

MOVIMENTO NO TAV: VIDEOSORVEGLIANZA COME MEZZO DI CONTRASTO AL SABOTAGGIO DELLA CONTINUITA' DEI CANTIERI

Nel mio lavoro ho cercato di analizzare quello che può definirsi uno dei fenomeni di maggiore impatto sociale degli ultimi anni.

Sono partito analizzando la storia del movimento No Tav fin dalla sua nascita e ho fatto una rassegna dei suoi momenti salienti e degli episodi eclatanti che l'hanno visto coinvolto e citato nelle cronache di tutta Europa.

Dal punto di vista della security, è balzato subito all'occhio come questo lavoro dovesse concentrarsi sui mezzi a disposizione che le imprese pubbliche e private, coinvolte nel progetto della costruzione della linea ad alta velocità Torino-Lione, utilizzano per contrastare i continui tentativi di sabotaggio dei cantieri, l'aggressione fisica nei confronti dei lavoratori e la continua minaccia di messa a rischio del corretto proseguimento del business plan aziendale nelle tempistiche programmate.

Dopo un'analisi dei più eclatanti atti di sabotaggio e manifestazione messi in atto dagli "attivisti" del movimento, ho cercato di individuare quello che è risultato il mezzo di contrasto più utilizzato dalle aziende coinvolte nel progetto per cercare di garantirsi una continuità di business: la videosorveglianza.

Ho cercato quindi di fare un'analisi più dettagliata dei vari elementi che compongono le telecamere professionali odierne, partendo dall'evoluzione della **tecnologia TVCC** e analizzandola nei suoi elementi fondamentali, definendo sistemi come le **unità di brandeggio**, la complessità e la componentistica dei **monitor**, i **dispositivi di controllo delle immagini multiple**, il funzionamento del **selettore ciclico**, strumento utilizzato dalle forze dell'ordine per individuare i manifestanti in quanto consente

la visualizzazione di immagini in serie, provenienti da diverse telecamere fino ad arrivare alla spiegazione di dispositivi quali, il **divisore di quadro**, le **matrici video** e i **multiplexer**.

Segue poi un'analisi delle **smart grid**, che rappresentano l'evoluzione delle attuali reti di distribuzione elettrica relativamente alla crescente domanda di energia e all'evoluzione nelle tecnologie informative: un'efficiente soluzione dal punto di vista energetico e soprattutto economico.

I soggetti interessati dalle **smart grid** infatti, sono tutte le utenze che spaziano dal semplice utilizzatore e dai produttori di energia fino ai cantieri della TAV, i quali, essendo bersaglio preferito degli "attivisti" devono mettere in conto anche l'eventualità, non troppo remota, di subire improvvise e imprevedute interruzioni della fornitura di energia elettrica.

Ho poi analizzato varie tipologie di "attacco" ai sistemi come l'attacco **MITM** (Man In The Middle) e l'attacco **Replay**, soffermandomi poi sui limiti giuridici della videosorveglianza e i soggetti titolari autorizzati all'utilizzo di essa, facendo una dettagliata analisi sulle norme giuridiche di riferimento.

Il lavoro si conclude poi con un'analisi delle possibili evoluzioni di questi sistemi, partendo dall'utilizzo del **cloud computing**, accennando a concetti quali i **costi** e l'**accessibilità**, fino ad arrivare all'utilizzo dei **droni** come nuova frontiera della videosorveglianza remota.

In conclusione, l'analisi svolta ha inteso illustrare da una parte, il ruolo effettivo e concreto che le moderne infrastrutture di videosorveglianza possono svolgere in direzione della creazione di un sistema efficiente e flessibile per il controllo remoto delle aree critiche dei cantieri della TAV in Val di Susa, dall'altra parte, si è anche avuto modo di osservare come gli ostacoli a una piena efficienza delle tecnologie di videosorveglianza provengano in realtà dall'esterno, dal rischio insito nella Rete e rappresentato dalla Cyber criminalità e, soprattutto, dai limiti legislativi e giuridici frapposti all'esecuzione della videosorveglianza.