on seventeen federal charges, most of which were later dropped. (He will be sentenced in
October.)

Doyon was distraught, but he continued to hack—and to seek attention. He appeared, masked, at
a Toronto screening of a documentary about Anonymous. He gave an interview to a reporter
from the National Post and boasted, without substantiation, “We have access to every classified
database in the U.S. government. It’s a matter of when we leak the contents of those databases,
not if.”

In January, 2013, after another Anon started an operation about the rape of a teen-age girl in
Steubenville, Ohio, Doyon repurposed LocalLeaks, a site he had created two years earlier, as a
clearinghouse for information about the rape. Like many Anonymous efforts, LocalLeaks was
both influential and irresponsible. It was the first site to widely disseminate the twelve-minute
video of a Steubenville High School graduate joking about the rape, which inflamed public
outrage about the story. But the site also perpetuated several false rumors about the case and it
failed to redact a court document, thus accidentally revealing the rape victim’s name. Doyon admitted to me that his strategy of releasing unexpurgated materials was controversial, but he recalled thinking, “We could either gut the Steubenville Files . . . or we could release everything we know, basically, with the caveat, Hey, you’ve got to trust us.”

In May, 2013, the Rustle League, a group of online trolls who often provoke Anonymous, hacked Doyon’s Twitter account. Shm00p, one of the leaders of Rustle League, told me, “We’re not trying to cause harm to the guy, but, just, the shit he was saying—it was comical to me.” The Rustle League implanted racist and anti-Semitic messages into Doyon’s account, such as a link to www.jewsdid911.org.

On August 27, 2013, Doyon posted a note announcing his retirement from Anonymous. “My entire life has been dedicated to fighting for justice and freedom,” he wrote. “‘Commander X’ may be invincible, but I am extremely ill from the exhaustion and stress of fighting in this epic global cyber war.” Reactions varied from compassion (“you deserve a rest”) to ridicule (“poor crazy old gnoll. Maybe he has some time for bathing now”). Covelli told me, “The persona has consumed him to the point where he can’t handle it anymore.”

The first Million Mask March took place on November 5, 2013. Several thousand people marched in support of Anonymous, in four hundred and fifty cities around the world. In a sign of how deeply Anonymous had penetrated popular culture, one protester in London removed his Guy Fawkes mask to reveal that he was the actor Russell Brand.

While I attended the rally in Washington, D.C., Doyon watched a livestream in Canada. I exchanged e-mails with him on my phone. “It is so surreal to sit here, sidelined and out of the game—and watch something that you helped create turn into this,” he wrote. “At least it all made a difference.”

We arranged a face-to-face meeting. Doyon insisted that I submit to elaborate plans made over encrypted chat. I was to fly to an airport several hours away, rent a car, drive to a remote location in Canada, and disable my phone.

I found him in a small, run-down apartment building in a quiet residential neighborhood. He wore a green Army-style jacket and a T-shirt featuring one of Anonymous’s logos: a black-suited man with a question mark instead of a face. The apartment was sparsely furnished and smelled of cigarette smoke. He discussed U.S. politics (“I have not voted in many elections—it’s all a rigged game”), militant Islam (“I believe that people in the Nigerian government essentially colluded to create a completely phony Al Qaeda affiliate called Boko Haram”), and his tenuous position within Anonymous (“These people who call themselves trolls are really just rotten, mean, evil people”).

Doyon had shaved his beard, and he looked gaunt. He told me that he was ill and that he rarely went outside. On his small desk were two laptops, a stack of books about Buddhism, and an overflowing ashtray. A Guy Fawkes mask hung on an otherwise bare yellow wall. He told me, “Underneath the whole X persona is a little old man who is in absolute agony at times.”

This past Christmas, the founder of the news site AnonInsiders visited him, bearing pie and cigarettes. Doyon asked the friend to succeed him as Supreme Commander of the P.L.F.,
offering “the keys to the kingdom”—all his passwords, as well as secret files relating to several Anonymous operations. The friend gently declined. “I have a life,” he told me.

On August 9, 2014, at 5:09 P.M. local time, Kareem (Tef Poe) Jackson, a rapper and activist from Dellwood, Missouri, a suburb of St. Louis, tweeted about a crisis unfolding in a neighboring town. “Basically martial law is taking place in Ferguson all perimeters blocked coming and going,” he wrote. “National and international friends Help!!!” Five hours earlier in Ferguson, an unarmed eighteen-year-old African-American, Michael Brown, had been shot to death by a white police officer. The police claimed that Brown had reached for the officer’s gun. Brown’s friend Dorian Johnson, who was with him at the time, said that Brown’s only offense was refusing to leave the middle of the street.

Within two hours, Jackson received a reply from a Twitter account called CommanderXanon. “You can certainly expect us,” the message read. “See if you can get us some live streams going, that would be useful.” In recent weeks, Doyon, still in Canada, had come out of retirement. In June, two months before his fiftieth birthday, he quit smoking (“#hacktheaddiction #ecigaretteswork #old,” he later tweeted). The following month, after fighting broke out in Gaza, he tweeted in support of Anonymous’s Operation Save Gaza, a series of DDoS strikes against Israeli Web sites. Doyon found the events in Ferguson even more compelling. Despite his idiosyncrasies, he had a knack for being early to a cause.

“Start collecting URLs for cops, city government,” Doyon tweeted. Within ten minutes, he had created an I.R.C. channel. “Anonymous Operation Ferguson is engaged,” he tweeted. Only two people retweeted the message.

The next morning, Doyon posted a link to a rudimentary Web site, which included a message to the people of Ferguson—“You are not alone, we will support you in every way possible”—and an ultimatum to the police: “If you abuse, harass or harm in any way the protesters in Ferguson, we will take every Web based asset of your departments and governments off line. That is not a threat, it is a promise.” Doyon appealed to the most visible Anonymous Twitter account, YourAnonNews, which has 1.3 million followers. “Please support Operation Ferguson,” he wrote. A minute later, YourAnonNews complied. That day, the hashtag #OpFerguson was tweeted more than six thousand times.

The crisis became a top news story, and Anons rallied around Operation Ferguson. As with the Arab Spring operations, Anonymous sent electronic care packages to protesters on the ground, including a riot guide (“Pick up the gas emitter and lob it back at the police”) and printable Guy Fawkes masks. As Jackson and other protesters marched through Ferguson, the police attempted to subdue them with rubber bullets and tear gas. “It looked like a scene from a Bruce Willis movie,” Jackson told me. “Barack Obama hasn’t supported us to the degree Anonymous has,” he said. “It’s comforting to know that someone out there has your back.”

One site, www.opferguson.com, turned out to be a honeypot—a trap designed to collect the Internet Protocol addresses of visitors and turn them over to law-enforcement agencies. Some suspected Commander X of being a government informant. In the #OpFerguson I.R.C., someone named Sherlock wrote, “Everyone got me scared clicking links. Unless it’s from a name I’ve seen a lot, I just avoid them.”
Protesters in Ferguson asked the police to reveal the name of the officer who had shot Brown. Several times, Anons echoed this demand. Someone tweeted, “Ferguson police better release the shooter’s name before Anonymous does the work for them.” In a community meeting on August 12th, Jon Belmar, the Chief of the St. Louis Police Department, refused. “We do not do that until they’re charged with an offense,” he said.

In retaliation, a hacker with the handle TheAnonMessage tweeted a link to what he claimed was a two-hour audio file of a police radio scanner, recorded around the time of Brown’s death. TheAnonMessage also doxed Belmar, tweeting what he purported to be the police chief’s home address, phone number, and photographs of his family—one of his son sleeping on a couch, another of Belmar posing with his wife. “Nice photo, Jon,” TheAnonMessage tweeted. “Your wife actually looks good for her age. Have you had enough?” An hour later, TheAnonMessage threatened to dox Belmar’s daughter.

Richard Stallman, the first-generation hacker from M.I.T., told me that though he supports many of Anonymous’s causes, he considered these dox attacks reprehensible. Even internally, TheAnonMessage’s actions were divisive. “Why bother doxing people who weren’t involved?” one Anon asked over I.R.C., adding that threatening Belmar’s family was “beyond stupid.” But TheAnonMessage and other Anons continued to seek information that could be used in future dox attacks. The names of Ferguson Police Department employees were available online, and Anons scoured the Internet, trying to suss out which of the officers had killed Brown.

In the early morning of August 14th, a few Anons became convinced, based on Facebook photos and other disparate clues, that Brown’s shooter was a thirty-two-year-old man named Bryan Willman. According to a transcript of an I.R.C., one Anon posted a photo of Willman with a swollen face; another noted, “The shooter claimed to have been hit in the face.” Another user, Anonymous|11057, acknowledged that his suspicion of Willman involved “a leap of probably bad logic.” Still, he wrote, “i just can’t shake it. i really truly honestly and without a shred of hard evidence think it’s him.”

TheAnonMessage seemed amused by the conversation, writing, “#RIPBryanWillman.” Other Anons urged caution. “Please be sure,” Anonymous|2252 wrote. “It’s not just about a man’s life, Anon can easily be turned on by the public if something truly unjust comes of this.”

The debate went on for more than an hour. Several Anons pointed out that there was no way to confirm that Willman had ever been a Ferguson police officer.

Anonymous|3549: @gs we still don’t have a confirmation that bry is even on PD

Intangir: tensions are high enough right now where there is a slim chance someone might care enough to kill him

Anonymous|11057: the only real way to get a confirmation would be an eyewitness report from the scene of the crime. otherwise it’s hearsay and shillery

Anonymous|11057: the fastest way to eliminate a suspect is to call him a suspect . . . we are all terrified of being unjust, but the pegs keep fitting in the holes . . .

From www.newyorker.com/magazine/2014/09/08/masked-avengers  2 September 2014
Many Anons remained uncomfortable with the idea of a dox. But around 7 A.M. a vote was taken. According to chat logs, of the eighty or so people in the I.R.C., fewer than ten participated. They decided to release Willman’s personal information.

Anonymous|2252: is this going on twitter?
anondepp: lol

Anonymous|2252: via @theanonmessage ?
TheAnonMessage: yup
TheAnonMessage: just did
anondepp: its up

Anonymous|2252: shit
TheAnonMessage: Lord in heaven…
Anonymous|3549: . . .have mercy on our souls
anondepp: lol

At 9:45 A.M., the St. Louis Police Department responded to TheAnonMessage. “Bryan Willman is not even an officer with Ferguson or St. Louis County PD,” the tweet read. “Do not release more info on this random citizen.” (The F.B.I. later opened an investigation into the hacking of police computers in Ferguson.) Twitter quickly suspended TheAnonMessage, but Willman’s name and address had been reported widely.

Willman is the head police dispatcher in St. Ann, a suburb west of Ferguson. When the St. Louis Police Department’s Intelligence Unit called to tell him that he had been named as the killer, Willman told me, “I thought it was the weirdest joke.” Within hours, he received hundreds of death threats on his social-media accounts. He stayed in his house for nearly a week, alone, under police protection. “I just want it all to go away,” he told me. He thinks that Anonymous has irreparably harmed his reputation. “I don’t see how they can ever think they can be trusted again,” he said.

“We are not perfect,” OpFerguson tweeted. “Anonymous makes mistakes, and we’ve made a few in the chaos of the past few days. For those, we apologize.” Though Doyon was not responsible for the errant dox attack, other Anons took the opportunity to shame him for having launched an operation that spiralled out of control. A Pastebin message, distributed by YourAnonNews, read, “You may notice contradictory tweets and information about #Ferguson and #OpFerguson from various Anonymous twitter accounts. Part of why there is dissension about this particular #op is that CommanderX is considered a ‘namefag/facefag’—a known entity who enjoys or at least doesn’t shun publicity—which is considered by most Anonymous to be bad form, for some probably fairly obvious reasons.”
On his personal Twitter account, Doyon denied any involvement with Op Ferguson and wrote, “I hate this shit. I don’t want drama and I don’t want to fight with people I thought were friends.” Within a couple of days, he was sounding hopeful again. He recently retweeted messages reading, “You call them rioters, we call them voices of the oppressed” and “Free Tibet.”

Doyon is still in hiding. Even Jay Leiderman, his attorney, does not know where he is. Leiderman says that, in addition to the charges in Santa Cruz, Doyon may face indictment for his role in the PayPal and Orlando attacks. If he is arrested and convicted on all counts, he could spend the rest of his life in prison. Following the example of Edward Snowden, he hopes to apply for asylum with the Russians. When we spoke, he used a lit cigarette to gesture around his apartment. “How is this better than a fucking jail cell? I never go out,” he said. “I will never speak with my family again. . . . It’s an incredibly high price to pay to do everything you can to keep people alive and free and informed.?”
Masked Avengers. 763 likes · 1 talking about this. Hard hitting melodic beats accompanied with our thoughts. Facebook is showing information to help you better understand the purpose of a Page. See actions taken by the people who manage and post content. Page created â€“ 19 February 2011. People.