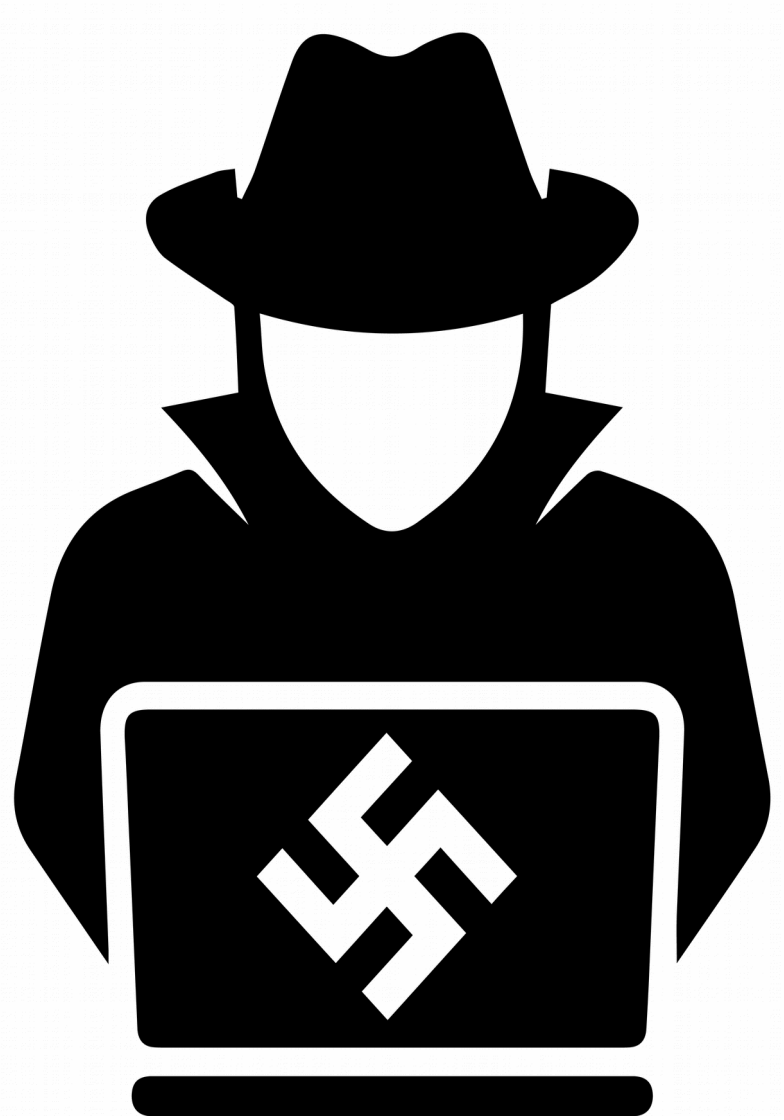
COMBATING ENEMY SURVEILLANCE

A PRIVACY & SECURITY GOYS™ PRACTICAL GUIDE



T.ME/PRIVSECGOY

DISCLAIMER

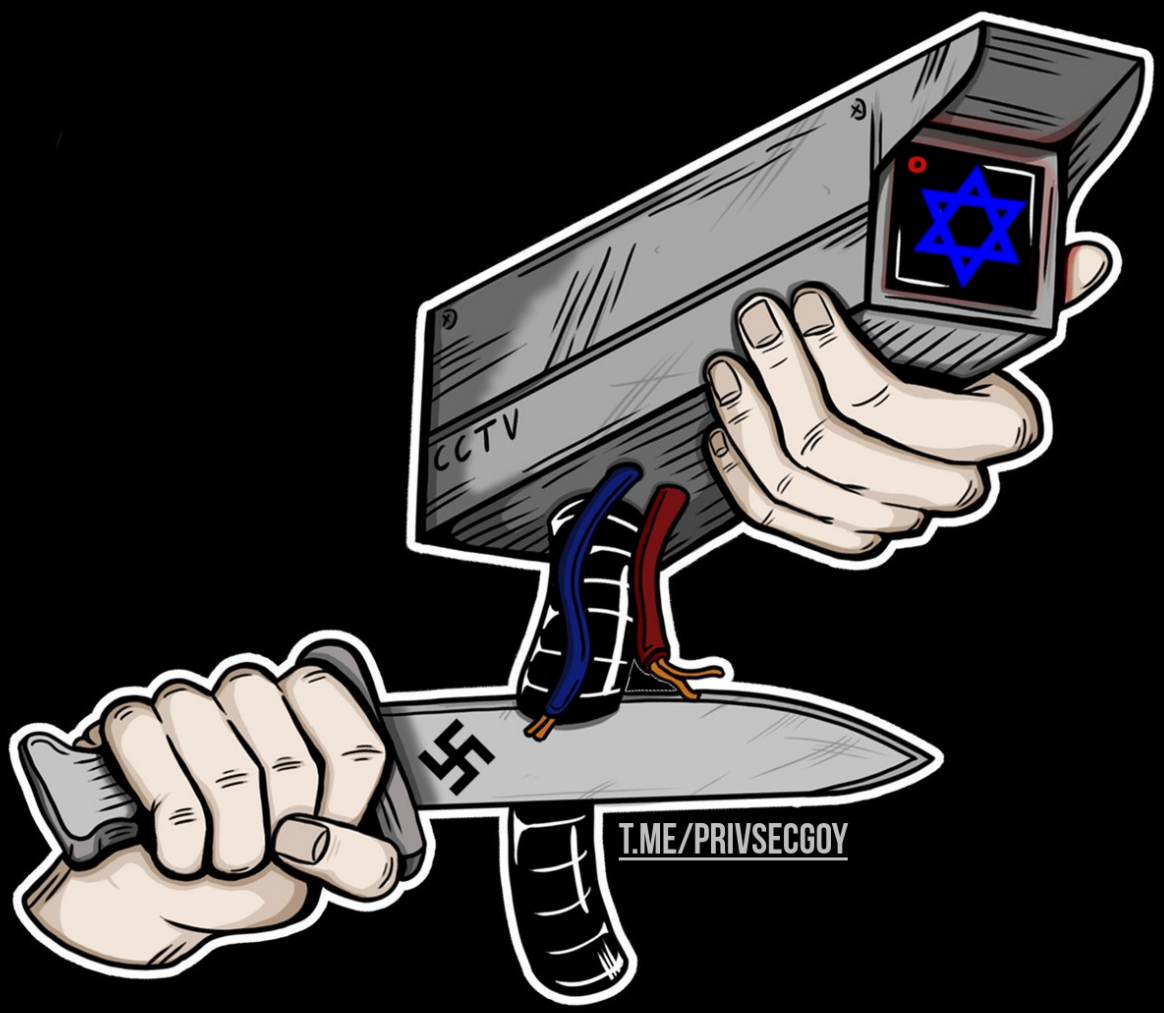
The content discussed herein describes techniques and practices that may be illegal in your jurisdiction. The onus is on the reader to keep up to date with their local laws and regulations. As good, law-abiding goyim, we do not condone the destruction of property that is not your own.

On an unrelated note, all public cameras are paid for with your tax dollars.

TABLE OF CONTENTS

WHAT ARE CCTV CAMERAS? 5
WHY DESTROY THEM? 8
TYPES OF CAMERAS 9
METHODS OF ATTACK 11
PLANNING AND EXECUTING AN ANTI-SURVEILLANCE ACTION 15
AN ANARCHIST'S EXPERIENCES 17
THANK YOU 18

DESTROY



SURVEILLANCE

WHAT ARE CCTV CAMERAS?

Closed-**c**ircuit **T**ele**v**ision (CCTV) is the use of video cameras to transmit a signal to a specific place on a set of monitors. These surveillance systems allow entities to monitor great spans of area remotely. The purpose is generally to record the environment to be used as evidence for when a crime happens. Some may be actively monitored by personnel to detect unauthorized activity as it happens, but most are not.

There are three types of security cameras:

1. Public
2. Corporate
3. Residential

Public cameras serve as the System's eyes. As the name suggests, they monitor and record public areas. In some areas, this may be non-existent. In others, there may be public CCTV covering practically every angle of urban areas, such as in China or the Netherlands. [These people are being recorded from the moment they step outside of their home, to the moment they get back. If they have personal spyware like Amazon's Echo/Alexa, Google Home/Nest, a smartphone, etc., they have no privacy anywhere. As one can imagine, it would be difficult to do anything in these areas without the System knowing who you are. It is important, then, to stop the System from expanding their surveillance capacity before it reaches this point.]

Corporate cameras are cameras used in the private sector to surveil their business's property and assets. Large businesses, such as supermarkets, colleges, and construction sites are typically the most likely to be actively monitored by personnel (security guards). Corporate cameras are primarily used to save money on insurance, as they record evidence on theft or damage to property. Many external corporate cameras also record public areas, such as roads and sidewalks. While the police technically require a warrant to view/seize private CCTV footage, >99% of businesses will provide these recordings voluntarily. [If you park your car in a Walmart parking lot before putting up fliers on public property, don't expect Walmart to destroy the tapes for you.]

Finally, residential cameras are privately-owned CCTV systems that are used to surveil homes and personal property.

A CCTV's storage capacity is limited to the budget of their owner. One camera system may be as simple as one 480p camera recording at 20 frames per second (fps), one monitor, and a dedicated 500GB hard drive. This setup would allow for 22 consecutive days of 24/7 video if using MPEG-4 encoding, or 33 days if using the superior H.264 encoding. After the hard drive has been filled, it will rewrite over the oldest footage.

NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	694	1388	2082	2776	3470	4164
352 x 240		# Days	266	532	798	1064	1330	1596
704 x 480		# Days	86	172	258	344	430	516
1280 x 1024	High Quality	# Days	26	52	78	104	130	156

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	346	692	1038	1384	1730	2076
352 x 240		# Days	132	264	396	528	660	792
704 x 480		# Days	42	84	126	168	210	252
1280 x 1024	High Quality	# Days	12	24	36	48	60	72

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	230	460	690	920	1150	1380
352 x 240		# Days	88	176	264	352	440	528
704 x 480		# Days	28	56	84	112	140	168
1280 x 1024	High Quality	# Days	8	16	24	32	40	48

Table 1. Video Surveillance Storage Matrix (assumes MPEG-4 encoding)

NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	1080	2160	3240	4320	5400	6480
352 x 240		# Days	414	828	1242	1656	2070	2484
704 x 480		# Days	134	268	402	536	670	804
1280 x 1024	High Quality	# Days	40	80	120	160	200	240

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	540	1080	1620	2160	2700	3240
352 x 240		# Days	206	412	618	824	1030	1236
704 x 480		# Days	66	132	198	264	330	396
1280 x 1024	High Quality	# Days	20	40	60	80	100	120

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	360	720	1080	1440	1800	2160
352 x 240		# Days	138	276	414	552	690	828
704 x 480		# Days	44	88	132	176	220	264
1280 x 1024	High Quality	# Days	14	28	42	56	70	84

Table 2. Video Surveillance Storage Matrix (assumes H.264 encoding)

Compare this to something like a college campus, that may require >100 cameras. This would require >50 TB to achieve the same storage capacity, using the same camera quality and fps. [Note that the property owner does not necessarily need to physically possess these hard drives. Corporations often utilize cloud storage in lieu of or in addition to purchasing hard drives.] In almost all cases, a private individual will have a smaller budget than a large business, and there is typically little point for a home owner to keep months of video footage if nothing happened. Corporate and government entities may choose to keep footage indefinitely (or at least for 6+ months), depending on what their objectives may be.

As a general rule of thumb, 80% of CCTV systems use between 60GB and 600GB of data storage; 99% use between 6GB and 6TB. If someone's budget was extremely tight, they could use something as small as a 4GB memory stick and have the camera only record movement in an area with little activity.

tl;dr – Don't rely on your target (or an adjacent property) to overwrite footage of you without noticing what you've done. Only the weakest adversaries would fail to notice damage to their cameras until after the incident was overwritten. And even if this undeterminable length of time has passed, it is extremely easy for them to make backups of selected incidents on another hard drive or on physical media like a DVD-R.

WHY DESTROY THEM?

If you have two brain cells to rub together, you understand that we are living under a tyrannical and oppressive anti-White regime. As long as this System remains kosher, we are to remain persecuted and systemically replaced, with the end-goal of genociding us out of existence.

Say what you will about this dysgenic dystopia we have inherited, but at the very least, it is a very target-rich environment. Unlike what the misled Marxists involved with BLM/Antifa believe, it's not just the police who have to go. The *entire* System is a fair target, and **every attack on the System is praise-worthy.**

From a less revolutionary perspective, mass surveillance is an affront to our privacy. It doesn't reduce crime, and raises anxiety in people who have no intention on breaking the law. As mentioned earlier, CCTV is primarily used to collect and analyze evidence after a crime, and is used to save money on (((insurance))).

Public CCTV is expensive to maintain. These cameras are also prone to failing. An 2013 audit of the City of Philadelphia found that the $15,000,000 system was only operational 32% of the time. Additionally, a 2008 Report by UK Police Chiefs concluded that "only 3% of crimes were solved by CCTV," and in London, a Metropolitan Police report showed that in 2008 only one crime was solved per 1000 cameras.

Bottom line: **a high-trust society does not require cameras!** We don't have that, so it must be known for everyone regardless of political affiliation that the entire System needs to be destroyed in order for us to survive as anything more than a pathetic slave-class. **Cameras serve to indict dissidents who take direct action against a System that seeks to destroy us.**

TYPES OF CAMERAS

1. **Dummy CCTV Cameras** often implement the stereotypical blinking red light, which is a tell-tale sign to most criminals that it is fake. These fake cameras are used because they are dirt-cheap, and as such, are most likely to be implemented outside of private homes. The government and businesses tend to avoid using these, because they have the budget for an operational CCTV system, and having false cameras does them no favors from an insurance perspective.
2. **Bullet Type Cameras** are designed for capturing images in a fixed area. These cameras are recognized by their thin and cylindrical design. There are also classifications of Ultra Bullet distinguished by their smaller size and cheaper price.
3. **Dome Cameras**, named after the shape of their housing are designed for in-store installations. It works in two ways as it is unobtrusive but visible, thus, it warns people that the area is protected by a CCTV network and gives comfort to its clients for its security. It is hard to tell where the camera is facing from afar.
4. **Discreet CCTVs** are cameras in disguise, they could look like a fan or any other thing that would not seem suspicious in the area. They are also useful for back-up surveillance in installations where the primary CCTV equipment is of a more traditional nature, i.e. standard cameras. In this case, covert cameras can operate as a back-up where primary cameras are disabled by an intruder. The use of hidden cameras is “discouraged” by the U.K. government, but other governments, agencies, and institutions may have different policies.
5. **Day/Night Types** are used for 24/7 installation, these cameras compensate light conditions with its wide dynamic range to function in glare, direct sunlight, reflections and strong backlight.
6. **Varifocal Cameras** are designed to allow zooming in and out without losing focus on the image.
7. **Network Cameras** allow transmission of images through the internet with controlled bandwidth.

8. **Wireless cameras** are cameras that may or may not be connected to the internet. These cameras use signaling devices to transmit images from camera to viewing area.
9. **Pan-tilt-zoom (PTZ) Cameras** can rotate accordingly. There are variations of these cameras that are programmable and are manually controllable. This allows viewers to have more freedom and control on viewing things.
10. **High definition cameras** are often used in casinos or high risk establishment. With its high resolution lens, capturing images are possible giving viewers a finer detail on taken images.

METHODS OF ATTACK

I've looked at what some self-described anarchists have used as tactics, and have listed some of them here. It is typical for these posers who claim to be "revolutionaries" that most of their plans are not permanent. They provide temporary and almost intentionally harmless measures, which hammers home the idea that their end-goals are more in line with "covering CCTV cameras so they can publicly drink booze, smoke weed, and do kick-flips in a skate park at night" rather than "the complete destruction of this System."

Plastic/garbage bag

(Leftist) anarchists claim that one simple method is to "use a plastic bag filled with glue. Use industrial grade bags, which are thicker. Sometimes a camera going into repair will be 'bagged' over, so it's visually ambiguous."

I personally think that's retarded; if you are close enough to put a bag over the camera, there is no reason to fuck around with coating the interior of the bag with glue. They also claim it's important to remove the bag afterwards; "people need to see the units [sic?] smashed." Generally, this isn't true. I understand the idea behind making it obvious that the camera was destroyed in order to "motivate more revolutionaries to take up arms," but using an overt destruction method will bring more System attention to it than anything. A security guard on patrol will notice a shattered CCTV camera long before a civilian would. It'll get replaced eventually, but don't needlessly tip off the enemy. Bag it, smash the lens with a hammer, and then walk away.

+ Cheap
+ Quick
+ Gives clear indication of inoperability
- Requires physical access to camera
- Glue is only semi-permanent at best

Sticker or tape

Simply placing a sticker or tape over lens. Only advantage to do this over smashing the camera (as far as I'm concerned) is that you attract less attention with a sticker or electrical/duct tape on the lens rather than the sight/sound of causing real damage.

+ Cheap
+ Quick
+ Covert
+ Gives clear indication of inoperability
- Not permanent

Paint gun

A child's water gun filled with household paint. "Fast, fun and easy." Easy to disable many cameras in a short period of time. Carry reserve paint in plastic containers. Filter paint to remove lumps to avoid blockages in the gun. Go for lens first, and then feel free to cover the rest of the camera.

The anarchists claimed to have used "super soaker SC 400 – 2000 Edition camoflaged [sic] for urban night actions." Use disposable clothing in case paint lands on you.

+ Medium-range; no climbing required
+ Clear indication of inoperability
- Paint is easily removed

Cable cutting

Cables can be cut with shears, a hatchet, etc. Make sure the tools are insulated with a rubber handle to prevent potential shock from camera power supply, and ideally wear electric shock-resistant footwear.

Anarchists claim that this method "requires complete costly rewiring" and creates "satisfying sparks emitted when cables cut." The anarchist who wrote that clearly watched too many action movies. Cutting cables should not cause a power surge, but just to be safe, cut one wire at a time instead of the whole cable at once. More on this on page 15.

+ Gives clear indication of inoperability
+ Semi-permanent
+ Costly and time-consuming for the System to replace wiring
+ May appear as if the camera is undergoing repair if wires are dangling (covert)
- Requires physical access to wiring, which is not typically exposed
- Many modern cameras are wireless

Block drop

“Climb to the roof of the building on which the camera is mounted with some heavy weights eg concrete blocks and drop them on the cameras below. Get correct drop position by dropping small stones first. Camera will be totally destroyed in a shower of sparks. Scaling tall buidlings [sic] with concrete blocks requires a certain level of fitness. Pay careful attention to safety of others below. This is a seriously hardcore method.”

This is a total LARP to me. Nobody is “scaling” buildings to drop concrete blocks on cameras. If you’re dead set on using rocks, treat cameras like Muslims do with gays and stone them instead.

Laser Pointer

During the BLM/Antifa riots of 2020, several civilian combatants aimed high-powered lasers in the faces of riot police to cause blindness. While the enforcers of jewish tyranny are always a good target, you can also use these to temporarily or permanently blind cameras.

Some activists report laser pointers as weak as 5mW are effective enough, but I personally would opt for something stronger than 100mW. Try to burn something like a paper napkin to see how long it takes to cause marks. If it can burn paper, it can burn a camera lens. Hold the laser in specific areas and wait a while. If you see smoke, that’s a great indicator that it is permanently destroyed.

The major drawback of this method is that it is difficult to verify whether or not you have destroyed the camera sufficiently (assuming there are no physical signs like smoke), unless you have access to the footage (via a camera’s public IP address) or have a guy on the inside who is able to verify the status of the camera (a bribed or sympathizer security guard on duty).

+ Long-range
+ Concealable
+ Discreet destruction of cameras
+ Can be attached to binoculars for better stability
- Requires focus and stability to keep laser on the same spot
- May be difficult to verify destruction of lens
- May be difficult to purchase high-power laser without paper trail

The jew fears the outdoor camera destroyer

PLANNING AND EXECUTING AN ANTI-SURVEILLANCE ACTION

1) Scout out the locations of cameras in your town or city region and make a map. Once the map is made, examine camera locations to determine intersections and roads to focus on. You may want to free up certain routes of travel from cameras or you may just want to get them out of your neighborhood. You may even try to eliminate them from your city entirely.

2) Take note of which poles have cameras mounted on them (some poles may have multiple cameras mounted). Observe which direction the cameras are pointing and look around the area to see if there is a way to approach the base of the traffic poles while minimizing exposure to the cameras. Near the ground on the traffic pole is a base plate. The base plate is about one foot off of the ground and is either metal or plastic with the approximate dimensions of 4-inches by 5-inches. The base plate is where you can access the cameras cables. The base plate is typically held in place with a single screw that requires a six-sided hex wrench to unscrew (turn counter-clockwise to unscrew). Some base plates occasionally require a flat-head screw driver or other tool to remove. Also, observe what the cables look like that connect to the camera at the top of the pole. You will need to find these cables when you open the base plate. They are typically two separate black round wires or a single black wire (with the two wires integrated). When you open the base plate there will be a jumble of wires of different colors (red, white, green, etc.). The colorful wires are used for traffic lights and are easy to decipher from the black cables. You will cut the black wires.

3) Dress to conceal your features and to prevent the transfer of finger prints. Disposable face masks are your friend. Cold weather is a good time to do this type of action, as you can wear scarves, hats, and gloves without appearing conspicuous. Halloween might be another good time to go out. You want your face to be obscured to hide your identity should you be observed or archived on camera. Wear gloves when handling tools, the base plate or wires.

4) Clean your tools. You will need a wire cutter and a hex wrench set – find one that is not metric and has wrenches of different sizes as there is some variation in screw sizes used on the base

plates. Occasionally, the base plate will require a flathead screwdriver. (In this town you will also need tin snips to cut through a metal band that the city has placed over the base plate after the first incident of camera sabotage occurred). Try to find wire cutters that have insulated handles certified for electrical work to reduce the chance of shock. Tools should be cleaned thoroughly of finger prints if you have touched them before, use mineral spirits to wipe them down. You may want to dispose of your wire cutters after use or file them down and store them in a safe place. These tools are fairly affordable or stealable. Try to acquire them long before the action from an area away from where the action will occur. Pay in cash if purchased.

5) Deployment considerations. Aside from operating solo, there's a couple other formats to consider:

Street Demonstrations – A group of people who have experience with this method of sabotage could take advantage of street demonstrations to cut the wires of intersection cameras and then blend back into the crowd. Using a BLM or MAGA (if that's still a thing in the current year) rally as cover would be ideal.

Small Group – This can be done with a group of trusted friends who coordinate their activities and select intersections to disable. You will want to consider whether to pair up, work alone, mob an intersection, or try some other combination. Maybe a small group could stand around and conceal the person gaining access to the camera wires.

6) Other Methods – Traffic cameras that are used for ticketing by taking a photo of your license plate when running a red light are often lower to the ground. These can often be spray-painted over as they are reachable from the ground. The cables on these cameras are typically protected by metallic flexible tubing requiring more than wire cutters to cut through.

AN ANARCHIST'S EXPERIENCES

"When the wires are cut, there is typically one black wire that sparks and one that doesn't. The one that sparks is the power source. When the wires are cut, the positive and negative wires sometimes touch, this causes arcing of the electricity, which causes the spark. It is hoped that this occasionally causes a power surge and destroys the camera unit. Cutting this wire will sometimes cause pitting on the wire cutters. Of the thirty cameras cut, only once was shock felt, only once was a loud "bzzzzt" sound heard along with a big spark, and occasionally all of the intersection lights would go out for some unexplained reason. These cameras don't require much voltage, so accidental shock should not lead to any injury to yourself. Wearing insulated gloves or shoes will add more layers of protection against shock if you want to be extra safe. DON'T DO THIS TYPE OF ACTIVITY IN THE RAIN! The wire that doesn't spark is used to transfer the images via fiber optic or coaxial cable. ~~As far as I know the fiber optic cable cannot be spliced back together requiring the entire cable to be completely replaced.~~"

The last sentence is incorrect; fiber-optic cable can be easily spliced, but this still requires time, resources, and manpower to fix. The cameras you destroy will likely be repaired, but remember that we are fighting a war of attrition. The System will die by a million cuts. Every action against the camera surveillance network has a cost, and will eventually become too costly for your city to maintain on its limited budget.

THANK YOU

Thank you for reading this guide! If you found this free guide particularly helpful, consider sending some shekels our way. I humbly accept crypto donations. Mix and send some Bitcoin to make the jew intelligence agencies monitoring us lose their minds. ☺

My Bitcoin address:
bc1qmu8fwtexd76vsy0vtka4cv9je0un5nkq50d3mm

My Monero address (one line):
435fDoJe16fcnjaufhLdYpR1pywz83jjh9UaHwLNxTJ3EXWkRA6DFkggZ3NUup6LQJTGW86mFnYGhdiFQewHRTvAHqHoX5u

卐卐卐

Our **Hidden Service:**
goysec74znsyewq3nu2i3kmwozxptc3lx22jg67km6r2we37ejiaz5yd.onion
Our **Telegram**
Channel: @PrivSecGoy
Chat: @PrivSecChat
Keep our servers running! Our **Monero Address (one line):**
44afqsvYK6qeqPsNftcqWeJNSqYjP8jXtFcX2A8AQDKzCR1pusDSUehXNJBCqjmf4oVwd7VsRr2NZVMdEEe6i78ESzYcXWp