# OpISIS 8.8: Winter 2010-2011 (Part 1)

On: September 29, 2022

Before heading into the remainder of events that occurred during the winter of 2010-2011, here's a quick recap about Christopher Doyon a.k.a. Commander X. In early December 2010, he infiltrated Anonymous via Operation Payback and then took credit for single-handedly taking down Mastercard's website. He also used Anonymous' IRC channels to recruit hackers for his personal operations.

After notifying the media and successfully recruiting at least one hacker, Doyon DDoS'd the government website of Santa Cruz County, a coastal area in California where he had been living since the spring of 2009. Hours after the attack, he called in to a local radio show with a poorly disguised voice under his new persona, Commander X.

He blamed the attack on a fictitious character he created and then repeatedly encouraged naive, local activists to commit cybercrimes by downloading (and using) a DDoS tool from his website. He even said that it was perfectly legal. It wasn't.

Less than two weeks later, he was arrested and his laptop was seized by the feds, on or around December 27, 2010. This was confirmed by Doyon's own attorney, local activists, and a book that Doyon published in 2017.

After he was released, Doyon did what he pretty much always does. He ran. According to the media, he spent the first three months of 2011 in San Francisco and the surrounding areas, and this is where Doyon's story finally starts to collide with events previously reported on in this series like the Arab Spring, #OpIsrael, and, eventually, the Mauritania Attacker, Teamr00t, and Anonghost.

## #OpTunisia, the Arab Spring, #OpIsrael, and Operation Payback

On November 28, 2010, WikiLeaks released thousands of U.S. diplomatic cables that *The New York Times* described as an "unprecedented look at back-room bargaining by embassies around the world, brutally candid views of foreign leaders and frank assessments of nuclear and terrorist threats." Among the thousands of documents that WikiLeaks released were cables about the Tunisian government, President Ben Ali, and widespread corruption:

> Some of the memos, which first appeared in November, were widely available in Tunisia after the WikiLeaks document dump, according to regional experts. They were translated and disseminated through private websites and social networking sites.
>
> One overarching theme of the cables: corruption. Many refer to Ben Ali's family as 'The Family,' which stood above the law and ruled the country without any control or restraint from the outside. Nepotism extended to the family of Ben Ali's wife, Leila, whose numerous siblings occupied critical government position or were the owners of media, airlines,

> assembly plants and distribution rights, according to one cable sent to Washington from Tunis in 2008.
>
> A U.S. Embassy cable from 2008 stated that Ben Ali's 'quasi-mafia' family lived in opulence, indulging in excessive consumption and authoritarian tactics to rule the country.
>
> The same cable revealed that the first lady of Tunisia benefited personally from a 2007 real estate boom. She received a valuable piece of land and $1.5 million in assistance from the government for the construction of the Carthage International School, which she later sold to investors from Belgium for 'a huge, but undisclosed sum,' according to the secret cable.
>
> 'There were a lot of specific details in the cables that the public had not been exposed to before the release. There is no question that WikiLeaks added substantial evidence to the story that people already knew,' said Shibley Telhami, Anwar Sadat professor for peace and development at the University of Maryland. (pbs.org)

On December 7, 2010, three days before Doyon said he infiltrated Anonymous, *The Guardian* reported that the government of Tunisia, a small, north African country wedged between Algeria and Libya along the Mediterranean Sea, had blocked the website of a Lebanese newspaper for publishing the U.S. cables.

Ten days later, a twenty-six-year old fruit vendor named Mohamed Bouazizi set himself on fire in the Tunisian town of Sidi Bouzid after police confiscated his produce. He became a symbol of freedom and resistance against Ben Ali's corrupt regime, and his actions set off a 28-day campaign of civil unrest throughout the country.

Meanwhile, Doyon arrived in San Francisco on or around January 1, 2011, after allegedly fleeing Santa Cruz within forty-eight hours of the FBI confiscating his laptop. The very next day, members of Anonymous turned their attention to the Tunisian protests and on January 4th, Huffington Post announced, "Anonymous shuts down Tunisian govt websites after violence and web censorship."

In his 2017 book, "Behind the Mask: An Inside Look at Anonymous," Doyon admits

that once Anonymous' Operation Tunisia came into fruition he immediately became deeply involved in it. For instance, he claimed that on January 7th, an anonymous Tunisian hactivist approached him for help extracting and publishing documents that proved there was "huge corruption within the security forces in our country."

"Send me the data you have on the networks," Doyon told them. He then gathered his "own crew as well as a couple of AntiSec folks and we created a private back-channel in IRC and set to work." Months later, aljazeera.com wrote:

> Tunisian Anons collaborated with their international counterparts on Operation Tunisia, which was launched on January 2 – well before most Western media outlets had clicked onto the fact that there was a revolution underway.
>
> 'We did initially take an interest in Tunisia because of WikiLeaks, but as more Tunisians have joined they care more about the general internet censorship there, so that's what it has become,' one Anon told Al Jazeera in the midst of the DDoS attacks on selected Tunisian government sites.
>
> As Anons realised the significance of what was taking place in Tunisia – and the fact that it was being ignored by foreign media – they collaborated with Tunisian dissidents to help them share videos with the outside world.
>
> Anonymous quickly created a 'care packet', translated into Arabic and French, offering cyberdissidents advice on how to conceal their identities on the web, in order to avoid detection by the former regime's cyberpolice.
>
> They used their collective brainpower to develop a greasemonkey script – an extension for the Mozilla Firefox web browser – to help Tunisians evade an extensive phishing campaign carried out by the government.

Just so we're clear about what Doyon did, unbeknownst to members of Anonymous, **SIX DAYS** after the FBI seized the electronic devices Doyon used for

Operation Payback and the DDoS attack against Santa Cruz, he fled to San Francisco. From this new location, he used a newly-adopted online identity named Commander X, his super secret underground militia group called the Peoples Liberation Front (PLF), the Tunisian Revolution, and local coffee shop WIFI, to plant himself deeper into Anonymous.

Unless Doyon confessed to all of this to members of Anonymous, my guess is that the hackers involved in #OpTunisia had no idea they were working with a guy whose devices and online identity (fake and real) were now in the hands of the feds.

On January 15th, Tunisian protestors successfully ousted President Ben Ali and the revolutionary spirit spread like wildfire across other countries like Libya, Egypt, Yemen, Syria, and Bahrain, sparking what became known as the Arab Spring.

Ten days later, Anonymous launched Operation Egypt and, again, Doyon placed himself directly inside the operation. According to his book, during the "early stages of the Egyptian Revolution," Doyon worked in "two principle areas, media and offensive cyber-attacks."

He also said that he was involved with data collection and created a spider that collected the "fax numbers and E-Mail addresses of every single Egyptian." Then, he supposedly separated civilian data from government data. Uh huh, could someone explain to me how he would know if a personal email address was owned by a civilian or a government employee? Anyhoo—

Doyon allegedly created the software program so he could "wage psychological warfare on the Egyptian government," while sending "valuable information and encouragement to the Egyptian people." The best part is that he did this alleged data scrapping from a coffee shop's free WIFI. Let's hope the guy connected to a VPN first.

The second best part? Again, there is literally nothing in Doyon's past to suggest that he had the skills to create such a program. Remember, in 2009, Doyon was touring with the Grateful Dead and then running around California as the "Wizard of Haight-Asbury," selling such services as tarot card readings and money spells. Additionally, the PLF didn't appear to exist until infiltration, and the leader of this super secret underground militia was a phony character Doyon created and used to recruit hackers.

# Anonymous Operations, Operation Payback Arrests, #OpIsrael, and HBGary Federal

At the same time that Anonymous was fighting censorship via #OpTunisia and #OpEgypt, the FBI was honing in on those involved in Operation Payback. #OpIsrael was also slowing taking shape. From #OpISIS Part 3:

> As these countries roiled in turmoil, #OpIsrael slowly took shape and the following is an attempt to put this operation's gradual development in context with both the hacktivist/WikiLeaks scene I reported on in the previous article and the Arab Spring.
>
> For example, when protests erupted in Libya and Egypt in January 2011, the U.K. police arrested five people in connection with 'Operation Payback,' an Anonymous operation that targeted 'companies and institutions considered hostile to WikiLeaks,' such as PayPal.
>
> In early February, unrest in Cairo's Tahrir Square turned violent as the battle for control between President Mubarak's supporters and protestors escalated. Meanwhile, the hashtag #OpIsrael was posted on Twitter for the first time by Simplon.co founder, Frédéric Bardeau (@fbardeau), who claimed that "Could we launch #Opisrael?" was heard in an "anon" Internet Relay Chat (IRC).

Without question, December 2010 through February 2011 were insanely busy months:

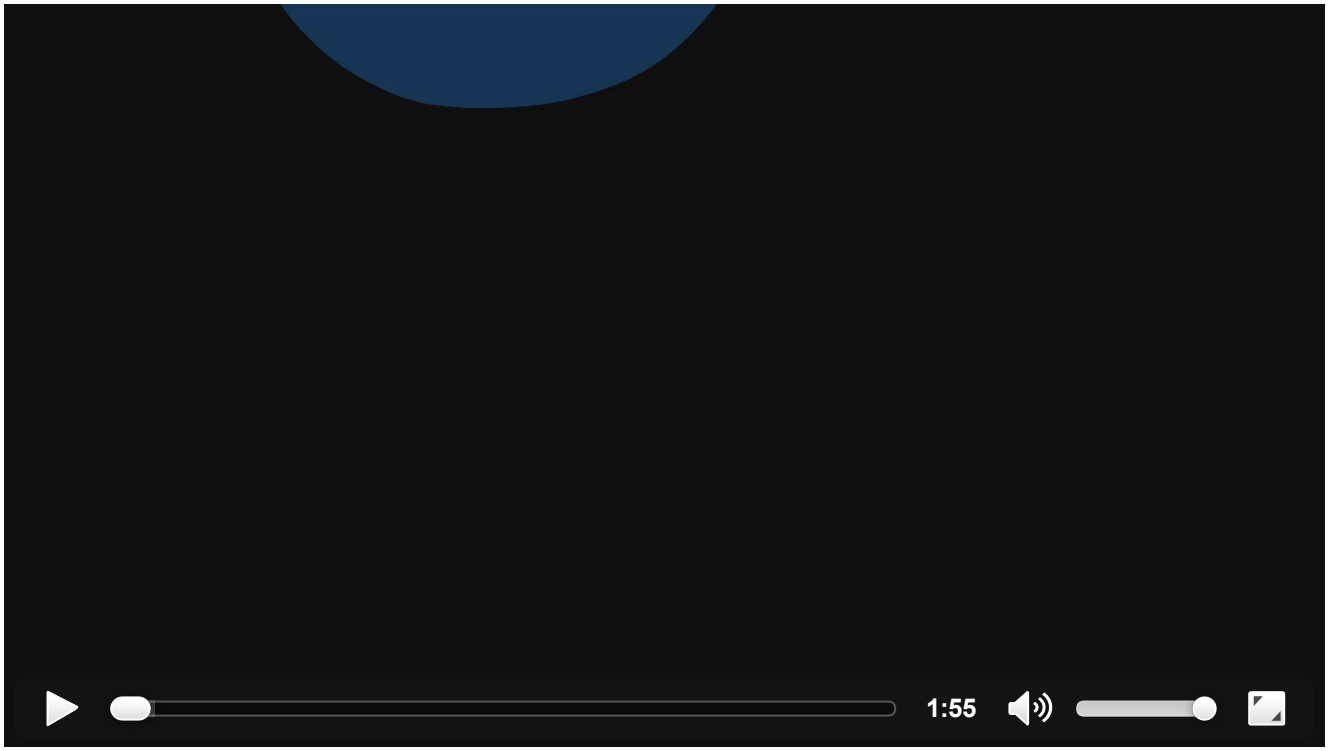
- Multiple Anonymous operations were launched (Operation Payback, Operation Tunisia, Operation Egypt)
- Doyon infiltrated Anonymous in early to mid-December 2010, and continued to do so further via #OpTunisia and #OpEgypt
- In late December 2010, Doyon became an early (if not the earliest) Operation Payback participant to have his devices seized by the feds

- The investigation into Operation Payback expanded exactly one month after the F.B.I. seized Doyon's laptop with the arrest of five people in the U.K. and forty federal search warrants served in the U.S.
- Widespread political unrest spread across the Middle East
- #OpIsrael was first mentioned on Twitter

In addition, the media reported that while Doyon was running around the San Francisco area, he created a leak platform called Local Leaks in January 2011. The creation date is unknown (to me), as is whether or not Doyon created it before or after the FBI served those forty Operation Payback warrants on January 27, 2011.

Remember, in the first major interview conducted with Doyon by *Ars Technica* in December 2012, he lied to the media outlet and said that he was served one of those warrants in what I believe was his attempt to hide from Anonymous the fact his Operation Payback laptop was seized by the feds one month prior.

Doyon later repurposed the Local Leaks website during the 2012 Steubenville rape case, and heroically assisted hackers in exposing the rapists…while simultaneously posting egregiously false information and doxing the rape victim. But long before this pseudo-hacker decided to inadvertently terrorize a high school student, there was Bank of America and HBGary Federal.



## Liked it? Take a second to support Jimmysllama on Patreon!

BECOME A PATRON

---

SHARE THIS:

Share

### Post Disclaimer

Disclaimer: Ten thousand more pages of disclaimers to follow.

If you were mentioned in this article because your associate(s) did or said something stupid/dishonest, that's not a suggestion that you did or said something stupid/dishonest or that you took part in it. Of course, some may conclude on their own that you associate with stupid/dishonest individuals but that's called having the right to an opinion. If I've questioned something that doesn't make sense to me, that's not me spinning the confusing material you've put out. That's me trying to make sense out of something that doesn't make sense. And if I've noted that you failed to back up your allegations that means I either missed where you posted it or you failed to back your shiz up.

If I haven't specifically stated that I believe (my opinion) someone is associated with someone else or an event, then it means just that. I haven't reported an association nor is there any inference of association on my part. For example, just because someone is mentioned in this article, it doesn't mean that they're involved or associated with everyone and everything else mentioned. If I believe that there's an association between people and/or events, I'll specifically report it.

If anyone mentioned in this article wants to claim that I have associated them with someone else or an event because I didn't disclose every single person and event in the world that they are NOT associated with, that's called gaslighting an audience and it's absurd hogwash i.e. "They mentioned that I liked bananas but they didn't disclose that I don't like apples. Why are they trying to associate me with apples???" Or something similar to this lovely gem, "I did NOT give Trish the thumb drive!" in order to make their lazy audience believe that it was reported

they gave Trish the thumb drive when, in fact, that was never reported, let alone inferred.

That's some of the BS I'm talking about so try not to act like a psychiatric patient, intelligence agent, or paid cyber mercenary by doing these things. If you would like to share your story, viewpoint, or any evidence that pertains to this article, or feel strongly that something needs to be clarified or corrected (again, that actually pertains to the article), you can reach me at jimmysllama@protonmail.com with any questions or concerns.

I cannot confirm and am not confirming the legitimacy of any messages or emails in this article. Please see a doctor if sensitivity continues. If anyone asks, feel free to tell them that I work for Schoenberger, Fitzgibbon, Steven Biss, the CIA, or really just about any intelligence agency because your idiocy, ongoing defamation, and failure as a human is truly a sight to behold for the rest of us.

If I described you as a fruit basket or even a mental patient it's because that is my opinion of you, it's not a diagnosis. I'm not a psychiatrist nor should anyone take my personal opinions as some sort of clinical assessment. Contact @BellaMagnani if you want a rundown on the psych profile she ran on you.

## LEAVE A REPLY

Enter your comment here

SUBSCRIBE TO BLOG VIA EMAIL

Enter your email address to subscribe to jimmysllama.com and receive notifications of new posts by email.

Email Address

Subscribe

RECENT POSTS

#OpISIS 8.8: Winter 2010-2011 (Part 4) October 11, 2022
#OpISIS 8.8: Winter 2010-2011 (Part 3) October 4, 2022
An Ongoing Log of All My Tweets Twitter Is Censoring (By Not Allowing Me to Retweet Them) October 3, 2022
Death By Algorithm October 1, 2022
Twitter Tactics: How Twitter Employees Use a Little-Known Censorship Tactic To Minimize Engagement and Readership October 1, 2022

---