A.S.
2012/13

TESINA MATURITÁ

“SPIONAGGIO INFORMATICO”

L’evoluzione spionistica della guerra affrontata su diversi tematiche

Studente : Federico Di Fabio
Istituto : ITIS G. Vallauri
Indirizzo : Informatica

INDICE

PREMESSA

Nella mia tesi ho deciso di proporre il tema dello spionaggio informatico,perché mi affascina molto l'evoluzione della guerra nel corso degli anni,soprattutto nel '900.

Premetto di non essere un esperto in materia,ma grazie al percorso di studi intrapreso mi è stato possibile soffermare i miei interessi su alcuni argomenti che mi sono stati proposti. Quindi ho voluto iniziare la stesura della tesi con un piccolo punto riguardante cosa è per me la guerra e su come sia stato possibile arrivare a parlare di cyber-guerra.

Nell'ambito della contesa tra due stati,mi ha sempre interessato la strategia con cui i pretendenti alla scontro si preparavano alla guerra,e su come questo si ripercuoteva sul fattore politico-economico del paese in questione. Informandomi su questo tema mi ha colpito la nuova forma di guerra che da pochi anni ha invaso il mondo intero,la guerra cibernetica.,e quindi ho deciso di proporlo come argomento d'esame.

Nella tesi che segue ho spiegato il significato di "spionaggio informatico",a cui poi ho collegato le materie studiate durante l'anno,per cercare di dare una nuova definizione alla parola **guerra**.

La tesi è strutturata nelle seguenti fasi :

1. Introduzione all'argomento scelto : Qui ho proposto un analisi dell'argomento centrale studiato,spiegando passo passo i punti fondamentali relativi ad esso.
2. Spiegazione del percorso didattico intrapreso : Qui ho voluto proporre una mappa concettuale dei collegamenti effettuati tra le materie studiate e l'argomento proposto. Al termine di questa spiegazione ho stilato,materia per materia,una documentazione relativa all'argomento intrapreso ed al collegamento effettuato.
3. Conclusione : In questa fase ho appuntato le risposte alle domande sull'argomento intrapreso per dare un idea di quale percorso ho intrapreso.
4. Angolo informativo : Nell'ultima parte ho proposto prima un glossario dove verrà spiegato il significato di alcuni termini incontrati nella lettura della tesi,per chiarire il loro significato e poter correggere alcuni chiarimenti. Questi termini sono contrassegnati dall'asterisco e dalla parola evidenziata in nero. In secondo luogo ho inserito la lista di libri,articoli ed interviste che mi hanno aiutato ad esporre il concetto della tesi.

DEFINIZIONE

La **spionaggio informatico** indica l'insieme delle attività di natura illecita,divulgate attraverso l'utilizzo di strumenti informatici. A questo genere di attività vengono legati i termini di **Hacker** ed **Hacking**.

La parola Hacker deriva dal verbo inglese "to hack",cioè "fare a pezzi,e si identifica in quell'individuo intenzionato ad affrontare sfide a livello intellettuale,superando i limiti a lui imposti.

Altro è,se si vuole definire l'Hacker a livello informatico,in quanto si fa riferimento a quel gruppo di persone che utilizzano le proprie conoscenze in materia per violare i limiti di sicurezza imposti dal computer ed irrompere nel suo sistema.

L'Hacking si definisce come l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema hardware o software. Ed è questo il fulcro principale delle attività di un hacker,ovvero violare la sicurezza informatica di un sistema. Garantire la **sicurezza** di un sistema,infatti,significa impedire che esso sia omesso da operazioni esterne o non autorizzate ; quando si parla di **integrità** si intende la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali oppure effettuate da una terza parte.

Dopo aver definito l'hacker e le sue attività,e parlato della sicurezza dei dati,diamo uno sguardo alla realtà del mondo hacker.

Molto spesso il lavoro degli hacker viene sfruttato anche per **aumentare la sicurezza informatica**. Scoprendo falle di sicurezza nei programmi o nei sistemi informatici, infatti, rendono disponibili informazioni su come "mettere una pezza" a quella stessa falla. Casi del genere accadono quasi quotidianamente, e uno degli ultimi ha visto coinvolta Skype, costretta a correre ai ripari dopo che degli hacker russi avevano trovato un modo per resettare le password degli account.

Quindi non sempre il lavoro degli hacker è inteso come minaccia,ma come detto prima,un aiuto per l'evoluzione dei sistemi di sicurezza. Infatti è da qui che viene fuori una divisione sostanziale degli hacker,ovvero : 1) "**White hat hacker**". 2)"**Black hat** hacker".

1) I White hat hacker,detti anche a cappello bianco, sono quelli che riescono ad inserirsi in un sistema o in una rete per aiutare i proprietari a prendere coscienza di un problema di sicurezza. Molte di queste persone sono impiegate in aziende informatiche di sicurezza,lavorando legalmente.

2) I Black hat hacker,detti anche a cappello nero,invece,sono collegati al vandalismo informatico e rappresentano quel gruppo di persone con grandi conoscenze informatiche ma con fini illeciti. Nella maggior parte dei casi, un black hat lavora per causare un danno, o per prelevare informazioni private e spesso per trarne profitti economici. Il black hat hacking è l'atto che compromettere la sicurezza informatica di un sistema senza l'autorizzazione del proprietario, di solito con l'intento di accedere ai computer connessi alla rete.

Un'altra definizione da illustrare è quella relativa al **cracker**,simile al black hat hacker,ovvero colui che elude qualsiasi blocco di sicurezza,solamente per trarne profitto. Infatti Molti hacker tentano di convincere l'opinione pubblica che gli intrusi dovrebbero essere chiamati cracker piuttosto che hacker. La differenza fra attacco di hacking e attacco di cracking risulta importante: mentre un hacker si impegna per sottrarre dei dati da un sistema informatico, il cracker concentra le sue forze sul danneggiamento del sistema informatico sia a livello software sia, quando possibile, a livello hardware.

Dopo aver illustrato alcuni concetti base relativi al tema principale dello spionaggio informatico,andiamo ad illustrare la diffusione e la nascita di tale fenomeno.

DIFFUSIONE

Lo spionaggio è la pratica per ottenere segreti,solitamente da rivali o nemici,per ottenere vantaggi militari, politici od economici,attraverso opportune operazioni segrete.

Lo spionaggio ha avuto una grande evoluzione nella storia e soprattutto nel XX secolo,causa la necessità di ottenere informazioni nemiche durante il periodo della guerra. Infatti durante la prima e la seconda guerra mondiale si possono individuare molti movimenti e organizzazioni di spionaggio che furono fondamentali per il conflitto che si stava fronteggiando. Un esempio molto importante fu quello relativo al codice Zimmermann, nell'ottica dell'entrata in guerra degli USA.

Invece durante il secondo conflitto mondiale si può vedere l'evoluzione dello spionaggio si possono vedere i primi "spionaggi tecnologici" che avranno un ruolo importante nell'era bipolare. E infatti è proprio nel periodo della guerra fredda che troviamo una grande opera di

spionaggio soprattutto da parte dei sovietici che riuscirono ad entrare in possesso della documentazione dei laboratori americani nucleari. Durante lo scontro tra le due potenze,USA e URSS, l'attività di spionaggio giocò un ruolo fondamentale,poiché portò entrambe le nazioni ad una corsa agli armamenti sempre più frenetica,esempio più eclatante quello relativo alla bomba H.

Dopo aver illustrato l'evoluzione spionistica durante i conflitti che hanno caratterizzato gli anni del 900',portiamo avanti il discorso fino ad arrivare ai primi anni '90. Infatti è proprio in questi anni che si può vedere la nascita dello "spionaggio informatico" in concomitanza con l'evoluzione di ***Internet****.

Qui di seguito viene illustrata la cartina mondiale della cosiddetta "cyber-guerra fredda"; dove si notano i tre principali stati in corsa per gli armamenti :

Si possono delineare di anno in anno ed ormai di mese in mese i trend delle minacce informatiche. L'attenzione dei cyber-criminali si è spostata dal furto di informazioni personali alla sottrazione di capitale intellettuale di aziende e organizzazioni internazionali.

Gli illeciti posti in essere dalla criminalità organizzata non sono sostanzialmente cambiati nel corso del tempo: essi si sono adattati in risposta a più ampi cambiamenti sociali e tecnologici e alle opportunità che le moderne applicazioni informatiche hanno introdotto nella gestione di attività quotidiane. Da recente studio, i cyber-crimini differiscono dai crimini più comuni in quattro modi:

1. sono più facili da porre in essere.
2. richiedono poche risorse rispetto al potenziale profitto o danno causato.

3. possono essere commessi in una giurisdizione senza essere fisicamente presenti in essa.
4. spesso non sono chiaramente illegali.

Il cyber-spionaggio da parte di attori statali è estremamente difficile da distinguere dal cyber-spionaggio da parte di individui o gruppi. Le tecniche di attacco possono essere molto simili. La differenza principale è la motivazione alla base dell' intrusione,che è più probabile che sia di matrice politica o economica.

La cyber-criminalità ha assunto i contorni di una vera e propria ***economia sommersa****, globalizzata ed efficiente, dove beni sottratti illegalmente e servizi fraudolenti vengono venduti e acquistati e dove il giro d'affari stimato è misurabile in milioni di dollari.

L'economia sommersa legata alla cyber-criminalità ha spostato di recente l'attenzione sul furto di capitale intellettuale aziendale. Il capitale intellettuale comprende tutto il valore derivante dalla proprietà intellettuale di una società, in particolare segreti commerciali, copyright, formule proprietarie, piani di marketing, risultati di ricerca e sviluppo e anche codici sorgente.

Si può analizzare un esempio di queste attività criminali,ovvero l'Operazione Aurora. Questa operazione offensiva mirata su Google ed almeno 30 altre società, ha rappresentato un attacco sofisticato progettato per rubare capitale intellettuale. Secondo Google l'attacco avrebbe avuto origine in Cina, sfruttando le falle nella sicurezza degli allegati di posta elettronica, al fine di introdursi nelle reti interne di grandi corporate finanziarie e di difesa, in quello che è stato definito "parte di uno sforzo concertato di spionaggio politico e aziendale".

Altri attacchi di maggiore importanza sono stati attribuiti all'**Anonymous**. L'Anonymous è un fenomeno di Internet che rappresenta l'insieme delle attività, intraprese da una singola persona o gruppi di persone,volte a raggiungere uno scopo comune. Oltre ad essere considerato come un nuovo fenomeno del Web,esso è visto anche come un vero e proprio movimento hacker che ha l'obiettivo di organizzare proteste politico-economiche al fine di raggirare il sistema. Anonymous è composto in gran parte da utenti provenienti da diverse ***imageboard**** e ***forum****. Questi utenti si incontrano in rete su molti siti e social network,quali face book e twitter,per aiutare le persone a mettersi in movimento con le proteste nel mondo reale. Anonymous non ha leader o partiti che lo controllano, si basa sul potere collettivo dei suoi partecipanti che agiscono individualmente in modo che l'effetto della rete benefici il gruppo.

Il simbolo del "busto senza capo" rappresenta l'organizzazione senza leader e l'anonimato.

La maschera di Anonymous rappresenta la sua firma sulle operazioni completate

« Noi siamo Anonymous. Noi siamo legione. Noi non perdoniamo. Noi non dimentichiamo. Aspettateci! **».** Il motto di questa organizzazione dice tutto si chi ne fa parte e sulle attività che intraprende. Dal 2006 ad oggi sono molte le operazioni di spionaggio in rete,con conseguenti arresti,attribuite ad Anonymous. La nascita di questo movimento rappresenta ormai una completa rivoluzione ed evoluzione del sistema politico-economico.

L'espansione del crimine informatico su scala mondiale mette a repentaglio la sicurezza di individui, aziende, e nazioni in modo costante e se la seconda guerra mondiale fu denominata ***guerra totale****,negli anni successivi si assisterà alla "cyber-guerra totale".

OPERAZIONI E ATTACCHI

In questa fase andremo a spiegare le tipologie di attacco legate alla "guerra informatica".

La **guerra informatica**,dall'inglese hacker warfare,è quell'attività rientrante nelle operazioni di ***information warfare**** che utilizza hacker informatici per colpire la rete informatica avversaria.

Con la cyber-warfare si analizza un nuovo riassetto delle concezioni organizzative militari. Le tradizionali strutture gerarchiche si vedono progressivamente sopraffatte da sistemi a rete. Si fanno così spazio entità operative caratterizzate da:

- ridotta consistenza numerica;

- elevato livello di supporto tecnologico;
- efficacia assoluta.

Le regole base di questa guerra sono :

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno tecnologie che agevolino le attività investigative e l'acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;
- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico (IFF - "Identification Friend or Foe").

In questo conflitto è solito arruolare,come nuovi mercenari,hacker capaci di aggredire un sistema informativo protetto, orientandosi in complessi sistemi informatici e telematici.

Gli attacchi legati a questa metodologia di guerra sono di 3 tipi :

1. Attacchi ai sistemi.
2. Attacchi alle informazioni.
3. Attacchi alle reti.

- Gli **attacchi al sistema** danneggiano il sistema operativo di un computer. Sono relativi alla paralisi totale degli elaboratori o semplici malfunzionamenti;modifiche al software di base;danneggiamento di programmi applicativi; interruzione di assistenza e manutenzione.

- Gli **attacchi alle informazioni** hanno l'obiettivo di determinare quali computer ed apparati di rete siano attivi, raccogliendo informazioni. In seguito, attraverso altri programmi che sfruttano queste vulnerabilità, si entra di forza nei sistemi bersaglio e li si manipola per prenderne il controllo completo; ad esempio si può giungere ad acquisire i privilegi di amministratore o decifrare le password degli utilizzatori. Come in ogni attività illegale, si cerca poi di coprire le tracce informatiche inevitabilmente lasciate da questa attività

intrusiva. Quindi spesso questo tipo di attacchi sono legati ad operazioni di cancellazione e modifica dei database; inserimento indebito dei dati;furto di elementi di conoscenza.

- Gli **attacchi alla rete** hanno il compito di "infettare" la rete Internet attraverso varie operazioni : 1) blocco del traffico dei dati. 2) distruzione di siti famosi. 3) intercettazione delle comunicazioni non autorizzate. 4) inserimento di comunicazioni indebite per disturbare il traffico. 5) propaganda di messaggi politici che possono essere inviati ai residenti di una rete.

La diffusione di questo genere di attacchi sta dilagando in tutto il mondo in quest'ultimo decennio, ne ricordiamo due rimasti nella storia con i nomi di Titan Rain e Moonlight Maze. Intanto negli ultimi anni gli Stati Uniti d'America hanno ammesso di essere stati sotto attacco da parte di diversi Stati, ad esempio Cina e Russia.

Notizia rilevante,in merito all'argomento,è sicuramente quella inerente al più grande attacco informatico mai dichiarato nella storia di internet, proveniente dall'azienda olandese Cyberbunker. Dalla sua sede, in un bunker dismesso della Nato nei Paesi Bassi, Cyberbunker ha fatto partire un'operazione di ***distributed denial-of-service (DDoS)****, che invia traffico anomalo verso i server di Spamhaus, un'organizzazione non profit con sede a Ginevra.

CAUSE E CONSEGUENZE

Come già illustrato in precedenza,gli Stati Uniti D'America hanno ammesso pubblicamente di essere stati attaccati da Russia e Cina,e sull'argomento ci sono molte questioni ancora da definire. Ad esempio le cause che hanno portato le tre potenze economiche del mondo ad alimentare questi cyber-attacchi, iniziando una vera e propria "guerra dell'informazione",già definita in precedenza.

Le cause principali della cyber guerra sono molteplici, dalle proteste di stampo politico e sociale a sfide rivolte al potere di certe infrastrutture che detengono gran quantità di dati di interesse pubblico; da gruppi organizzati che rivendicano le proprie iniziative secondo obiettivi dichiarati,come ad esempio gli Anonymous,a singoli pirati che si "divertono" ad aggirare il sistema e a scovare eventuali falle nella sicurezza informatica di certe infrastrutture.

A volte queste cause sono collegate a eventi specifici, come le elezioni; altre volte, invece, non esistono cause apparenti, se non il semplice intento di silenziare le opinioni e la libertà di espressione.

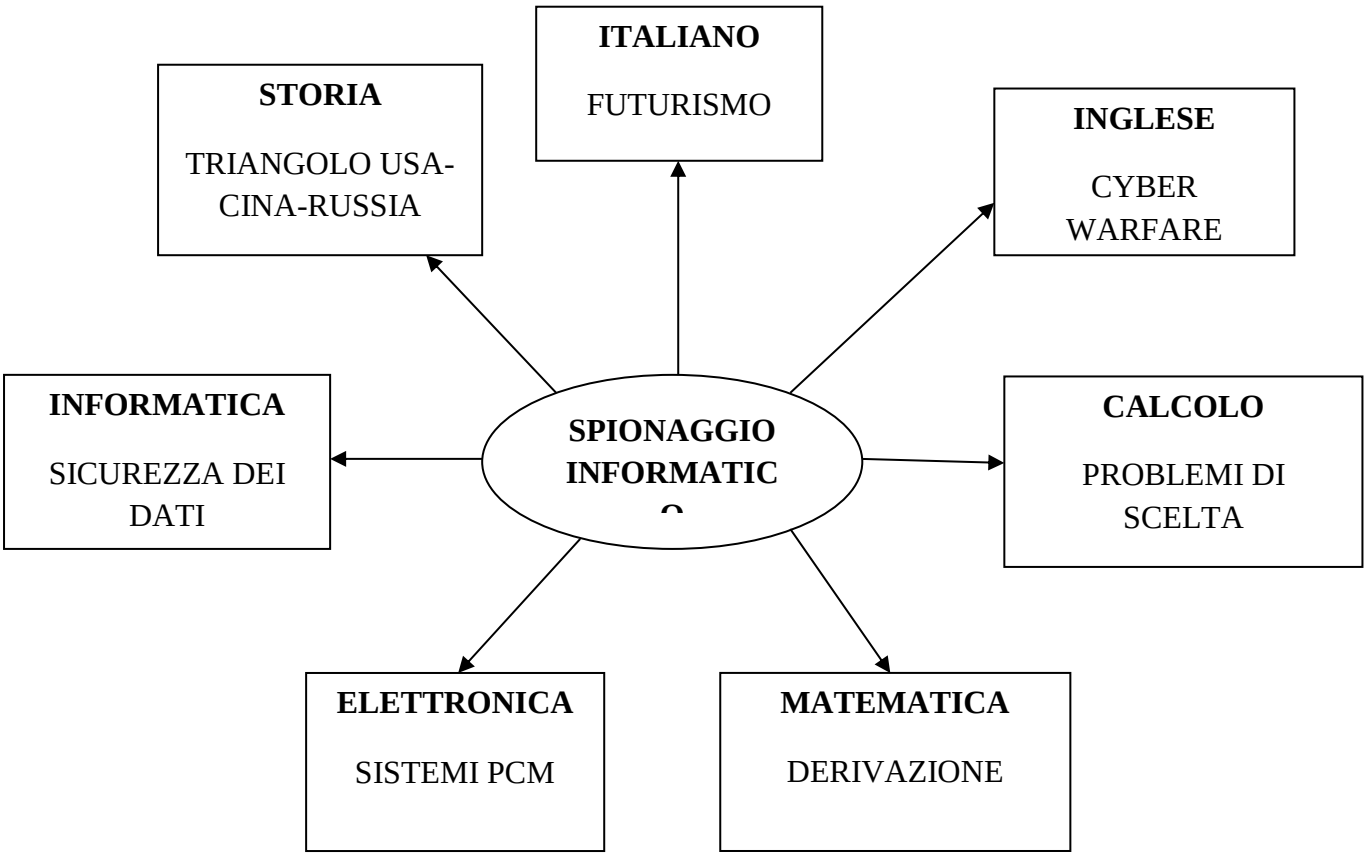
Quindi si può definire questa nuova guerra come strumento per stabilizzare il monopolio dell'economia mondiale,visti gli attacchi ai danni degli U.S.A., e per organizzare proteste politiche anonime.

SPIEGAZIONE

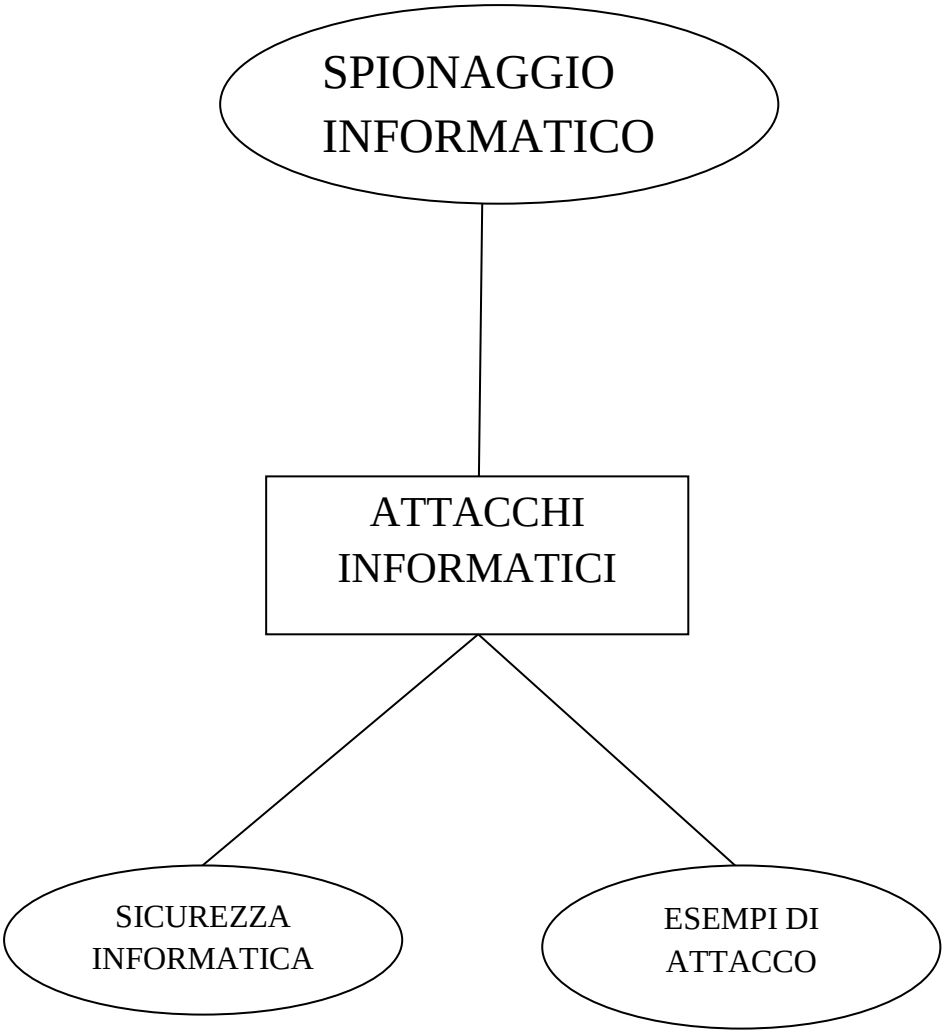
Dopo l'introduzione iniziale,dove veniva spiegata la nascita,la diffusione e la struttura dello spionaggio,si passa alla fase di spiegazione del percorso interdisciplinare intrapreso;strutturato in tre passi principali:

1) Mappa concettuale con i collegamenti nelle varie discipline intraprese.
2) Spiegazione dei collegamenti tra le materie scolastiche e l'argomento principale della tesi.
3) Introduzione alla suddetta materia.

MAPPA CONCETTUALE



INFORMATICA



In questa fase iniziale possiamo vedere come la sicurezza di un sistema occupi un parte molto importante quando si parla di spionaggio informatico e attacchi in rete. Gli argomenti che andremo ad affrontare riguardano soprattutto la sicurezza a livello informatico,come viene gestita attualmente e anche come viene violata.

SICUREZZA INFORMATICA

Per sicurezza si intende quella parte dell'informatica che si occupa delle minacce,degli attacchi e della protezione di un sistema informatico e dei dati in esso memorizzati. Al giorno d'oggi la questione sicurezza è diventata sempre più pressante in materia causa la diffusione a livello planetario di nuovi apparati tecnologici e la continua evoluzione degli attacchi hacker. Sulla base di questa definizione si possono distinguere due tipi di sicurezza : **attiva** e **passiva**.

1. La **sicurezza attiva** si occupa della protezione dei dati all'interno di un sistema,sia da eventuali accessi non autorizzati;sia dalle possibili modifiche non autorizzate.
2. La **sicurezza passiva** si occupa della difesa del sistema da utenti non autorizzati che possono accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Questo concetto è molto generale,basti pensare all'uso di porte blindate insieme a sistemi di riconoscimento vocale in molte aziende;questo esempio è da considerarsi strumento di sicurezza passiva.

E' chiaro che i due concetti di sicurezza appena espressi sono integrati tra loro poiché sono indispensabili per il mantenimento della protezione desiderata e anche perché le tipologie di attacco che un sistema può subire sono molte e quindi è necessario il supporto di tali strumenti.

I principali parametri di protezione del dato sono : disponibilità,integrità e riservatezza.

1. La Disponibilità misura la prontezza di un sistema nello svolgere determinate funzioni sotto condizioni pre-stabilite.
2. L'Integrità del dato si occupa di garantire la sua protezione da eventi **accidentali** o **indesiderati**.
3. La Riservatezza si occupa della protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti.

Parlando di integrità abbiamo introdotto le 2 principali cause di perdita di un dato ovvero gli eventi accidentali e quelli indesiderati.

Tra gli eventi accidentali troviamo gli attacchi hacking, condotti da utenti chiamati "hacker" che tramite l'uso di software particolari entrano all'interno del sistema, riuscendo ad ottenere piena disponibilità della macchina, per gestire risorse e dati senza avere i giusti requisiti richiesti; e l'accesso non autorizzato al sistema,che può sembrare simile al precedente ma che si distingue dal fatto di non utilizzare la rete per l'accesso al sistema.

Dopo aver introdotto la sicurezza andiamo ad analizzare le principali tecniche di difesa di un sistema.

GESTIONE DEGLI ATTACCHI

La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e di controllo degli accessi; anche se questo fatto fa parte della sicurezza normale e non della "sicurezza informatica".

Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema.

Per evitare invece gli eventi accidentali, non esistono soluzioni generali, ma di solito è buon senso dell'utente fare una copia di backup del sistema.

Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare. La sicurezza informatica si occupa anche di prevenire eventuali situazioni di Denial of service (DoS). I DoS sono attacchi sferrati al sistema con l'obiettivo di renderne inutilizzabili alcune risorse in modo da danneggiare gli utenti del sistema. Per prevenire le violazioni si utilizzano strumenti hardware e software. I principali strumenti utilizzati per mantenere la sicurezza sono : Antivirus, Backup, Sistema di autenticazione e Firewall.

1) L'**Antivirus** consente di proteggere il computer da file dannosi,o virus. Un buon antivirus deve essere continuamente aggiornato e mandato in esecuzione.

2) Il **Backup** è un sistema per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell'esecuzione di una copia di sicurezza dei dati di un computer per evitare che vadano perduti o diventino illeggibili.

3) Il **Firewall** garantisce un controllo sugli accessi al sistema e del traffico che lo attraversa. Protegge il sistema da attacchi esterni.

4) Un **Sistema di autenticazione** è utile soprattutto nelle aziende per verificare l'autentica autorizzazione di un utente per l'accesso al sistema. Come detto in precedenza è un componente di sicurezza passiva, ed oltre all'autenticazione tramite password di un utente si è passati alla verifica dell'impronta digitale o alla verifica vocale.

ESEMPI DI ATTACCO

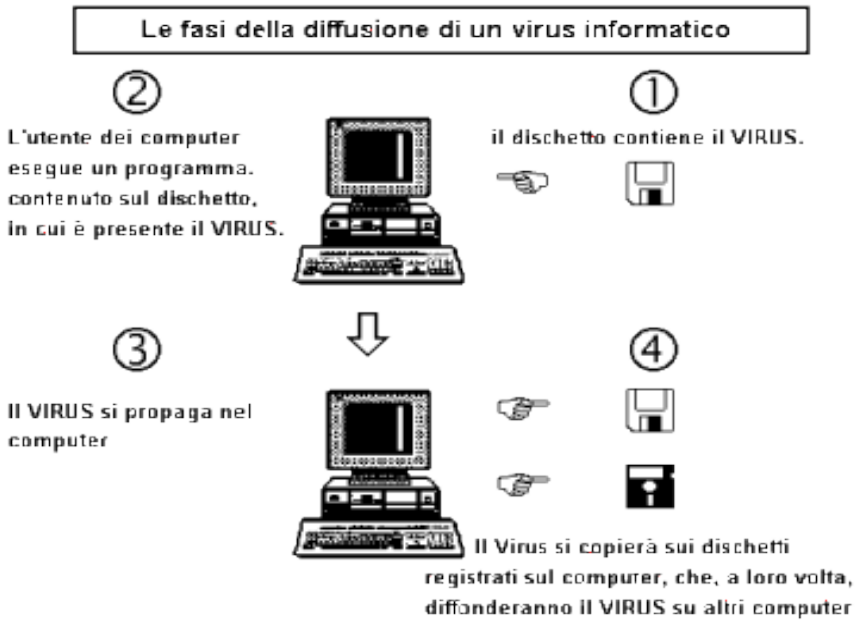
1) **Keylogger** : E' uno strumento che intercetta tutto ciò che un utente digita sulla tastiera del proprio, o di un altro computer. Ci sono due tipi di Keylogger : Hardware e Software.

   Hardware : vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera.

   Software : programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

   Si può utilizzare un firewall hardware o software per intercettare la connessione del processo.

2) **Virus** : E' un software, appartenente alla categoria dei ***malware****, che è in grado di infettare dei file in modo da riprodursi facendo copie di se stesso senza farsi rilevare dall'utente. Qui di seguito è riportato lo schema di diffusione di un virus informatico :

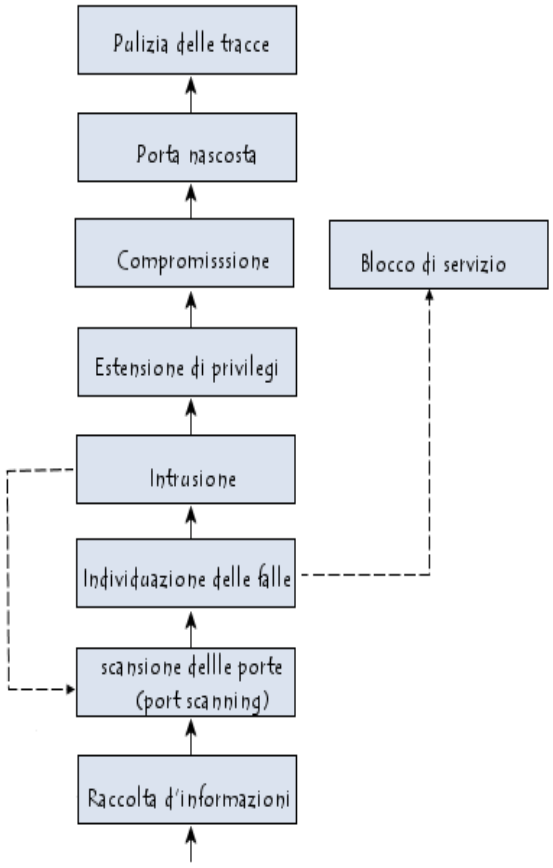


3) **Ingegneria sociale** : E' lo studio del comportamento individuale di una persona al fine di estorcere informazioni utili. Il *social engineer* comincia con il raccogliere informazioni sulla vittima per poi arrivare all'attacco vero e proprio. Durante la prima fase l'ingegnere cercherà di ricavare tutte le informazioni di cui necessita sul suo bersaglio. Superata questa fase, detta *footprinting*, l'ingegnere passerà alla fase successiva, cioè quella che gli permetterà di verificare se le informazioni che ha ricavato sono più o meno attendibili. La fase più importante, è lo studio dello stile vocale della persona per la quale vuole spacciarsi. In questa fase l'attaccante avrà sempre vicino a sé i propri appunti con tutte le informazioni raccolte nella fase di *footprinting*, dimostrandosi pertanto sicuro nel caso gli venisse posta qualche domanda.

CAPITOLO 4 : INFORMATICA

Qui di seguito è riportato uno schema che rappresenta le fasi che determinano la procedura di un attacco informatico.

SPIEGAZIONE DELLE FASI



1. Raccolta delle informazioni : Questa fase consiste nel mettere insieme il massimo di informazioni possibili riguardanti le infrastrutture di comunicazione della rete oggetto dell'attacco.
2. Scansione delle porte : Tecnica con lo scopo di prelevare informazioni da un computer connesso ad una rete,stabilendo quali porte siano in ascolto.
3. Localizzazione delle falle : Una volta completata la scansione, l'attaccante deve determinare se ci sono delle falle nel sistema di sicurezza così da poter bloccare i servizi attivi sulla rete.
4. Intrusione : Dopo aver schematizzato una mappa di attacco,l'**hacker** può procedere all'intrusione vera e propria. Per introdursi nella rete gli attaccanti fanno ricorso a diversi metodi tra cui l'**ingegneria sociale**.
5. Estensione dei privilegi : L'hacker cerca di ottenere l'accesso root per ottenere nuovi privilegi. Gli è quindi possibile installare uno ***sniffer****. Grazie a questa tecnica, il pirata può sperare di recuperare le coppie *login/password* che gli permettono di accedere agli account con dei privilegi estesi.
6. Compromissione : Questa tecnica d'usurpazione d'identità, chiamata **spoofing**, permette al pirata di penetrare delle reti privilegiate alle quali il terminale compromesso ha accesso.
7. Porta nascosta : Una volta compromesso un terminale,l'attaccante può voler tornare sulla scena del crimine; A questo scopo installerà un'applicazione per creare artificialmente una falla di sicurezza, si parla quindi di **backdoor.**
8. Pulizia delle tracce : Quando l'intruso ha raggiunto un livello di conoscenza sufficiente della rete, non gli resta che cancellare le tracce del suo passaggio eliminando i file che ha creato e pulendo i file di log dei terminali nei quali si è introdotto.

SQL INJECTION

Un'altro esempio di attacco informatico è l'**SQL injection.** Gli attacchi SQL injection sono degli attacchi verso i siti web che si appoggiano su database relazionali.
In questo tipo di siti, alcuni parametri sono passati al database sotto forma di una query SQL. In questo modo, se il webmaster non ha effettuato nessun controllo sui parametri passati nella query SQL, sarà possibile per un pirata modificare la query per accedere alla totalità del database, fino a modificarne il contenuto.
In effetti, alcuni caratteri permettono di scatenare numerose query SQL oppure di ignorare il seguito della query. Così, inserendo questo tipo di caratteri nella query, un pirata può potenzialmente eseguire la query da lui scelta.
Prendiamo ad esempio la query seguente, aspettando come parametro un nome utente :

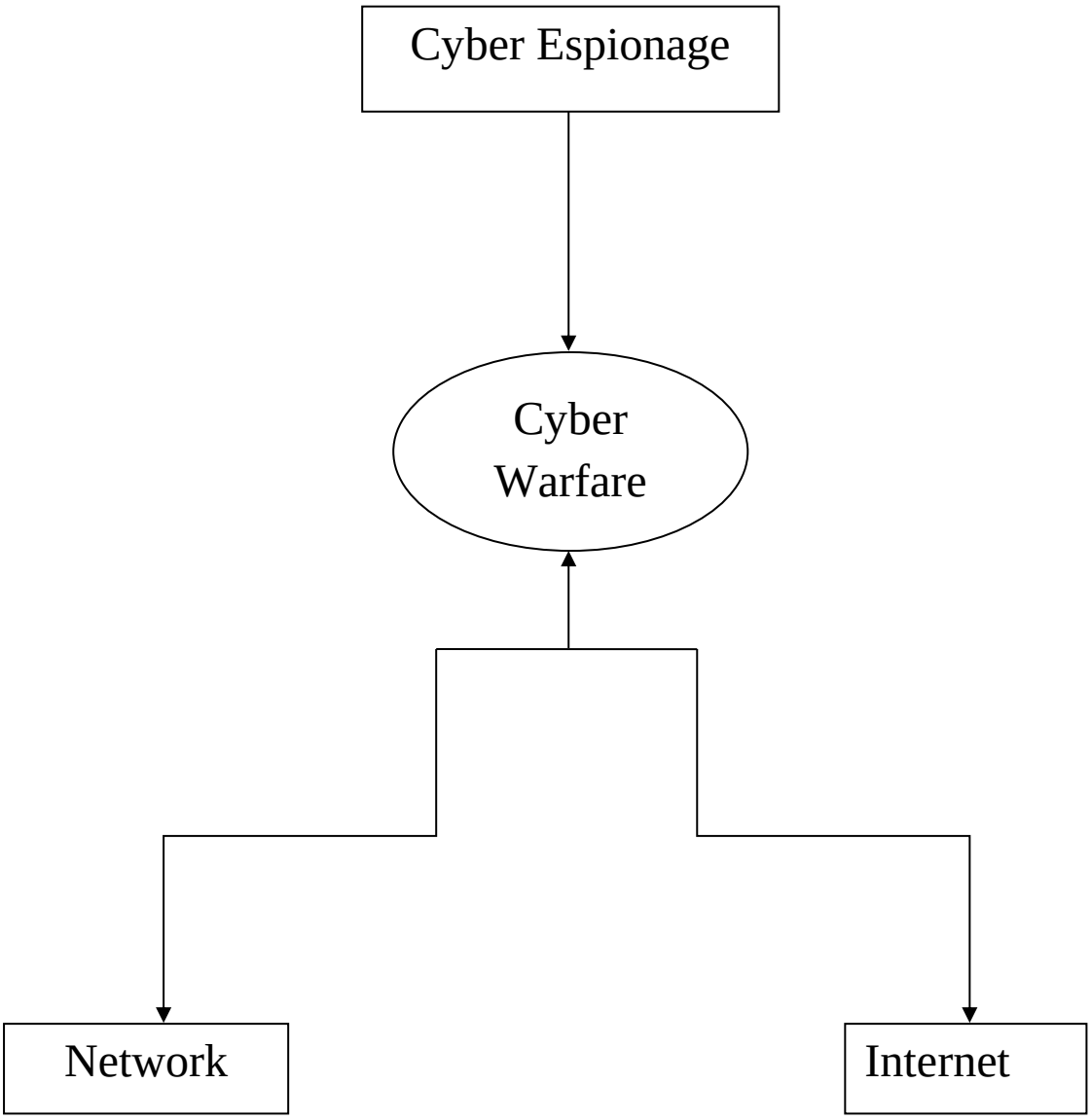
```
SELECT *
FROM  utenti
WHERE  nome="$nome";
```

Ad un pirata basterà inserire un nome come "poppo" OR 1=1 OR nome ="pippi" e la query cambia come segue :

```
SELECT *
FROM utenti
WHERE nome="poppo" OR 1=1 OR nome ="pippi";
```

In questo modo, con la query qui sopra, la clausola WHERE è sempre rispettata, il che significa che girerà le registrazioni corrispondenti a tutti gli utenti.

INGLESE



In this part of the thesis, we are going to deepen the discussion of the cyber-warfare and we are going to introduce networks and Internet, because they have an important role in the cyber-warfare.

CYBER-WARFARE

Cyber-Warfare is an activity which use computer hackers to hit the computer network half; it is a form of information warfare. It refers to politically motivated hacking, to conduct sabotage and espionage. Cyber-Warfare attacks can disable official websites and networks, disrupt essential services, steal or alter classified data. The most effective protection against cyber-warfare attacks is securing the security of information and **networks**.

Cyber-Warfare is characterized by the use of electronic technology, computer and telecommunication systems. It is a new form of terrorism but it is fought on the Internet. Computer hacking represents a modern threat in ongoing industrial espionage and as such is presumed to widely occur. In recent years, cyber warfare has become an issue of much concern among the major nations on the planet, and virtually every national military now has a branch dedicated to both conducting and defending against cyber warfare. So as the world becomes more networked, systems become susceptible to attacks in cyberspace. Although certain military systems remain accessible only by being present at a terminal on site, the vast majority of critical systems that control modern nations are now tied into the **Internet** in some way or another. While these systems are defended by high levels of security, they are breakable, and cyber warfare concerns itself with finding weaknesses and exploiting them. Many critical military systems are also susceptible to virtual attacks. The **Satellite systems**, for example, although protected by extensive level of security, have been breached. If an enemy were to take control of spy satellites or satellites which feed GPS data to aircraft and missiles, it could be a major blow to the military.

There are three sectors targeted by nations involved in cyber warfare: financial, infrastructures, and governmental. Financial attacks could disrupt the world's major markets by taking electronically-controlled of the economy, or by shutting down web-based operations of banks or retailers. Infrastructure attacks can damage a nation by shutting down critical utility systems, such as electrical grids, or interfering with the air traffic control system. Governmental attacks can turn off the communication between two officials governments, steal secret communications, social security information, or other personal data to the public.

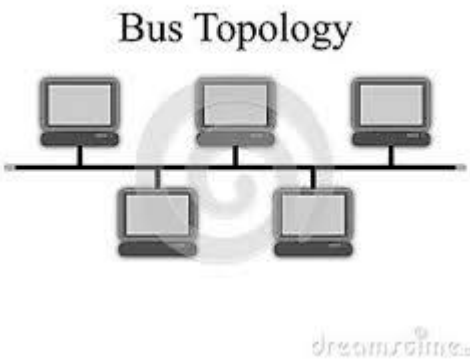
So this "new war" has brought new forms of technology and a new threat to fight, which is expanding worldwide with an unstoppable force.

Until now we have talked about cyber-warfare and its applications, but now we will do a brief introduction about two main elements that characterize this phenomenon : Network and Internet.

NETWORK

Network is a collection of computers and other devices linked either by physical or wireless means. A network can be made up of many computers across the world. They don't necessarily need to reside in the same room or in the same city but they must have a ***NIC****. A user, which take a part in a network, can share information with another user on the other side of the world. So a network increase the economy because a worker can share information without printing, copying, phoning or posting.

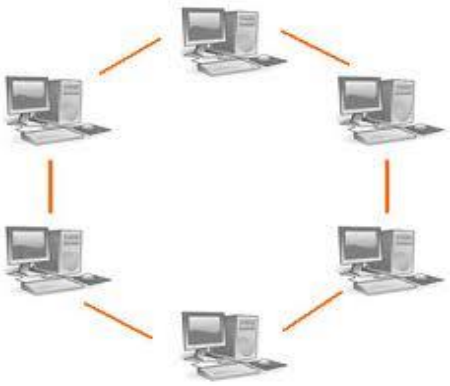
The structure of a network refers to its topology, which refers to the way that computers arranged in a network. There are 3 types of computer network topologies: **BUS**,**RING** and **STAR**.



EXPLANATION

The terminals are connected one to another along a common cable. A signal can be transmitted to all nodes, but only the destination node responds. This type of topology is cheap and reliable.

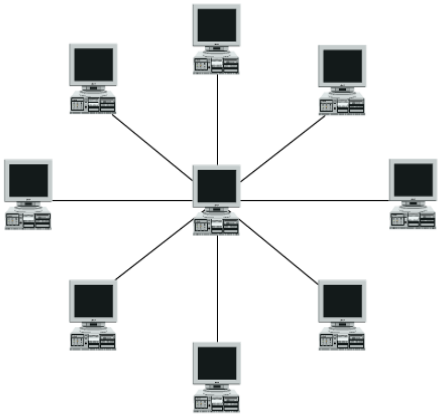
Ring Topology



EXPLANATION

It consist of a circular arrangement where all the computers are connected one to another. If a part fail, all the nodes will be affected. It can cover long distance but is difficult to set up and it is expansive.

Star Topology



EXPLANATION

It consist of a central host computer that are connected all the others nodes. A computer communicate with one another through the central host. This topology use more cabling than the others and it is more expansive.

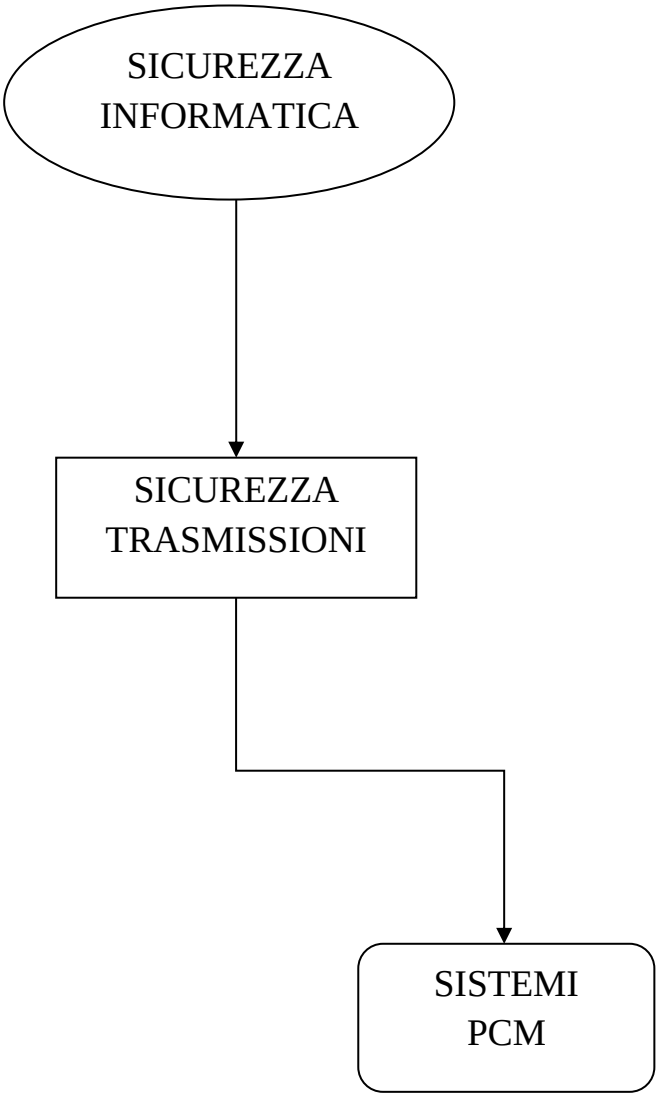
DEEPING : INTERNET

Internet is the world's biggest network. It is made up of millions computers and contain information about all the world. When you connect the Internet, you have access to an infinite numbers of information that all the computers shared. These computers, for the communication with each other, use a language called **IP**.

This communication provide a send of information. This process is complex and structured. The data is send in small packets and then a set of hardware process and routes them to their destination:

1. **HUBS** link set of computer to one another.
2. **BRIDGES** is a combination of hardware and software that link LANs with one another using the same protocol.
3. **GATEWAYS** are devices similar to bridges but convert data from one type of network to another; so they combine different type of networks.
4. **REPETEARS** amplify the data so that the signal doesn't weaken.
5. **ROUTERS** routes the data in the best way to reach destination.

ELETTRONICA

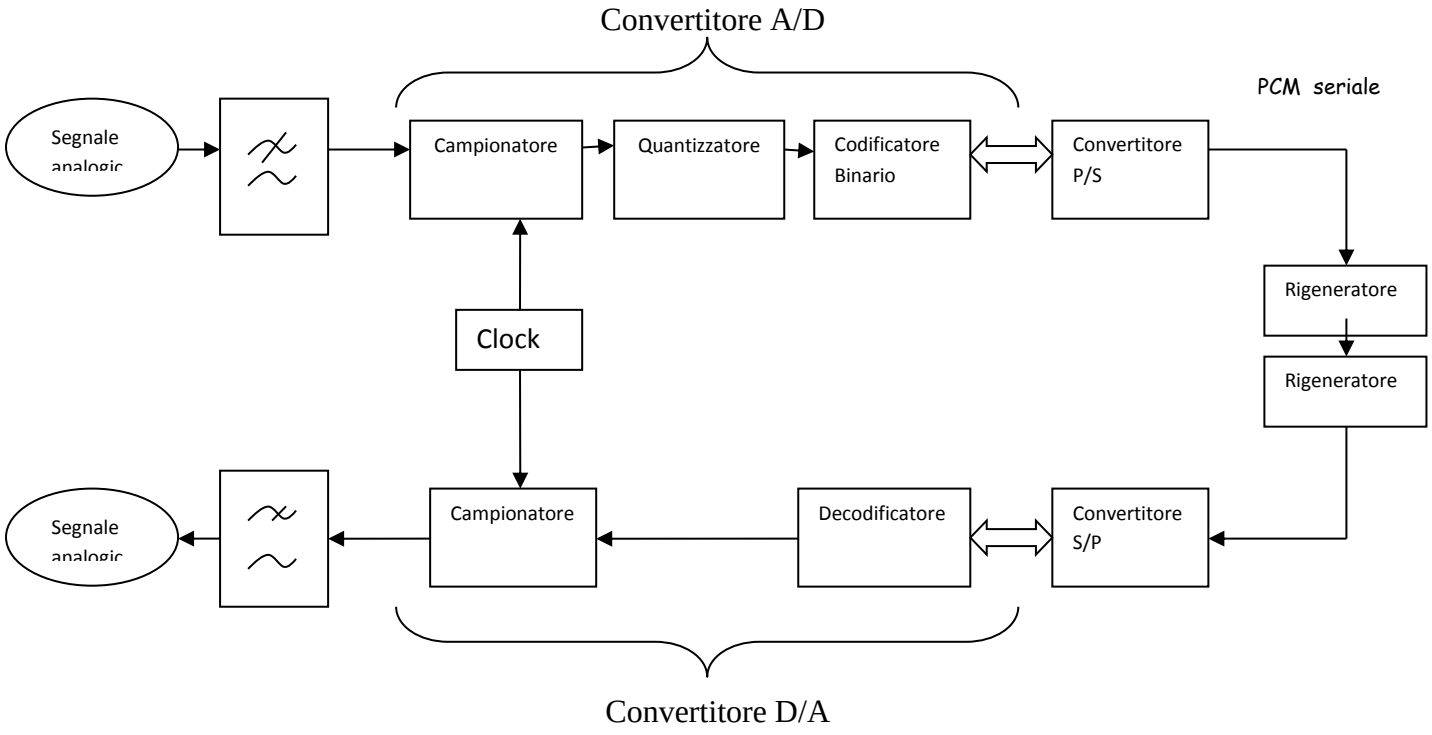


Un'altra parte della sicurezza informatica si occupa delle problematiche connesse alla trasmissione di informazioni in rete o su un sistema di telecomunicazioni ovvero alla protezione dei dati in transito e sugli accessi non autorizzati risorse e servizi di rete. In questa parte della tesi andremo a descrivere un sistema PCM,utilizzato per la trasmissione di segnali digitali.

SISTEMI PCM

PCM,acronimo di Pulse Code Modulation,ovvero modulazione di impulsi codificati,è un metodo di rappresentazione digitale di un segnale analogico. L'informazione viene prima campionata in intervalli di tempo regolari prelevando campioni di frequenza,e poi viene quantizzata approssimando i campioni appena prelevati con valori più accettabili rispetto ai livelli di quantizzazione. Il segnale viene trasmesso attraverso gli impulsi della portante in forma binaria;questa operazione rappresenta la codifica del segnale. Il segnale,difatti,è digitale poiché presenta una sequenza di due livelli che rappresentano le cifre 1 e 0 del sistema binario.

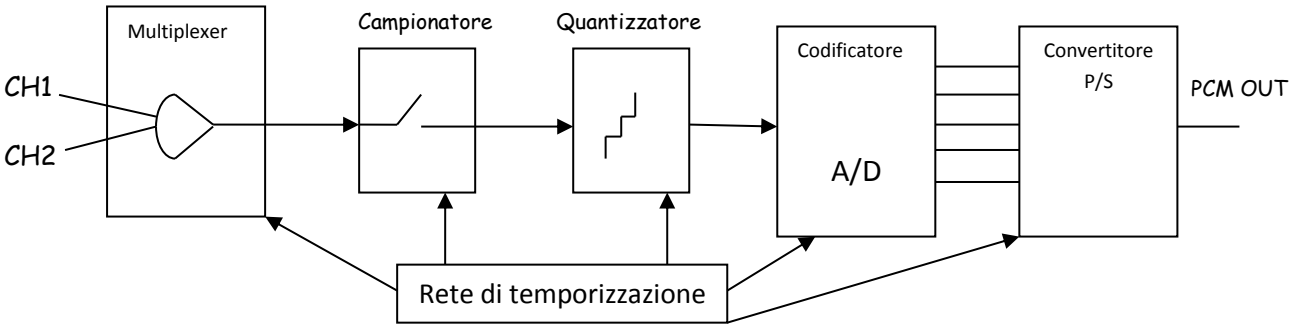
STRUTTURA SISTEMA PCM



1) **Convertitore A/D**: E' composto dall'insieme campionatore - quantizzatore - codificatore,e trasforma il segnale analogico in un segnale numerico.
2) **Convertitore P/S:** Effettua la serializzazione dei bit in uscita rendendo possibile il loro invio sul canale.
3) **Rigeneratore:** La presenza dei rigeneratori serve a mantenere stabile il rapporto S/N,quando i collegamenti sono molto lunghi.
4) **Convertitore D/A:** Composto dal decodificatore e dal campionatore;serve a produrre in uscita un segnale ***PAM**** quantizzato,per poi essere ricostruito dal filtro passa - basso (ordine superiore 7°/8°).

MODULATORE PCM

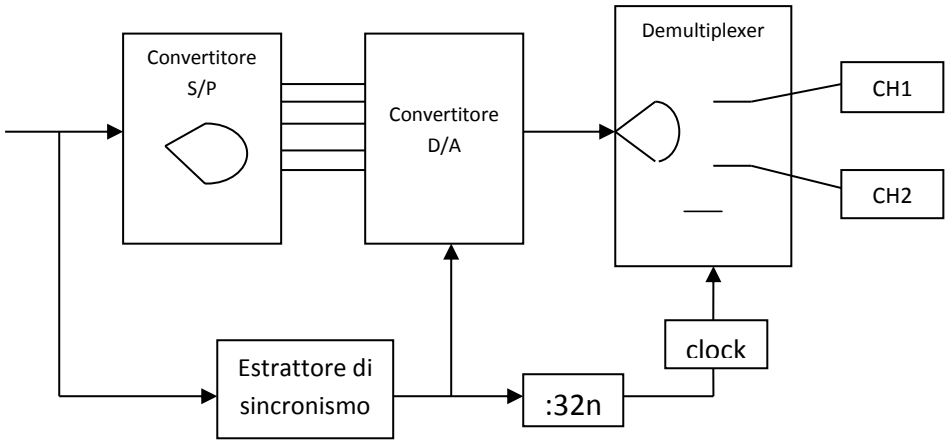
STRUTTURA



1) **Campionatore:** Il segnale viene campionato con una frequenza di campionamento f_c,generata da un clock. I valori dei campioni vengono memorizzati per rendere possibili le operazioni successive.
2) **Quantizzatore:** Rende il numero infinito di ampiezze in un numero finito di livelli codificabili.
3) **Codificatore:** Associa ad ogni livello qu~~ant~~izzato un codice binario.

Le 3 operazioni devono essere temporizzate tramite una rete di temporizzazione,poiché il modulatore PCM è digitale ed il suddetto funzionamento dipende dal clock,e perché i circuiti di trasmissione devono essere sincronizzati con quelli di ricezione per l'interpretazione.

DEMODULATORE PCM



1) **Convertitore S/P:** riceve il segnale PCM e converte gli impulsi in una stringa binaria di 8 bit.
2) **Convertitore D/A:** Restituisce il segnale quantizzato ad m livelli ed il campionatore ricampiona il segnale per ottenere il segnale PAM.
3) **Filtro passa - basso:** Ricostruisce il segnale PAM originale.

PARAMETRI

1. **Relazione tra la banda di frequenza del segnale da trasmettere e la banda di frequenza** del segnale numerico : $B_{PCM} = n \cdot B_f$.

   Da questa relazione si può notare che per un segnale PCM la banda minima richiesta è pari a n volte la banda del segnale originario. Viene utilizzato l'impulso a coseno rialzato che ha un andamento con ***fattore di roll-off**** pari a 0,5,provocando un allargamento della banda che si calcolerà con la seguente formula : $B_{PCM} = (1 + 0{,}5) \cdot n \cdot B_f = \frac{3}{2} \cdot n \cdot B_f$.

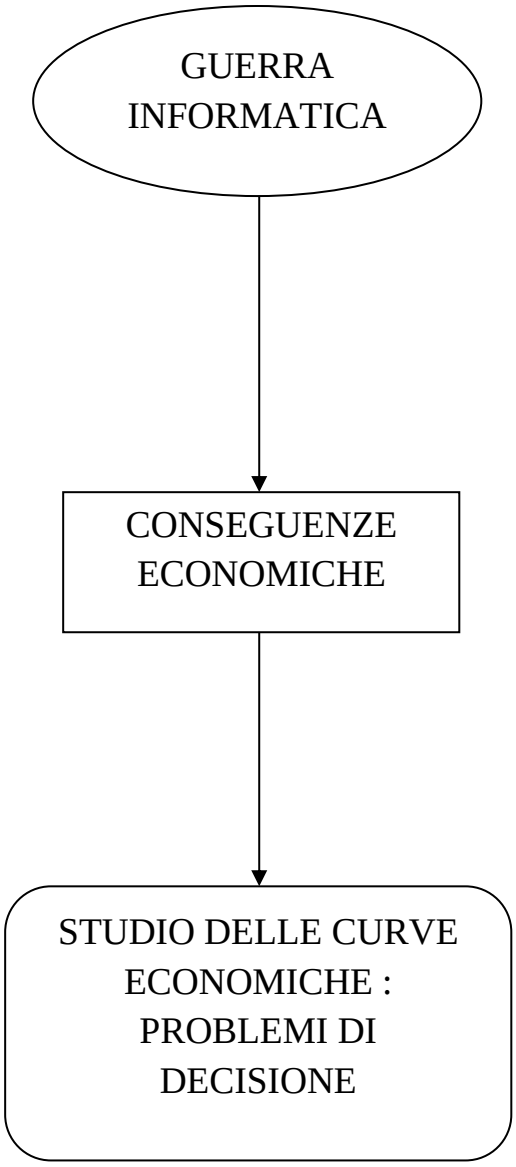
   Si può osservare che il segnale numerico occupa una banda maggiore rispetto a quello analogico,ma questo svantaggio viene compensato dai numerosi vantaggi che offre la trasmissione.
2. **Somma della durata degli n bit**,nei sistemi PCM ad un canale deve rispettare la seguente relazione : $n \cdot \tau \leq \Delta T_c = \frac{1}{f_c}$.

   Facendo riferimento ad un multiplexer telefonico sistema PCM/TDM ad m canali si deve verificare che : $m \cdot n \cdot \tau \leq 125\mu s$.

STORIA

Il motivo principale che portò al campionamento dei segnali era la necessità di far passare su un unico cavo diversi campioni provenienti da diverse fonti telegrafiche. L'ingegnere elettrico W.M. Miner, nel 1903, usò un commutatore elettro-meccanico per la multiplazione a divisione di tempo (TDM) di diversi segnali telegrafici, applicò in seguito questa tecnologia alla telefonia. Ottenne flussi audio intelligibili per canali campionati a 3500–4300 Hz: al di sotto la comunicazione era insoddisfacente. Questa TDM usava canali PAM(pulse-amplitude modulation) e non PCM. L'ingegnere inglese Alec Reeves pensò alla PCM per le comunicazioni vocali nel 1937 mentre lavorava per la International Telephone and Telegraph in Francia. Reeves brevettò questi studi in Francia nel 1938, e nel 1943 negli Stati Uniti. La prima trasmissione di un discorso mediante tecniche digitali fu utilizzata per le comunicazioni di alto livello degli Alleati durante la Seconda guerra mondiale nel 1943. La PCM negli anni cinquanta usava un tubo a raggi catodici con una griglia perforata per la codifica. Come in un oscilloscopio il raggio si muoveva orizzontalmente alla frequenza di campionamento e lo spostamento verticale era controllato dal segnale analogico d'ingresso. La griglia era progettata non per produrre codice binario semplice, bensì ***codice Gray***.

CALCOLO



In questa parte della tesi possiamo vedere come questo nuovo fenomeno del cyber-spionaggio abbia avuto risvolti anche nel settore economico riguardante le imprese. Un'impresa ha l'obiettivo di minimizzare le spese sostenute e di massimizzare il guadagno. Il compito della direzione è quello di coordinare i diversi obiettivi e di prendere decisioni in modo da ottimizzare la funzione economica. Per studiare l'ottimizzazione della funzione guadagno,quindi, andiamo ad esaminare alcuni problemi di decisione che si presentano ai dirigenti di impresa.

PROBLEMI DI DECISIONE

In qualsiasi problema di scelta si effettua una decisione per ottimizzare una funzione economica. La ***R.O.**** permette di individuare la scelta più conveniente tra tutte quelle proposte. La prima suddivisione,tra questi problemi,si può effettuare sulle variabili a cui dipende il problema. Le variabili di un problema di scelta non sono libere di prendere qualunque valore,ma sono condizionate da opportuni vincoli. Questi vincoli fanno si che le variabili possono assumere un insieme di valori detto campo di scelta,che può essere **discreto** (valori delle variabili sono in numero finito) o **continuo** (se i valori delle variabili sono di uno o più intervalli reali).

Un'altra classificazione riguarda le condizioni a cui è posta la scelta,ovvero:

1. **Problemi di scelta in condizioni di certezza** : Se i dati e le conseguenze si possono determinare inizialmente.
2. **Problemi di scelta in condizioni di incertezza** : Se alcuni dati sono variabili aleatorie.

I problemi di scelta si distinguono poi in :

1. **Problemi di scelta con effetti immediati** :Se tra la decisione e la realizzazione scorre un tempo molto breve.
2. **Problemi di scelta con effetti differiti** :Se tra la decisione e la realizzazione scorre un tempo discreto.

Dopo una breve introduzione ai problemi di scelta passiamo allo studio di quelli più semplici,ovvero i **problemi di scelta in condizioni di certezza con effetti immediati**, ossia quando si suppone che tutta la quantità prodotta sia venduta.

PROBLEMI DI SCELTA IN CONDIZIONI DI CERTEZZA

Questo problema consiste nel trovare il massimo o il minimo di una funzione economica oppure nel determinare il più conveniente procedimento tra i vari proposti.

La classificazione avviene attraverso le condizioni in cui si opera la scelta :

1. **Problemi di scelta nel caso continuo.**

La funzione economica è una funzione $y = f(x)$ che può assumere tutti i valori di un intervallo $[a, b]$.Per la risoluzione di tale problema si rappresenta sul piano xy la funzione obiettivo e si determinano il massimo e il minimo assoluto nell'intervallo $[a, b]$.

2. **Problemi di scelta nel caso discreto.**

In questo tipo di problemi si utilizza un metodo,detto criterio marginali stico,basato sullo studio del segno degli incrementi. Se gli incrementi sono positivi la funzione è crescente, e invece se sono negativi è decrescente. Si otterrà un massimo se Δf da positivo diventa negativo e invece si avrà un minimo se Δf da negativo diventerà positivo.

3. **Problemi di scelta fra due o più alternative.**

In questi casi sono presenti due o più funzioni che rappresentano le possibili scelte che l'impresa può effettuare per massimizzare il guadagno. Di solito entro certi limiti si adotterà una scelta,mentre entro altri limiti si opterà per un'altra alternativa,se essa risulterà più conveniente. La risoluzione consiste nel rappresentare graficamente tutte le funzioni obiettivo in un unico piano xy,e valutare le opportune scelte nei limiti imposti.

PROBLEMI DI SCELTA IN CONDIZIONI DI INCERTEZZA

Se parliamo di **problemi di scelta in condizioni di incertezza**,si fa riferimento al verificarsi di eventi aleatori. In questo tipo di problema,prima di applicare un criterio,bisogna calcolare per ogni alternativa i risultati dipendenti dal verificarsi degli eventi aleatori;poi si costruisce la matrice dei risultati. Da questa tabella si può vedere se c'è un'alternativa cui i valori siano migliori degli altri. Solamente dopo questo processo si passa all'applicazione del criterio del ***valor medio****. Questo criterio si applica quando agli eventi designati si può attribuire una distribuzione di probabilità. Bisogna calcolare per ogni alternativa il valor medio dei risultati:

$V_m = \sum_{i=1}^{i=n}(a_i * p_i)$. Si sceglie l'alternativa con valor medio maggiore se si tratta di un guadagno,invece si sceglierà quella con valor medio minore se si opererà su di un costo. Dopo aver calcolato il valor medio di ogni alternativa si passa al calcolo dello scarto quadratico medio : $\sigma(A_i) = \sqrt{\sum_{i=1}^{i=n}[\mathrm{a_i} - \mathrm{Vm_i}] * \mathrm{p_i}}$. Se le due alternative hanno lo stesso valor medio,si sceglie quella con scarto quadratico medio minore. Se le alternative hanno diverso valor medio,si stabilisce il livello massimo di rischio che si è disposti a sopportare,sottoforma di frazione e si confronta con lo scarto quadratico medio :

- Se $\sigma(A_i) \leq \frac{V_m}{n}$ $\Longrightarrow$ si confrontano i valor medi.
- Se $\sigma(A_i) > \frac{V_m}{n}$ $\Longrightarrow$ si scarta questa alternativa perché risulta troppo rischiosa.

Oltre al criterio del valor medio si può utilizzare un altro criterio che a differenza del valor medio,non tiene conto delle valutazioni delle probabilità degli eventi aleatori,tale criterio è detto del **maxmin** o del **minimax**,o anche detto *criterio del pessimista*.

Per trovare il massimo ,si considera per ogni alternativa il valore minimo dei relativi risultati e fra questi minimi si cerca il massimo. Si sceglie il massimo dei minimi.

Al contrario quando si parla di costi,per ogni alternativa si sceglie il risultato maggiore fra tutti i massimi si sceglie il minimo. Si sceglie l'alternativa corrispondente.

ESEMPIO

Per il noleggio di un furgone si può scegliere fra le seguenti 3 tariffe :

a) €0,5 al chilometro più un diritto fisso di €15;
b) €60 fissi per una percorrenza fino a 100km e €0,4 per i chilometri eccedenti;
c) €0,8 al chilometro senza spese fisse.

Determinare l'alternativa più conveniente in funzione dei chilometri da percorrere.

Dati

a) $S_u = €0{,}5/km; S_f = €15.$
b) €60 fino a 100km e €0,4 per i km>100.
c) $S_u = €0{,}8/km.$

Svolgimento

a) $S(x) = 0{,}5x + 15 \qquad y = 0{,}5x + 15$

	x	y
$A \equiv$	$(0$	$15)$
$B \equiv$	$(100$	$65)$

b) $S(x) = 60 + 0{,}4 \cdot (x - 100) \qquad y = 0{,}4x + 20$

	x	y
$C \equiv$	$(0$	$20)$
$D \equiv$	$(100$	$60)$

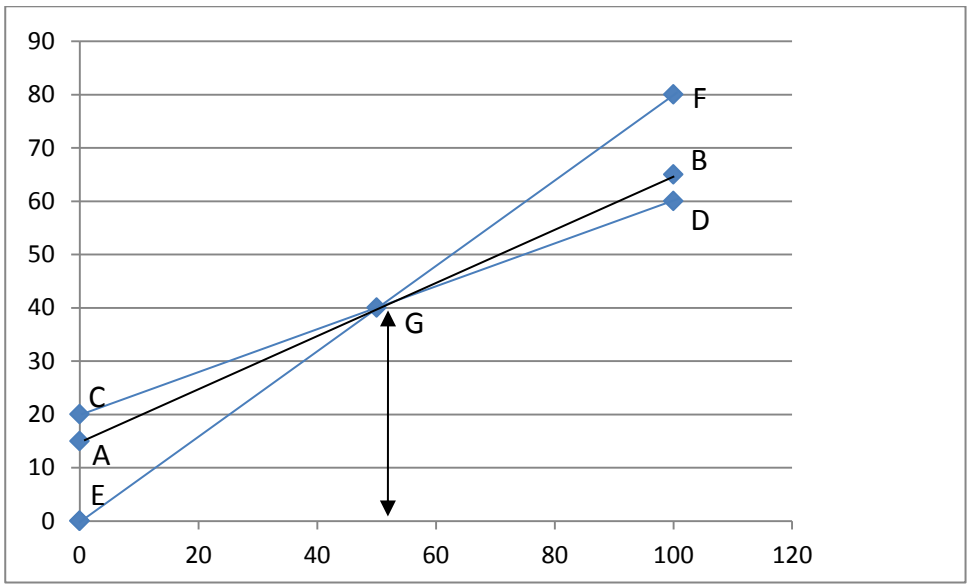
c) $S(x) = 0{,}8x \qquad y = 0{,}8x$

	x	y
$E \equiv$	$(0$	$0)$
$F \equiv$	$(100$	$80)$

Sistema per trovare il punto di intersezione delle 3 rette

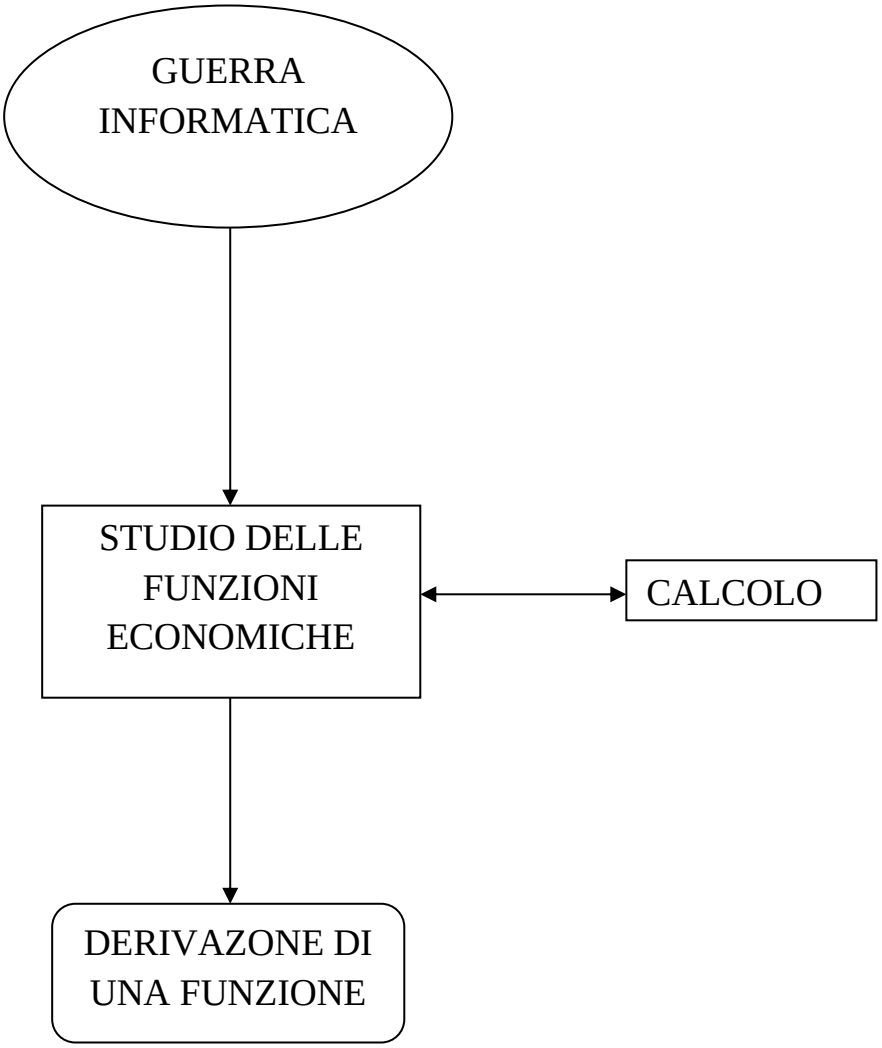
$$\begin{cases} y = 0{,}5x + 15 \\ y = 0{,}4x + 20 \\ y = 0{,}8x \end{cases} \qquad \begin{cases} \text{----------} \\ 0{,}4x = 20 \\ \text{----------} \end{cases} \qquad \begin{cases} \text{----------} \\ x = 50 \\ y = 40 \end{cases} \qquad P_0 \equiv (50; 40)$$

Grafico



Conviene l'alternativa C per una percorrenza di $0 \leq x \leq 50$;conviene l'alternativa B per $x \geq 50$.

MATEMATICA



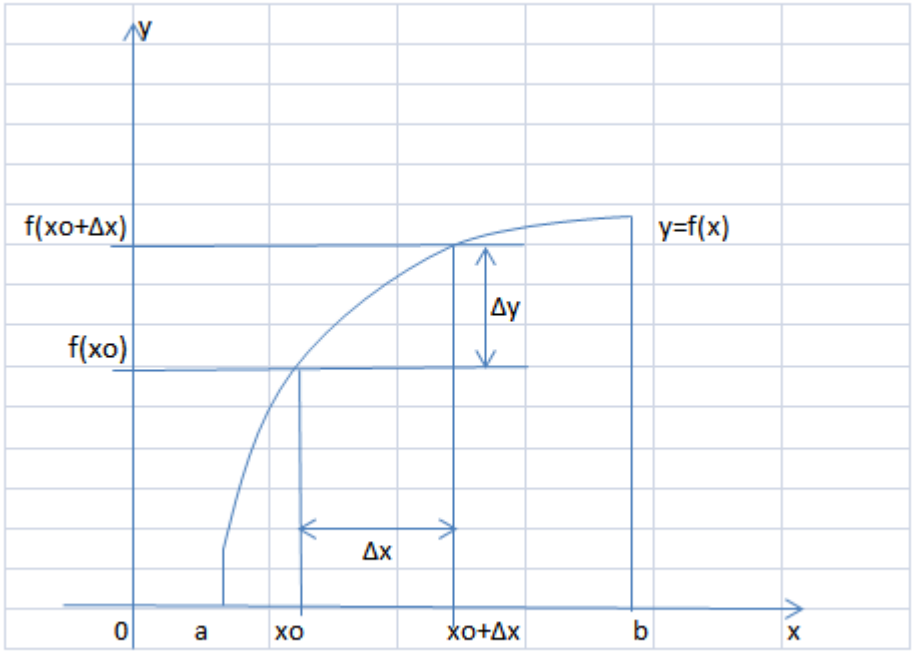
Dopo aver parlato dello studio delle curve economiche,inerente alle conseguenze che il cyber-spionaggio ha portato in scena; approfondiamo l'argomento delle funzioni economiche analizzando la metodologia di svolgimento per la ricerca del massimo e del minimo di una funzione. Per prima cosa definiamo il concetto di derivata e poi passiamo allo studio delle sue applicazioni.

DERIVATA

La **derivata** di una funzione è la misura di quanto il valore della funzione stessa cambi al variare del suo argomento. La derivata di una funzione f in un punto x_0 è il valore del coefficiente angolare della retta tangente alla curva nel punto. Nella spiegazione della derivata andiamo ad analizzare il concetto di rapporto incrementale.

RAPPORTO INCREMENTALE

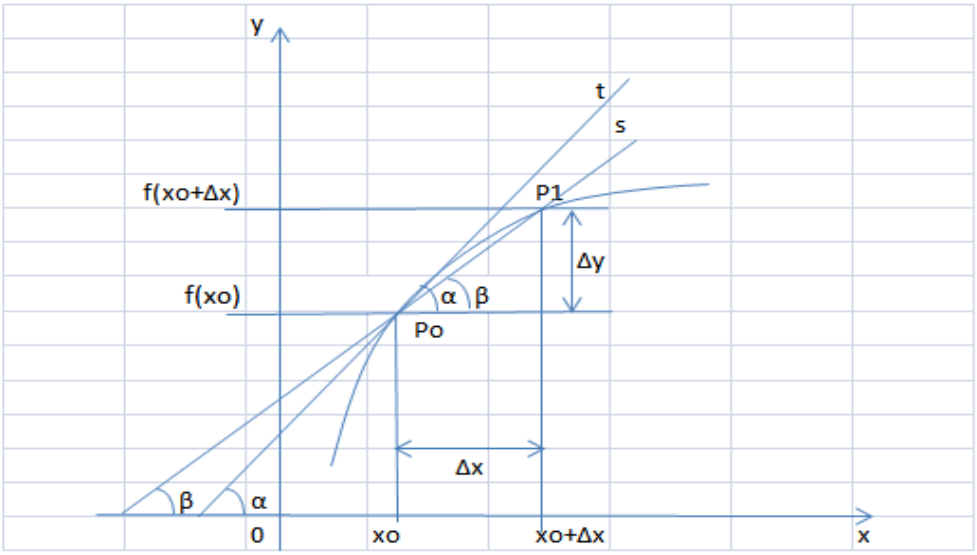
Sia f(x) definita in un intervallo (a,b) e siano x_0 un punto all'interno di questo intervallo e $y_0 = f(x_0)$ il valore assunto dalla funzione per $x = x_0$. Se alla x diamo un incremento Δx,cioè passiamo dal punto x_0 al punto $x_0 + \Delta x$;anche la variabile y subirà una variazione,portandola dal valore $f(x_0)$ al valore $f(x_0 + \Delta x)$. Quindi chiamiamo **incremento della funzione** la differenza $f(x_0 + \Delta x) - f(x_0)$.



E chiamiamo **rapporto incrementale** il rapporto tra l'incremento subito dalla funzione f(x) e l'incremento dato dalla variabile indipendente x.

$$\frac{\Delta y}{\Delta x} = \frac{\Delta f(x)}{\Delta x} = \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}$$

DIMOSTRAZIONE GEOMETRICA



Sia $y = f(x)$ l'equazione della curva rappresentata sul grafico e siano Po e P_1 i due punti di coordinate Po (x_0;$f(x_0)$) e P1 ($x_0+\Delta x$;$f(x_0+\Delta x)$). Allora il rapporto incrementale:

$$\frac{\Delta f(x)}{\Delta x} = \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}$$

Rappresenta la tangente dell'angolo β che la retta passante in Po e P_1 forma con la retta passante per Po e parallela all'asse x;questo rapporto rappresenta il coefficiente angolare **m** della retta che passa per Po e P_1.

Indicando con α l'angolo che la retta t forma con l'asse x risulta evidente che :

$\alpha = \lim_{P_1 \to P_0} \beta$ e anche $m = \tan\alpha = \lim_{P_1 \to P_0} \tan\beta$

E per quello detto in precedenza si può dire :

$m = \lim_{\Delta x \to 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x} = f'(x_0)$. Concludiamo la spiegazione dicendo che la derivata di una funzione f(x) nel punto x_0 rappresenta il coefficiente angolare della retta tangente alla curva di equazione $y = f(x)$ nel suo punto di ascissa x_0.

ALTRI TIPI DI DERIVATE

Tra i vari tipi di derivate esistenti,per la ricerca del massimo o del minimo relativo è importante lo studio delle **derivate parziali**.

La **derivata parziale** è una prima generalizzazione del concetto di derivata di una funzione reale alle funzioni di più variabili;o più semplicemente è la derivata di una funzione a più variabili. Si calcola tenendo presenti le regole di derivazione di volta in volta considerando una incognita come variabile e l'altra come costante.

La derivata parziale in un punto rispetto alla prima variabile di una funzione $f(x,y)$ rappresenta la pendenza della curva ottenuta intersecando il grafico di f (una superficie contenuta nello spazio), con un piano passante per il punto parallelo al piano $y = 0$.

Spiegazione dello svolgimento di un esercizio

$z = x^2 - xy + 3y^2 + 3x + 4y$

1) Calcolo delle derivate rispetto ad x e y.
   $f'_x = 2x - y + 3 \qquad f'_y = -x + 6y + 4$
2) Sistema tra le due derivate prime.

$$\begin{cases} f'_x = 2x - y + 3 \\ f'_y = -x + 6y + 4 \end{cases} \qquad \begin{cases} 12y + 8 - y + 3 = 0 \\ \text{----------} \end{cases}$$

$$\begin{cases} 11y = -11 \\ \text{----------} \end{cases} \qquad \begin{cases} y = -1 \\ x = -2 \end{cases}$$

3) Calcolo del Punto P_0

$P_0 \equiv (-2;-1;f(-2;-1)) \qquad z = 4 - 2 + 3 - 6 - 4 \qquad z = -5$

$P_0 \equiv (-2;-1;-5)$

4) Calcolo delle derivate seconde e delle derivate miste
   $f''_{xx} = 2 \qquad f''_{yy} = 6 \qquad f''_{xy} = -1 \qquad f''_{yx} = -1$

5) Calcolo dell'Hessiano

Hessiano : determinante della matrice quadrata

$$\begin{vmatrix} f''_{xx} & f''_{xy} \\ f''_{yx} & f''_{yy} \end{vmatrix} = f''_{xx} \cdot f''_{yy} - f''_{xy} \cdot f''_{yx}$$

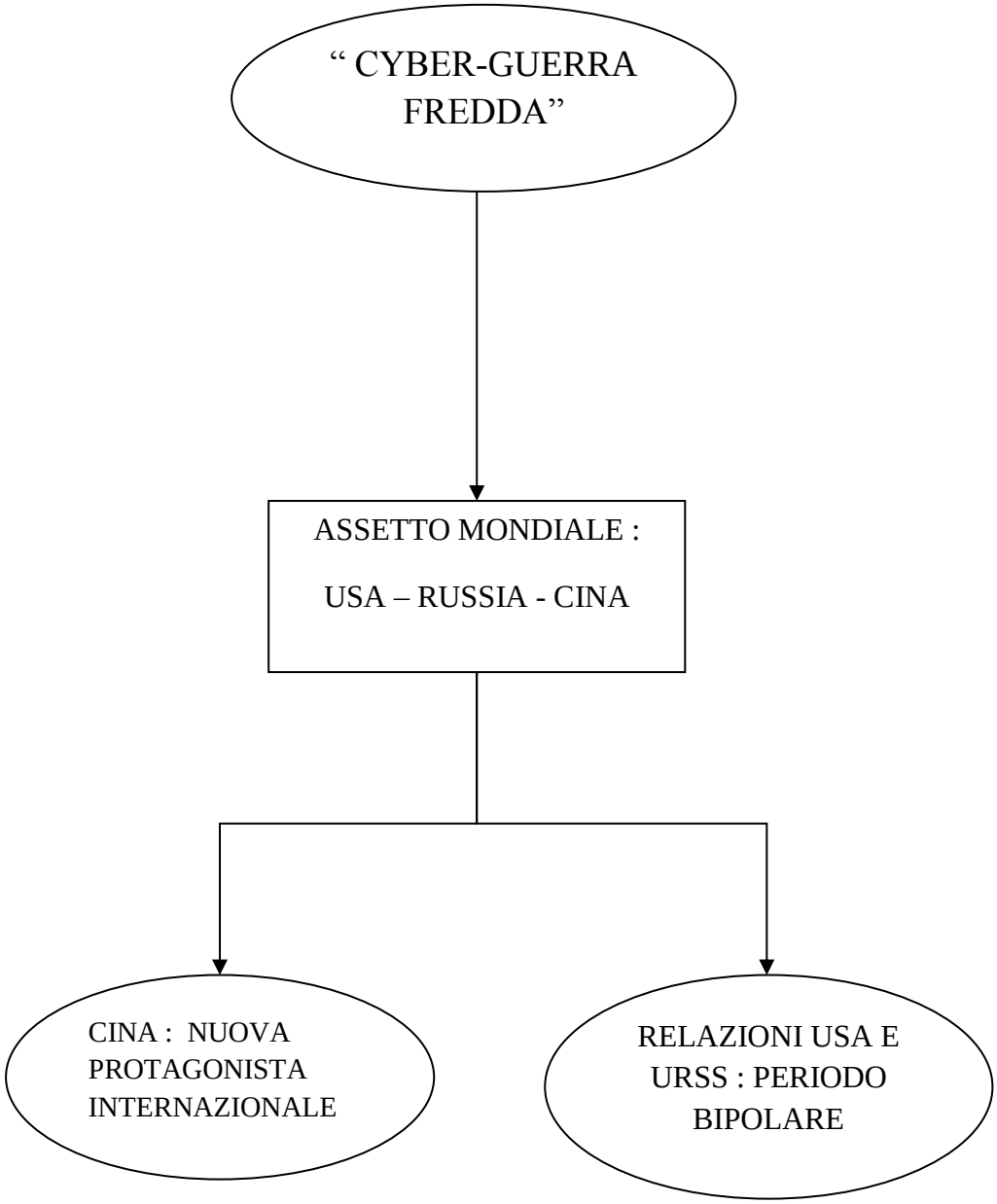
$\begin{vmatrix} 2 & -1 \\ -1 & 6 \end{vmatrix} = 12 - 1 = 11$ L'hessiano è > 0 e $f''_{xx} > 0$ quindi P_0 è un minimo relativo

L'hessiano può determinare che tipo di punto si sta studiando,ovvero se è un massimo,un minimo o un punto di sella;qui di seguito viene riportata la spiegazione dei possibili punti che si possono determinare.

MAX. relativo	MIN. relativo	SELLA
$\begin{cases} H(P_0) > 0 \\ f''_{xx}(P_0) < 0 \end{cases}$	$\begin{cases} H(P_0) > 0 \\ f''_{xx}(P_0) > 0 \end{cases}$	$\begin{cases} H(P_0) < 0 \end{cases}$

Durante lo svolgimento del precedente esercizio si è notato che le due derivate miste sono uguali. Infatti tutte le derivate miste di qualsiasi derivata sono uguali;tale regola è espressa dal **Teorema di Schwarz**. Per le due derivate seconde miste,continue in un insieme aperto, $\frac{\partial^2 f}{\partial y \partial x}$ e $\frac{\partial^2 f}{\partial x \partial y}$ vale la relazione : $\frac{\partial^2 f}{\partial y \partial x} = \frac{\partial^2 f}{\partial x \partial y}$.

STORIA



In questo capitolo si analizzerà l’aspetto del mondo d’oggi con le ormai potenze economiche affermate USA,Russia e Cina. Questa situazione attuale è stata caratterizzata da conflitti avvenuti in passato fra le tre nazioni; basti pensare al periodo “freddo” dove gli USA e la vecchia URSS si contendevano il potere nucleare offerto dalle nuove tecnologie,che portò il mondo sull’orlo di una catastrofe atomica. Ed è proprio in questo periodo che si poté vedere l’ascesa della Cina di Mao Tse-tung come nuovo stato autonomo. Infatti è al termine del periodo bipolare che le tre superpotenze intrapresero il cammino verso la loro affermazione. Sono queste relazioni che hanno

portato questi tre stati verso una nuova guerra fredda,non combattuta sul fronte ma bensì in rete, che ultimamente ha preso il nome di "cyber-guerra fredda".

Dopo questa breve introduzione sull'ascesa delle tre superpotenze odierne,passiamo allo studio generale del periodo che ne ha caratterizzato l'evoluzione.

RAPPORTI USA-URSS

Al termine della 2° guerra mondiale si tenne la conferenza di Yalta nel 1945,dove si crearono i presupposti per la divisione dell'Europa in due zone,sotto il comando dell'**URSS** e degli **USA**. Nel periodo compreso tra il 1945-1946 furono prese importanti iniziative economiche e territoriali riguardo l'assetto del mondo : creazione dell'**ONU** (Organizzazione delle Nazioni Unite),nascita della Banca Mondiale e l'istituzione di un tribunale militare internazionale con il quale vennero puniti i crimini di guerra con i processi a Norimberga contro i gerarchi nazisti. A questo periodo di estrema collaborazione emersero i primi dissapori,nella Conferenza di Potsdam (1945). Questi contrasti si finalizzarono con l'enunciazione della **dottrina Truman** e la nascita del **Cominform** : La guerra fredda era iniziata.

L'Europa era divisa in due blocchi : L'Oriente controllato dall'URSS e L'Occidente sotto l'influenza degli Stati Uniti. Questo clima portò alla suddivisione della Germania creando due linee opposte : nella Germania occidentale gli USA costituirono la Repubblica federale tedesca con a capo il cancelliere Adenauer, nella Germania orientale ci fu la nascita della Repubblica democratica tedesca. Infine da questi primi presupposti per un conflitto si arrivò all'istituzione di due vere e proprie alleanze quali il **Patto atlantico** e il **Patto di Varsavia**. Mentre negli USA cominciarono le persecuzioni a favore dell'anticomunismo con il ***maccartismo****; in URSS iniziò la repressione contro le ideologie filoccidentali. Per quanto riguarda la ricostruzione economica si può tener conto dell'intervento americano prima con la valorizzazione del libero mercato e poi con il piano Marshall (1948-1958) a favore degli stati europei; soprattutto Inghilterra e Francia rispettivamente con la politica del Welfare State e la nascita della Quarta Repubblica Francese.

La guerra fredda colpì anche i popoli asiatici,soprattutto la **Cina**. In Cina scoppio la guerra civile tra i comunisti di Mao e i nazionalisti di Chiang,supportati rispettivamente da URSS e USA. Da queste tensioni scoppiò la guerra di Corea che durò tre anni e che portò ad una continua corsa agli armamenti che si concluse con l'esplosione della bomba H da parte degli USA e dalla dichiarazione dell'URSS di possedere tale arma. Questo nuovo quadro politico portò all'ennesima creazione di un sistema di alleanze da parte degli USA. Dopo la pesante guerra combattuta in Corea, la guida

dell'URSS passò nelle mani di **Krusciov**,causa la morte di Stalin, che basava la sua politica sulla coesistenza pacifica dei due blocchi. Nel 1956 Krusciov denunciò i crimini commessi da Stalin procedendo così ad una destalinizzazione che però non eliminò i gulag. Quattro anni dopo negli USA veniva eletto presidente **John Fitzgerald Kennedy** che fin da subito volle rafforzare la democrazia. La politica di Kennedy incontro due particolari situazioni di crisi : 1) La crisi tedesca che portò all'istituzione del muro di Berlino,diventato poi il vero simbolo della guerra fredda. 2) La crisi di Cuba dove Kennedy dovette fronteggiare la rivoluzione di **Fidel Castro**,che avvicinò Cuba all'URSS, e fu proprio quest'ultima che scatenò la reazione americana,causa l'installazione di basi missilistiche a Cuba,sfiorando la guerra atomica nel 1962. Dopo la scampata catastrofe ebbe inizio una politica di distensione tra i due blocchi,favorita anche dallo spirito pacifista di papa Giovanni XXIII. Questa situazione non ebbe il tempo di decollare che tra il 1963 e il 1964 scomparivano papa Giovanni XXIII per morte naturale,Kennedy assassinato a Dallas il 22 Novembre 1963 e Krusciov che fu destituito causa i mancati traguardi raggiunti.

Nel 1964,al posto di Krusciov,era divenuto segretario del partito comunista Leonid Brežnev,che promosse due nuovi piani economici incentrati sullo sviluppo dell'industria leggera e sul potenziamento delle fattorie per migliorare le condizioni di vita dei lavoratori agricoli. In politica estera Brežnev non si distaccò dalla linea della distensione tra i due blocchi;esempio gli accordi sulla limitazione delle armi missilistiche tra Usa e Urss,firmati a Mosca nel 1972. Il governo di Brežnev non fu però in grado di attuare un concreto sviluppo produttivo ed economico,e prese una brutta piega quando nel 1968 Brežnev si prese la colpa di un **colpo di forza ai danni della cecoslovacchia**. Aleksander Dubček,segretario del partito comunista,aveva avviato in Cecoslovacchia un programma di democratizzazione con l'appoggio del popolo. Di fronte a questo atto Brežnev ricorse all'intervento armato. Nell'agosto del 1968 le truppe sovietiche posero fine a quella "**primavera di Praga**" che aveva acceso tante speranze nei Paesi dell'Est. L'intero territorio cecoslovacco fu occupato e Dubček fu destituito.

Nel Novembre del 1963,dopo l'assassinio di Kennedy,era salito alla presidenza degli USA il democratico Lyndon Johnson. Johnson adottò il programma detto della "grande società",incentrato sulla lotta alla discriminazione razziale. Durante la sua presidenza,la politica della coesistenza pacifica fu messa a dura prova dall'intervento americano nel **Vietnam**,iniziato con Kennedy nel 1962. Le decisioni della conferenza di Ginevra del 1954 non furono gradite dagli Americani,che non dettero il loro consenso agli accordi. Le elezioni non si tennero e nacquero due stati separati : a nord una repubblica popolare comandata da Ho Chi Minh con capitale Hanoi,e a sud uno stato comandato direttamente dagli USA,sotto il regime di Ngo Dinh Diem con capitale Saigon. Il

governo di Diem si rivelò corrotto dando origine ad una forte opposizione del paese portata avanti dai vietcong. Da qui ebbe origine l'invio dei primi aiuti americani a Saigon. L'intervento americano in Vietnam provocò contestazioni e proteste all'interno del paese e convinse Johnson a rinunciare ad una nuova candidatura nel 1968.

Alla fine degli anni 60' il bipolarismo Usa-Urss mostrava segni di crisi a causa dei rispettivi attacchi in Vietnam e in Cecoslovacchia. Di fronte a questa disgregazione le due superpotenze reagirono in modi diversi : L'Unione Sovietica rimase ancorata alla logica della spartizione in sfere d'influenza. Gli Stai Uniti invece non si abbandonarono al recupero di schemi di rigido controllo sul mondo. L'iniziativa partì dal presidente repubblicano **Richard Nixon** che fece di tutto per riconquistare credibilità e prestigio internazionale. Nixon attuò una politica di riavvicinamento alla Cina di Mao. L'avvicinamento cino-americano accentuava sulla scena mondiale il "**confronto a tre**" fra Usa,Cina e Urss. A caratterizzare la presidenza Nixon fu il ritiro delle truppe americane dal Vietnam. Così a Parigi nel gennaio del 1973 ci fu l'accordo che sanciva il ritiro degli aiuti americani a Saigon e lasciava ai due Vietnam il compito della pacificazione. Questo segnò la **prima grave sconfitta nella storia degli Usa**. I successivi scontri portarono il Vietnam sotto il controllo del governo comunista di Hanoi. Nell'agosto del 1974 il presidente americano Nixon fu costretto a dimettersi. La stampa intercettò **atti di spionaggio** ai danni del concorrente avversario nelle elezioni; fu definito il **caso Watergate.** Nixon lasciò il posto al vicepresidente Gerald Ford. Nel 1980 divenne presidente degli Stati Uniti Ronald W. Reagan. Egli attuò un intenso programma di liberazione e di deregolamentazione al fine di contrarre le voci di spesa dei bilanci. Questa linea economica incrementò il prodotto nazionale lordo e riuscì a contenere l'inflazione,e bilanciò la disoccupazione. Altre tensioni tra i due blocchi Usa-Urss provenivano dal settore militare causa la sostituzione dei vecchi missili con dei nuovi missili balistici da parte dell'Urss. Questo provocò la risposta di Reagan che annunciò nel 1983 un progetto di difesa strategica detto "**scudo spaziale**". Non mancarono le proteste dalle correnti pacifiste,anche perché questa nuova corsa agli armamenti gravò sull'economia dell'Europa Orientale.

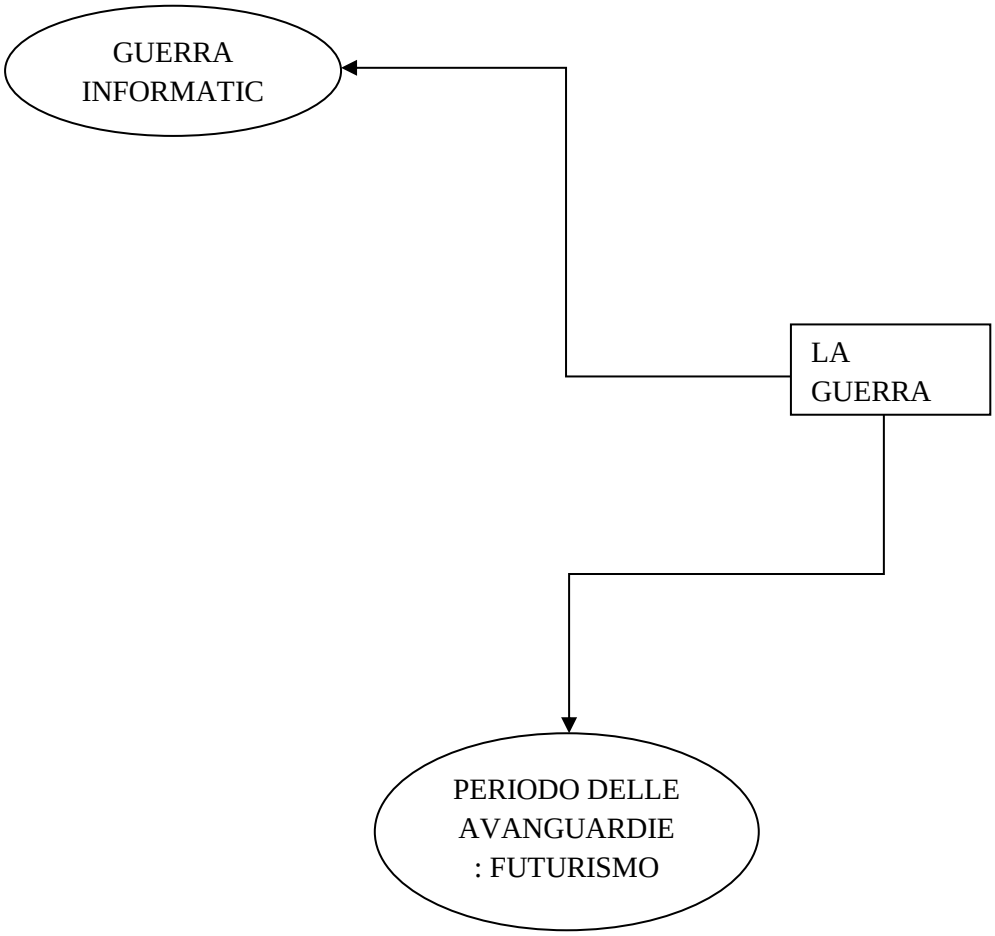
L'Unione Sovietica di Brežnev vide in declino la stabilità del suo modello politico e ideologico su vari versanti,soprattutto la crisi che colpì l'economia tra la fine degli anni 60' e l'inizio degli anni 80',si rivelò come il fattore più importante della debolezza sovietica. Nel Novembre del 1982 moriva Brežnev e veniva eletto nuovo segretario del partito **Michail Gorbaciov**. L'attività del nuovo leader si basò su due termini : **glasnost*** e **perestrojka***. Gorbaciov richiedeva una riduzione delle spese militari e l'inserimento del Paese nel circuito commerciale mondiale. Nell'ottobre del 1986 Gorbaciov ordinò il ritiro delle truppe dall'Afghanistan e nel 1987 assieme agli Usa ordinò di

distruggere 2700 dei rispettivi missili;questo fatto costituiva il primo passo verso la via del disarmo. In Urss la riforma di Gorbaciov si stava attuando;prima trovò l'appoggio del repubblicano George Bush,nuovo presidente americano dal 1988, e poi riprese i rapporti diplomatici con la Cina. Nel 1991 la struttura del patto di Varsavia fu sciolta e nel Luglio dello stesso anno fu firmato il trattato **Start 1** che portò alla riduzione del 40% gli armamenti nucleari. Gorbaciov si mostrò meno efficiente in campo economico e portò ben presto alla diffusione della povertà. Questa crisi portò a nuove pressioni da parte delle altre Repubbliche quali Estonia,Lettonia e Lituania. Intanto **Boris Eltsin** conquistò il 60% dei voti nelle elezioni per il presidente della repubblica russa nel 1991. Le tensioni aumentarono e sfociarono in un colpo di stato organizzato da esponenti del partito comunista e del **Kgb**. Il colpo di stato fallì e molte repubbliche proclamarono la loro indipendenza. Il 9 dicembre 1991 Eltsin dichiarò sciolta l'URSS. Il 25 dicembre 1991 Gorbaciov si dimise dalla sua carica. Si sanciva la fine dell'epoca del bipolarismo e della guerra fredda iniziata 50 anni prima.

EVOLUZIONE CINA

Come già detto in precedenza la guerra fredda ebbe le sue ripercussioni anche in Asia dove al termine della guerra civile tra comunisti e nazionalisti,prevalse la linea Comunista di Mao Tse-tung che fece riconoscere la Cina dagli USA come stato autonomo. Mao intraprese un piano industriale quinquennale tra il 1953 e il 1958 con l'obiettivo principale di potenziare l'industria favorendo lo sviluppo dell'agricoltura e lanciando la politica del "grande balzo in avanti". A questa evoluzione sul piano della politica interna,seguì un duro scontro con l'URSS che sfociò con la rottura delle relazioni tra Pechino e Mosca,causa la mancata concessione dei piani nucleari da parte dell'URSS. Comunque la Cina riuscì a costruire un primo ordigno nucleare,causando liti interne che portarono il bipolarismo ad incrinarsi. Fallita la politica del balzo in avanti,Mao intraprese la via della rivoluzione rivolgendosi alle masse, aprendo la strada alla "rivoluzione culturale" basata sui principi di rigida eguaglianza che ben presto portò a livelli molto alti di tensione e violenze nel paese. Così nel 1967 Mao cessò il "nuovo corso" e tra il 1968-1969 si trovo a lottare con alcuni elementi dell'estrema sinistra nel momento in cui voleva indurre la sua Cina in una fase più moderata aprendo i contatti con l'occidente. Questa fase si concluse con l'avvicinamento degli USA e l'entrata della Cina nell'ONU. Nel 1976 alla morte di Mao,i suoi successori portarono ancora più in alto questa sua politica basata sul libero mercato e sulla proprietà privata congiungendo il progresso economico con la tradizione socialista e le riforme liberali;diventando la terza potenza mondiale.

ITALIANO



In questa parte andremo a spiegare il collegamento tra lo spionaggio informatico e il futurismo. Come punto d'incontro troviamo la guerra e la sua evoluzione nel tempo.

La guerra,nel corso degli anni,ha cambiato il suo significato. Da i primi due conflitti mondiali che cambiarono l'assetto del mondo per poi passare al periodo della guerra fredda dove troviamo una grande opera di spionaggio; dalla guerra in Iraq dove vengono messe alla prova nuove tecnologie in campo militare,fino ad arrivare ad oggi con la nascita della "guerra informatica",concetto che porta in campo nuove tecnologie e forme di attacco cibernetico. Quindi la guerra,su campo internazionale,è vista come strumento per risolvere contese tra due linee opposte,con l'intento di "portare pulizia là dove si è sporcato". Ed è proprio questo il concetto che i futuristi dei primi anni

del ‘900 attribuivano alla guerra. Questo tema poneva la guerra come << sola igiene del mondo>>. Infatti col passare degli anni si poté notare come la guerra prese un ruolo importante nel mondo e nella sua continua evoluzione.

Spiegata l’evoluzione della guerra e il suo ruolo planetario,passiamo con l’approfondire il movimento del Futurismo.

FUTURISMO

Il Futurismo nasce in Francia nel 1909 dal suo fondatore Filippo Tommaso Marinetti. Marinetti porta sulla scena un movimento nuovo e organizzato,infatti proprio nel 1909 pubblica il Manifesto del Futurismo,ovvero il simbolo della fondazione. In questo Manifesto vengono spiegate le idee fondamentali di tale movimento:


LE FIGARO

Le Futurisme

Échos

- **Abbandono della tradizione** : Il Futurismo volendo rinnovare la cultura, liquida tutto ciò che appartiene alla tradizione con il nome di << passatismo >>.
- **Culto della città industriale** : Esaltazione della società industriale e delle sue nuove invenzioni dove si distingue la macchina da corsa. La macchina promuove la nuova realtà che i futuristi portano sulla scena,ovvero la velocità.
- **Violenza e guerra** : Marinetti promuove la guerra come << sola igiene del mondo >>,e la violenza,“il pugno e lo schiaffo”. Da qui si può capire perché i futuristi furono favorevoli all’entrata in guerra dell’Italia nella “grande guerra”.

Nel 1912 Marinetti pubblicò un altro manifesto : il Manifesto tecnico della letteratura futurista dove elencava i principi che dovevano caratterizzare questo nuova letteratura.


Manifesto tecnico
della
letteratura futurista

- **Simultaneità** : Immediatezza,da parte del poeta,nell'esprimere i concetti.
- **Parole in libertà** : Lo scrittore non dovrà preoccuparsi,nello scrivere,della metrica,della sintassi e della punteggiatura. E' da questo tema che nasce il concetto di ***poesia visiva****.
- **Analogia** : Ricorrenza a paragoni tra cose diverse tra loro senza l'uso del "come" (invece di "uomo come un animale",dirà << uomo-animale >>).

La propaganda di questo movimento fu favorita dalla nascita di riviste come <<Poesia>> o <<Lacerba>>. Altri momenti importanti per la propaganda futurista furono le "serate futuriste dove si riscontra il concetto di violenza,poiché terminavano con lo scambio di pugni e lanci di oggetti.

Il Futurismo,al di là della violenza di certe posizioni,segnò una svolta nella storia letteraria e nella cultura,contribuendo a un processo di rinnovamento.

FILIPPO TOMMASO MARINETTI

Filippo Tommaso Marinetti nasce ad Alessandria d'Egitto nel 1876. Grazie alle condizioni agiate della sua famiglia passa il periodo della formazione in Francia,a Parigi,dove entrò in contatto con gli ambienti culturali della capitale e dove pubblicò le sue prime opere in francese.

Vissuto prevalentemente a Milano,fu il fondatore del Futurismo. Nel 1905 dà vita alla rivista <<Poesia>>,pubblicata fino al 1909,anno in cui pubblica il *Manifesto del Futurismo* sul giornale <<Le Figaro>>. Sempre nel 1909 pubblicò un altro manifesto importante del nuovo movimento : *Uccidiamo il chiaro di Luna!*,seguito dal romanzo *Mafarka il futurista.* Marinetti cercava di creare opere coerenti con i principi da lui proposti. Nel 1912 pubblica il *Manifesto tecnico della letteratura futurista* e la *Distruzione della sintassi*,e nel 1914 scrisse un testo composto da <<parole in libertà>>,ovvero *Zang Tumb Tumb*,come esperienza durante la guerra di Libia nel 1911. Interventista nato,pubblica nel 1915 il volume *Guerra,sola igiene del mondo*,e poi si arruola come volontario per la I° guerra mondiale. Dopo la guerra aderì al Fascismo pubblicando volumi che

esaltavano Mussolini ed il suo regime : *Futurismo e Fascismo,Canto eroi e macchine della guerra mussoliniana*. Morì a Bellagio,in provincia di Como,nel 1944.

OPERA

IL BOMBARDAMENTO

ogni 5 secondi cannoni da assedio sventrare
spazio con un accordo tam-tuuumb
ammutinamento di 500 echi per azzannarlo
sminuzzarlo sparpagliarlo all'infinito
Nel centro di quei tam-tuumb
spiaccicati (ampiezza 50 chilometri quadrati)
balzare scoppi tagli pungi batterie tiro
rapido Violenza ferocia regolarità questo
basso grave scandere gli strani folli agita-
tissimi acuti della battaglia Furia affanno
orecchie occhi
narici aperti attenti
forza che gioia vedere udire fiutare tutto
tutto taratatatata delle mitragliatrici strillare
a perdifiato sotto morsi schiaffi traak-
traack frustare pic-pac-pum-tumb bizz-
zzarie salti altezza 200m. della fucileria
Giù giù in fondo all'orchestra stagni
diguazzare buoi bufali
pungoli carri pluff plaff inpen-
impennarsi di cavalli flic flac zing zing sciaaack
lari nitriti iiiiii….. scalpiccii tintinnii 3
battaglioni bulgari in marcia croooc-craac
[LENTO DUE TEMPI] Sciumi Marita
o Karvavena croooc craaac grida degli
ufficiali sbataccccchiare come piattttti d'ottttone
pan di qua paack di là cing buuum
cing ciack [PRESTO] ciaciaciaciaciaak
su giù là là in-torno in alto attenzione
sulla testa ciaack bello Vampe
vampe
vampe vampe
vampe vampe
vampe ribalta dei forti die-
vampe
vampe
tro quel fumo Sciukri Pascià comunica tele-
fonicamente con 27 forti in turco in te-
desco allò Ibrahim Rudolf allô allô
attori ruoli echi suggeritori
scenari di fumo foreste

ANALISI DEL TESTO

In Zang Tumb Tumb,pubblicato nel 1914,Marinetti descrive la guerra balcanica del 1912-13 tra Grecia,Bulgaria e Serbia da una parte e Turchia dall'altra.

In questo teso si può notare la vera essenza del manifesto del futurismo,poiché Marinetti cerca di esprimere i concetti base del futurismo. Si possono analizzare 3 elementi principali nell'opera:

1. Le parole sono disposte in modo libero o disordinato;ad esempio la parola vampe ripetuta più volte
2. Dal punto di vista grafico le parole assumono più dimensioni (prima in corsivo,poi in neretto).
3. Linguaggio "pregrammaticale" composto da parole senza valore grammaticale,ma che rappresentano i suoni. Marinetti con questo linguaggio voleva trasmettere al lettore il caos e il frastuono che caratterizzano il bombardamento.

CAPITOLO 10 : ITALIANO

applausi odore di fieno fango sterco non
sento più i miei piedi gelati odore di sal-
nitro odore di marcio Timmmpani
flauti clarini dovunque basso alto uccelli
cinguettare beatitudine ombrie cip-cip-cip brezza
verde mandre don-dan-don-din-béèé tam-tumb-
tumb tumb tumb-tumb-tumb
-tumb Orchestra pazzi ba-
stonare professori d'orchestra questi bastonatissimi
suooooonare suooooonare Graaaaandi
fragori non cancellare precisare rittttagliandoli
rumori più piccoli minutisssssssimi rottami
di echi nel teatro ampiezza 300 chilometri
quadrati Fiumi Maritza
Tungia sdraiati Monti Rò-
dopi ritti alture palchi log-
gione 2000 shrapnels sbracciarsi ed esplodere
fazzoletti bianchissimi pieni d'oro Tum-
tumb 2000 granate
protese strappare con schianti capigliature
tenebre zang-tumb-zang-tuuum-
tuuumb orchestra dei rumori di guerra
gonfiarsi sotto una nota di silenzio
tenuta nell'alto cielo pal -lone
sferico dorato sorvegliare tiri parco aerostatico Kadi-Keuy .

CONCLUSIONI

Nella seguente tesi che è stata proposta,abbiamo visto come la nuova forma di spionaggio informatico,abbia avuto risvolti negativi per l'economia mondiale,e su come la criminalità ne ha usufruito per scopi illeciti. Da queste basi che si può definire il termine guerra al giorno d'oggi. La guerra ormai è uno strumento indispensabile per l'evoluzione di uno stato,sia a livello economico che a livello politico;anche se nel corso degli anni si è visto un cambiamento radicale degli armamenti. In questa nuova guerra che sta per dilagare,le armi utilizzate non saranno armi da fuoco,ma bensì armi cibernetiche che non produrranno il numero di vittime che si è potuto vedere nelle altre guerre del '900,ma porteranno gravi conseguenze a livello economico nei vari paesi. Mentre prima l'interesse della guerra,oltre a pendere sul lato monetario, era di natura espansionistica e bisognava conquistare il territorio e mantenerne il possesso;ora l'interesse è puramente economico con l'intento di arricchirsi con il capitale di un altro.

GLOSSARIO

Internet : E' la rete mondiale di computer ad accesso pubblico che rappresenta il principale mezzo di comunicazione di massa,che offre ai comunicanti una vasta gamma di informazioni.

Economia sommersa : L'insieme delle attività economiche che contribuiscono al prodotto interno lordo in questione,ma che non sono registrate e regolarmente tassate.

Imageboard : E' una tipologia di sito internet basata sulla pubblicazione di immagini da parte dei propri utenti.

Forum : E' l'insieme delle sezioni di discussione in una piattaforma informatica.

Guerra totale : Termine nato per indicare un conflitto in cui i paesi coinvolti utilizzano la totalità delle loro risorse per battere l'avversario.

Information warfare : E' una metodologia di conflitto armato,che utilizza l'informazione in ogni sua forma per superare militarmente l'avversario.

DDoS : Acronimo di Distributed Denial of Service. E' un malfunzionamento,causato da un attacco informatico,in cui si esauriscono le risorse di un sistema informatico che fornisce un servizio, fino a renderlo non più in grado di erogare il servizio.

Sniffer : Software capace di ascoltare il traffico di rete in provenienza o destinato ai terminali posti sullo stesso ramo. Tale attività può essere svolta sia per scopi legittimi per scopi illeciti.

Malware : Software creato con il solo scopo di causare danni più o meno gravi ad un computer.

Botnet : E' una rete formata da dispositivi informatici collegati ad Internet e infettati da malware, controllata da un'unica entità, il botmaster.

NIC : E' un'interfaccia digitale che svolge tutte le elaborazioni o funzioni necessarie a consentire la connessione dell'apparato informatico ad una rete informatica.

PAM : Tipo di modulazione dove l'informazione è codificata in ampiezza da una serie di impulsi.

Fattore roll - off : Il coefficiente di roll-off si utilizza per caratterizzare i filtri reali. Siccome i filtri ideali non esistono, il coefficiente di roll-off esprime l'ampiezza della curva di discesa che la risposta del filtro ha in prossimità della freq di taglio, il coeff varia da 0 a 1 ed è il rapporto fra la freq. di taglio e la banda aggiuntiva, cioè quella porzione di banda in prossimità della freq. di taglio in cui la risposta in frequenza del filtro ha una discesa non verticale

CAPITOLO 12 : GLOSSARIO

R.O. : E' l'applicazione del metodo scientifico a problemi che implicano il controllo di sistemi organizzati,al fine di fornire soluzioni che risolvano tali problemi.

Valor medio : Il Valor Medio è la somma di un insieme di valori,rapportata al numero dei suddetti valori.

Maccartismo : Fu un periodo della storia degli Stati Uniti caratterizzato dall'intenso sospetto anticomunista.

Glasnost : Parola russa che significa "trasparenza". Termine utilizzato per descrivere un presupposto della politica di Gorbaciov in Russia. La trasparenza introdusse un cambiamento radicale nel gestire la politica,promuovendo la libertà di stampa e di opinione.

Perestrojka : Parola russa che significa "ricostruzione". Termine utilizzato per descrivere un presupposto della politica di Gorbaciov in Russia. La perestrojka avviava radicali riforme nella struttura politico-economica del paese.

Poesia visiva : Tipo di poesia nata nei primi anni del '900,che mette in relazione la parola con l'immagine.

BIBLIOGRAFIA

LIBRI

- Dieci secoli di Letteratura 3A – *Realismo,Simbolismo,Avanguardie*;MURSIA SCUOLA.
- INFERENZA STATISTICA E RICERCA OPERATIVA,TRAMONTANA.
- Il nuovo Dialogo con la storia 3 – Il novecento;LA NUOVA ITALIA.
- Nuovo corso superiore di Matematica per trienni ITI D – Analisi infinitesimale;MINERVA ITALICA.
- INFORMATICA : Le basi di dati e il linguaggio SQL,ACCESS,MySQL,Database in rete.

SITI INTERNET

- http://www.wikipedia.it
- http://www.dmlogica.com
- http://it.kioskea.net/

ARTICOLI

- Michele Paris, Informatica, *La cyber-guerra tra USA e Cina*, in "altrenotizie", 22 Febbraio 2013.
- Andrea Curiat, Economia, Usa, *Quando il cyber-spionaggio è a fini economici*, in "Money", 11 febbraio 2013.
- Francesca Bosco e Chiara Cocciadiferro, Privacy in rete,*L'evoluzione del crimine informatico: dall'hacking all'underground economy*, in " La rivista di FormareNetwork".
- Paolo Attivissimo, Tecnologia, *Il più grande attacco informatico della storia*, in "Internazionale", 28 Marzo 2013.

INTERVISTE

- Intervista a Eugene Kaspersky, *L'Italia è pronta alla guerra informatica?*, 7 Luglio 2011.

Firma del candidato

_____