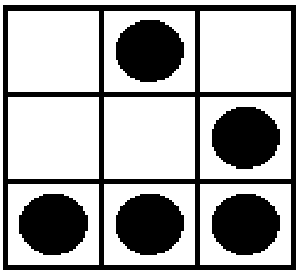
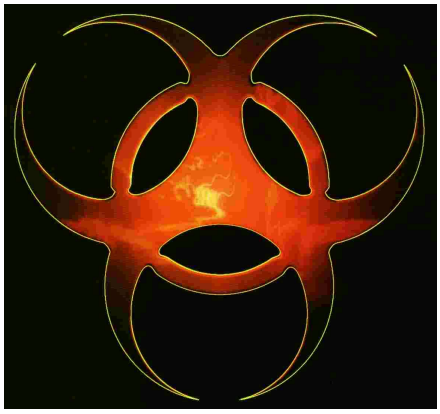
CRIMINALITA' INFORMATICA

I craker



Un **hacker** (termine coniato negli Stati Uniti del quale è difficile rendere una corretta traduzione in italiano) è una persona che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte, non limitatamente ai suoi ambiti d'interesse (che di solito comprendono l'informatica o l'ingegneria elettronica), ma in tutti gli aspetti della sua vita.

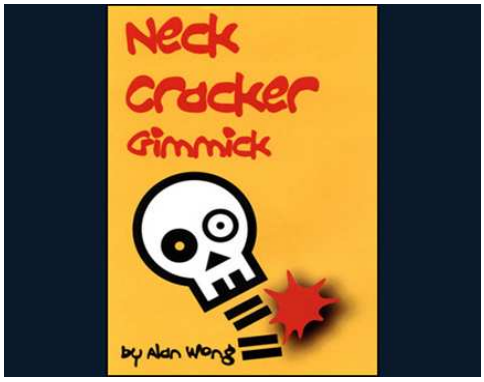
Esiste un luogo comune, usato soprattutto dai mass media (a partire dagli anni '80), per cui il termine hacker viene associato ai criminali informatici (la cui definizione corretta è, però, "cracker").
In ambito informatico il termine inglese indica colui che si ingegna per eludere blocchi imposti da qualsiasi software in genere. Il cracking può essere usato per diversi scopi secondari, una volta guadagnato l'accesso nel sistema desiderato o dopo aver rimosso le limitazioni di un qualsiasi programma. I cracker possono essere spinti da varie motivazioni, dal guadagno economico (tipicamente coinvolti in operazioni di spionaggio industriale o in frodi) all'approvazione all'interno di un gruppo di cracker (come tipicamente avviene agli script kiddie, che praticano le operazioni di cui sopra senza una piena consapevolezza né delle tecniche né delle conseguenze).



Il termine cracker viene spesso confuso con quello di hacker, il cui significato è tuttavia notevolmente diverso. Alcune tecniche sono simili, ma l'intenzione dell'hacker è generalmente l'esplorazione, il divertimento, l'apprendimento, senza creare reali danni. Al contrario, quella del cracker è talvolta distruttiva.

I più comuni tipi di attacco:

- SNIFFING: Si definisce **sniffing** l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).



I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso. Gli sniffer intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo. Inoltre possono offrire strumenti di analisi che analizzano ad esempio tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo o per ricostruire lo scambio di dati tra le applicazioni.
- SPOOFING: Lo **spoofing** è le tecnica con la quale un criminale informatico invia pacchetti modificando l'indirizzo IP del sorgente e facendo credere, quindi, all'host di destinazione e ai vari nodi che il pacchetto attraversa di provenire da un'altra sorgente. Le tecniche di spoofing possono essere distinte in: spoofing di indirizzi IP che per l'appunto falsifica la provenienza dei pacchetti, e spoofing di dati che consiste invece nel prendere il controllo del canale di comunicazione e nell'inserire, modificare o cancellare i dati che vi vengono trasmessi.

- NEGAZIONE DI SERVIZIO (DoS): In questo tipo di attacco si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server Web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile", quindi qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è soggetto al rischio di attacchi DoS.
Inizialmente questo tipo di attacco veniva attuata dai "cracker", come gesto di dissenso etico nei confronti dei siti web commerciali e delle istituzioni; ma oggi gli attacchi DoS hanno la connotazione decisamente più "criminale" di impedire agli utenti della rete l'accesso ai siti web vittime dell'attacco. Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva ad un comando proveniente dal cracker creatore. Se il programma maligno si è diffuso su molti computer, può succedere che migliaia di PC violati da un cracker, producano inconsapevolmente e nello stesso istante un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio.
- E-MAIL BOMBING; è una tecnica che prevede il bombardamento, con migliaia di messaggi di posta elettronica, della casella di un utente, per provocare un crash del server. Una delle possibili conseguenze risulta l'impossibilità di prelevare e visionare la propria posta non ancora scaricata al momento dell'attacco.

- SPAMMING o ***spamming*** (detto anche **fare *spam*** o ***spammare***) è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail. Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno **spammer**, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete mediante appositi programmi, ottenuti da database o semplicemente indovinati usando liste di nomi comuni.
Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli Internet Service Provider (ISP) e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato.
Un gran numero di spammer utilizza intenzionalmente la frode per inviare i messaggi, come l'uso di informazioni personali false (come nomi, indirizzi, numeri di telefono) per stabilire account disponibili presso vari ISP. Questo permette di muoversi velocemente da un account a un altro appena questo viene scoperto e disattivato dall'ISP. Gli spammer usano software creato per osservare connessioni Internet con scarsa sicurezza, che possono essere facilmente dirottate in modo da immettere i messaggi di spam direttamente nella connessione dell'obiettivo con il proprio ISP. Questo rende più difficile identificare la posizione dello spammer e l'ISP della vittima è spesso soggetto di aspre reazioni e rappresaglie da parte di attivisti che tentano di fermare lo spammer. Entrambe queste forme di spamming "nascosto" sono illegali, tuttavia sono raramente perseguiti per l'impiego di queste tattiche. Lo spamming è considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni.

- CODICE MALEFICO (MALWARE) Si definisce **malware** un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche *codice maligno*.

- LE BACKDOOR Le **backdoor** sono paragonabili a *porte di servizio* (cioè le porte del retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico. Queste "porte" possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica mentre più spesso da cracker intenzionati a manomettere il sistema. Possono anche essere installate autonomamente da alcuni *malware* (come virus, worm o trojan), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

- NUKING; la conoscenza dell'indirizzo IP numerico di un utente che sta navigando fornisce a un cracker la principale informazione che stava cercando. il nuke consiste infatti nel far resettare a distanza il computer della vittima, di cui si conosce l'indirizzo IP, sfruttando un bug di windows.

- PHISHING: In ambito informatico il phishing ("spillaggio (di dati sensibili)", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a messaggi che imitano grafico e logo dei siti istituzionali, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc..

Il processo standard delle metodologie di attacco di spillaggio può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (*phisher*) spedisce al malcapitato ed ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'email contiene quasi sempre avvisi di *particolari situazioni o problemi* verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
3. l'email invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.
4. il link fornito, tuttavia, *non* porta in realtà al sito web ufficiale, ma ad una *copia fittizia* apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

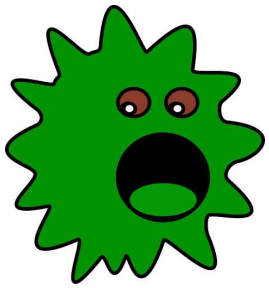
Computers viruses

Just as there are biological viruses that can be transmitted from person to person, so there are, by analogy, computer viruses that can be transmitted from computer to computer.
Unlike biological viruses, computer viruses do not occur naturally, but are the work of programmers (crackers). Perhaps originally, programmers developed these viruses as a way of showing how clever they were, but viruses are now developed in order to disrupt systems for political or other reasons.
A virus is a program or piece of code that is attached to or embedded in another program.
Note that viruses can only be associated with program files (not simple text files), but a macro in a world processing files is a kind of program, so viruses can be found in a word processing files.

WHAT EFFECT CAN VIRUSES HAVE?

It is impossible to provide a complete list of what viruses can do, because virus writers invent new effects on a regular basis. Viruses do many different things. Some are instantaneous, that is, they happen as soon as the program with which the virus is associated is run. Others viruses are moles and wait until an event triggers them; for example, one early virus went into action on a Friday the 13th.
Some effects of viruses are as follows:

- They copy themselves to other files.



- They make your screen image degrade or disappear.
- They erase files from your hard disk
- They send files from your computer at random to people in your e-mail address book and, at the same time, transfer the virus to them.
- They overwrite part of files.

The list goes on. In fact, almost anything bad that you can think of that can happen to your computer (apart from hardware failure) can be triggered by a virus. An effective way to control this si to add a firewall to your system.

HOW DO VIRUSES ARRIVE ON YOUR SYSTEM?

If you never connect to the Internet and never accept removable disks from anyone else, you should remain virus-free, particularly as it is reasonable to expect that commercial software does not contain viruses. However, you should not be complacent, and anyway, if your system remains sterile, then you are missing a lot of the advantages of having a computer, whether for business or leisure.

Viruses are transmitted to your system by transferring files onto it. This may be by transferring them from external media, but most commonly today, viruses are transferred within e-mail messages.
A third way that viruses can be transmitted is via World Wide Web. Many web pages are now much more than simple files containing text and figures; they may well include programs or scripts that can contain viruses. If you use the Web, you need anti-virus software that detects any viruses arriving by this method.

Criminalità informatica

I cambiamenti radicali nelle comunicazioni interpersonali e il costante incremento dell'utilizzo delle tecnologie informatiche in settori fondamentali della società, quali il lavoro, la pubblica amministrazione, la ricerca scientifica, hanno reso necessaria una modifica normativa che tutelasse questo complesso sistema telematico.

TIPOLOGIE DI REATO E SANZIONI DEI PRINCIPALI CRIMINI INFORMATICI

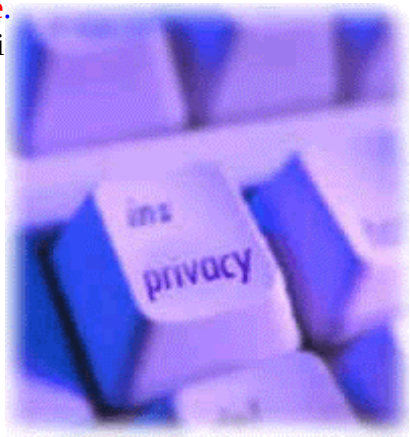
Di seguito vengono elencati alcuni reati contemplati dalla legge 547/93:

- Attentati a impianti di pubblica utilità. L'articolo 420 punisce chiunque commetta un fatto volto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità (ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti). La pena è più grave se dal fatto deriva la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione (anche parziale) del funzionamento del sistema. Ad esempio, il danneggiamento o la distruzione dei sistemi informatici di ospedali, caserme, ministeri è punito con la reclusione da 2 a 4 anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione (anche parziale) del funzionamento del sistema, la pena è la reclusione da 3 a 8 anni.
- Accesso abusivo a un sistema informatico o telematico (strettamente legato agli aspetti di riservatezza dei dati). L'articolo 615 ter punisce chiunque si introduca in un sistema informatico o telematico protetto da misure di sicurezza (ovvero vi si mantenga all'interno contro la volontà espressa o tacita di chi ha il diritto di escluderlo). È il reato tipico degli hacker che attraverso la rete telefonica riescono a penetrare in diversi sistemi informatici collegati alla rete stessa. L'accesso abusivo ad una banca dati protetta da misure di sicurezza (codici d'accesso, password, chiavi elettroniche ecc) ad esempio, comporta pene fino a 8 anni di reclusione;

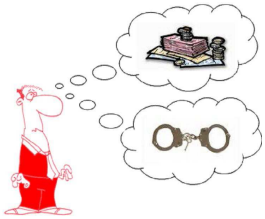
- Detenzione o diffusione abusiva di codici d'accesso a sistemi informatici o telematici. L'articolo 615 quater punisce chiunque, al fine di procurare a se o a altri un profitto o di arrecare a altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o

telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo;

- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. L'articolo 615 quinquies punisce chiunque diffonda, comunichi o consegni un programma informatico da lui stesso a da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento. Per la diffusione di virus informatici si rischia la reclusione sino a 2 anni e una sanzione pecuniaria;
- Violazione, sottrazione e soppressione di corrispondenza. Premesso che per corrispondenza si intende anche quella informatica o telematica, l'articolo 616 del codice penale punisce chiunque prenda cognizione del contenuto di una corrispondenza a lui non diretta, ovvero sottragga o distragga al fine di prenderne o farne prendere cognizione ad altri una corrispondenza a lui non diretta, ovvero del tutto o in parte la sopprima o distrugga. Questo ha valore anche per la lettura fraudolenza di e-mail. Tali reati sono puniti con la reclusione fino a 3 anni nel caso più grave.
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. L'articolo 617 quarter punisce chiunque fraudolentemente intercetti comunicazioni relative a un sistema informatico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. È ugualmente punito chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico in tutto o in parte il contenuto delle comunicazioni.
- Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche. L'articolo 617 quinquies punisce chiunque, fuori casi consentiti dalla legge, installi apparecchiature atte a intercettare, impedire, interrompere comunicazioni relative a un sistema informatico o intercorrenti tra più sistemi; tale comportamento sanzionato dal codice penale prevede la reclusione da 1 a 4 anni.



- Falsificazione, alterazione soppressione dal contenuto di comunicazioni informatiche o telematiche. L'articolo 617 sexies punisce chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altrui danno, formi falsamente ovvero alteri o sopprima, in tutto o in parte, il contenuto, anche occasionalmente intercettato, delle comunicazioni.
- Danneggiamento di sistemi informatici o telematici. L'articolo 635 bis punisce chiunque distrugga, deteriori o renda, in tutto o in parte, inservibili sistemi telematii o informatici altrui, ovvero programmi, informazioni o dati altrui.
- Frode informatica. L'articolo 640 ter punisce il reato di frode informatica. La frode informatica può realizzarsi attraverso l'alterazione del "funzionamento informatico o telematico" ovvero con l'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi. La pena può prevedere la reclusione fino a 5 anni.



- Duplicazione ai fini di profitto. È punito chiunque abusivamente duplichi, per poi trarne profitto programmi per elaboratore, o importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

Il criminale informatico e il suo raggio d'azione

TIPO DI CRIMINE	RIFERIMENTO LEGISLATIVO	CONSEGUENZE SOCIALI	OGGETTO DELLA TUTELA
Intrusioni informatiche con varie finalità (curiosità, spionaggio, operazioni economiche)	L. 547/93 art. 615 C.P.	La vittima prova disagio e vergogna, diffidenza verso i propri colleghi.	Sicurezza delle operazione, dei dati e delle informazioni personali.
Truffe a compagnie telefoniche	L. 547/93 art 640 C.P	Scarsa percezione del crimine. Diffidenza dei clienti verso le compagnie stesse.	Attività economica svolta dalle compagnie
Duplicazione e traffico illecito di software	L. 518/92	Aumenta la difficoltà nel percepire tale costume come reato, aumentano i controlli a sorpresa.	Attività economica degli sviluppatori delle software house.
Attentato alla rete o ai singoli sistemi tramite virus	L. 547/93 art 615 C. P.	Maggiore attenzione ai contatti tramite la rete,la provenienza dei programmi,; sviluppo del mercato degli anti-virus	Tutto ciò che danneggia il virus.
Installazione e/o utilizzo di strumenti per intercettare, registrare, impedire, modificare comunicazioni informatiche o telematiche	L. 547/93 art 617 C.P. (e altri)	Diffidenza verso qualsiasi comunicazione telematica, richi per la privacy e per la sviluppo di alcuni servizi in rete.	Sicurezza delle operazioni, dei dati e delle informazioni personali.

L'Home Banking

Con l'Home banking, anche detto banca online o banca via internet vengono indicate le operazioni bancarie effettuate dai clienti degli istituti di credito tramite una connessione remota con la propria banca, funzionalità resasi possibile con la nascita e lo sviluppo di Internet e delle reti di telefonia cellulare. Sotto il generico titolo di home banking sono infatti ricompresi sia servizi bancari di internet banking - che implicano una connessione con l'istituto bancario per mezzo di una rete informatica e tramite appositi portali web - che quelli di mobile banking - per i quali l'accesso avviene tramite reti GSM, GPRS e UMTS - come anche il phone banking che permette l'accesso ai servizi bancari per mezzo della rete di telefonia fissa e, solitamente, tramite l'utilizzo di sistemi di Interactive Voice

Response o di operatori di call center. Esso è uno dei fenomeni più interessanti di questo fine millennio, è un servizio delle Banche rivolto in particolar modo alle famiglie.
Letteralmente significa "la banca in casa", praticamente consiste nella possibilità di usufruire dei più svariati servizi bancari, senza doversi recare appositamente in banca, ma utilizzando semplicemente il PC installato nella propria abitazione.
In altre parole, non solo non è più necessario recarsi allo sportello per domandare all'impiegato informazioni relative ai propri risparmi, ma è possibile: leggere con più calma le condizioni dei diversi contratti; ottenere informazioni sul conto corrente; effettuare pagamenti di utenze; effettuare girofondi, nonché la possibilità di utilizzare il servizio di posta elettronica.

L'introduzione di questo sistema, oltre ad interessare le banche già esistenti, ha recentemente permesso la nascita di banche totalmente on-line (conti on-line "puri") per le quali le operazioni bancarie possono essere effettuate esclusivamente on-line (tali istituti di credito non possiedono, cioè, sportelli aperti al pubblico): queste ultime praticano condizioni d'interesse spesso migliori rispetto a quelle praticate sui conti correnti delle banche "tradizionali" e con costi di tenuta conto pari, o prossimi, allo zero. Ciò è reso possibile dall'abbattimento dei costi lavorativi e delle infrastrutture necessarie all'attività bancaria.
L'adozione di sistemi di home banking ha portato vantaggi sia alle banche che ai clienti degli istituti di credito: per la banca l'adozione di tali servizi comporta l'allargamento del target di clientela, potendo estendere i propri servizi anche all'estero, nonché una riduzione dei costi lavorativi; i clienti beneficiano invece della maggior comodità (accesso non geograficamente né temporalmente limitato) dei servizi di home banking e del loro minor costo rispetto ai servizi off-line.
Questo tipo i servizio va a vantaggio soprattutto di coloro che compiono un numero elevato di operazioni bancarie, ma oggigiorno avvantaggia anche il piccolo risparmiatore.
Infatti, divenendo più semplice e veloce la valutazione dei servizi e dei tassi offerti dalle diverse banche, anche la relativa scelta di affidare i propri risparmi ad una o ad un'altra agenzia, essendo fatta in base alla convenienza, attiverebbe un meccanismo concorrenziale che permetterebbe, da un lato l'abbassamento dei tassi, e dall'altro l'adozione, da parte delle banche stesse, di comportamenti più corretti nei confronti dei propri clienti. La Banca ,per contro, beneficia di tale servizio per il fatto di ridurre i costi del personale, nonché di godere di supporti elettronici.
Oggi sembra che tutte le banche si stiano preparando a questa importante rivoluzione, ed hanno quindi approntato siti Internet.

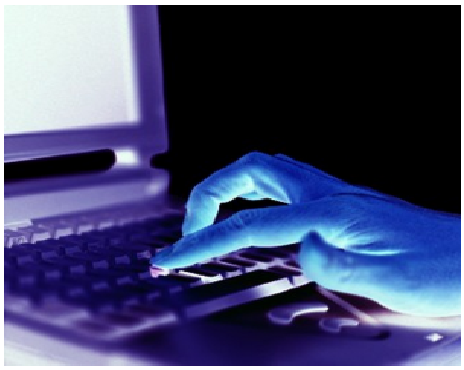
Alcuni dei servizi di home banking attualmente più diffusi sono:
Visione dell'estratto conto
Bonifici bancari on-line
Operazioni di ricarica del cellulare
Pagamenti on-line

Quali sono i vantaggi di un conto online?

I conto online permettono di effettuare interrogazioni e disposizioni in qualunque momento della giornata e non soltanto durante i normali orari di apertura della filiale.
Le operazioni disposte con l'home banking, inoltre, comportano commissioni inferiori rispetto a quelle effettuate in filiale, perché non richiedono l'intervento dell'operatore allo sportello.

L'home banking è pericoloso ?

Le banche offrono la massima sicurezza per l'home banking
Le informazioni relative al tuo conto sono riservate e protette da uno o più codici segreti, che dovrai inserire per accedere alla tua area riservata nel sito Internet della banca. Per effettuare disposizioni in genere è previsto un ulteriore "codice dispositivo". In alternativa o aggiunta al codice dispositivo, inoltre, alcune banche prevedono l'utilizzo di "chiavi di sicurezza" per le singole operazioni.



I codici vengono forniti in un'unica copia dalla tua banca nel momento in cui attivi un conto on line o le funzioni di home banking sul conto corrente tradizionale.

Come ci si può tutelare dalle truffe e dagli hacker?

Bisogna evitare di rispondere a qualunque e-mail che richieda l'inserimento di dati riservati, codici o informazioni personali: la banca non ti chiederà mai alcun dato via e-mail, perché si attiene alla massima riservatezza e sicurezza. Inoltre, ricordati di non cliccare su link che si trovano in e-mail sospette.

Decalogo della sicurezza

Con qualche piccola attenzione è possibile riconoscere le truffe che arrivano via e-mail e gli altri stratagemmi escogitati dai pirati informatici per carpire informazioni sui nostri conti on line.

Ecco un breve decalogo di regole da seguire per dormire sonni tranquilli:

1. **Diffida di qualunque e-mail ti richieda l'inserimento di dati riservati** riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o informazioni personali. La tua banca, infatti, non richiederà mai tali informazioni via e-mail.
2. **Le e-mail truffaldine di solito non sono personalizzate** e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (come scadenza, smarrimento, problemi tecnici eccetera); fanno uso di toni "intimidatori" (per esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente); promettono remunerazione immediata a seguito della verifica delle proprie credenziali di identificazione; non riportano una data di scadenza per l'invio delle informazioni.
3. **Nel caso in cui tu riceva e-mail con richieste di questo tipo, non rispondere** ma informa subito la tua banca tramite il call center o recandoti in filiale.
4. **Non cliccare su link presenti in e-mail sospette**, in quanto questi collegamenti potrebbero condurti a un sito contraffatto, difficilmente distinguibile dall'originale. Diffida inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, in particolare quelli con il simbolo @.
5. **Quando inserisci dati riservati in una pagina web, assicurati che si tratti di una pagina protetta**: queste pagine sono riconoscibili in quanto l'indirizzo comincia con "https://" e

non con “http://” e nella parte in basso a destra della pagina è presente un lucchetto. Per controllare l’autenticità della connessione sicura puoi fare doppio click sul lucchetto in basso a destra e verificare la correttezza delle informazioni di rilascio e validità che compaiono per il relativo certificato digitale.

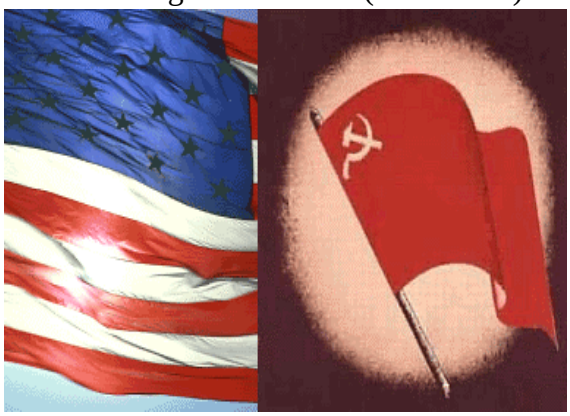
6. **Diffida se improvvisamente cambia la modalità con la quale ti viene chiesto di inserire i codici di accesso all’home banking**: per esempio se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (nuove finestre). In questo caso, contatta la vostra banca tramite il call center o recandoti in filiale.
7. **Controlla regolarmente gli estratti conto del conto corrente e della carta di credito** per assicurarti che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contatta la banca e/o l’emittente della carta di credito.
8. **Le aziende produttrici dei browser (i programmi che permettono di navigare in Internet) permettono di scaricare gratuitamente gli aggiornamenti del software (le patch) che incrementano la sicurezza** dei browser stessi. Sui siti di queste aziende è anche possibile verificare che il tuo browser sia aggiornato; in caso contrario, ti consigliamo di scaricare e installare le patch appena si rendono disponibili.

9. **Tieni sempre aggiornato il software antivirus**. In questo modo impedirai a e-mail o siti di phishing di installare sul computer , senza che tu te ne accorga, un “codice malevolo” atto a carpire le informazioni personali in un secondo momento, attivandosi nel momento in cui vengono digitate. Usa inoltre un software firewall per proteggere il traffico in entrata e in uscita dal tuo PC.
10. **In caso di dubbio, rivolgiti alla tua banca!**

La guerra fredda

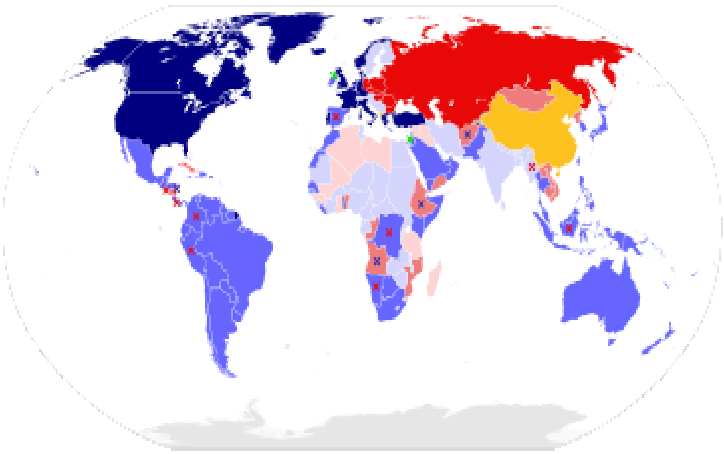
GUERRA FREDDA; IDEOLOGIE CONTRAPPOSTE

Fu definita guerra fredda (1945-1990) la contrapposizione che venne a crearsi alla fine della seconda guerra mondiale tra due blocchi internazionali, generalmente distinti come Ovest (gli Stati Uniti d'America, gli alleati della NATO ed i Paesi amici) ed Est (l'Unione Sovietica, gli alleati del Patto di Varsavia ed i Paesi amici). Questa fase di contrapposizione e di tensione politica tra due mondi si caratterizzò dalla radicalità ideologica, ma anche dalla scelta di evitare scontri militari globali, soprattutto dal momento in cui si verificò la condizione di equilibrio nucleare.

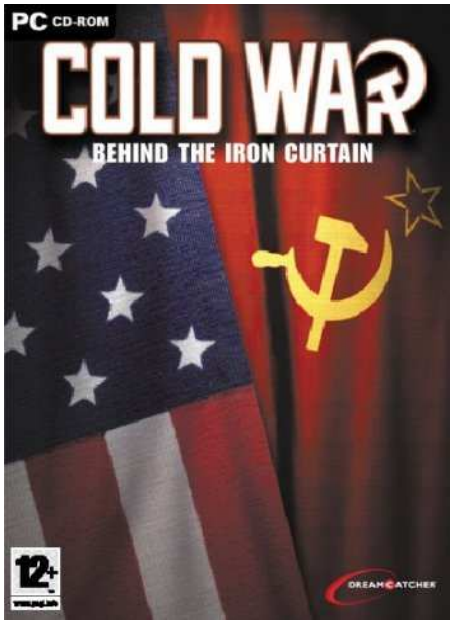


Tale tensione, durata circa mezzo secolo, pur non concretizzandosi mai in un conflitto militare diretto, da questo punto deriva infatti il termine metaforico “guerra fredda”, si sviluppò nel corso degli anni su vari campi: militare, spaziale, ideologico, psicologico, tecnologico, sportivo. Vi furono aggressive guerre di propaganda tra i blocchi USA e URSS: l'Est criticava l'Ovest in quanto promotore del capitalismo borghese e dell'imperialismo, che marginalizzano i lavoratori, mentre

l'Ovest criticava l'Est definendolo "impero del male", incarnazione di un totalitarismo antidemocratico sotto forma di dittatura comunista.
La guerra fredda si protrasse dalla fine della seconda guerra mondiale, fino al collasso dell'Unione Sovietica, nei primi anni novanta. Solo in alcune occasioni la tensione tra i due schieramenti prese la forma di conflitti armati, come la guerra di Corea, le guerre in Africa, la Guerra del Vietnam, l'invasione sovietica dell'Afghanistan e gli scontri in centro America.



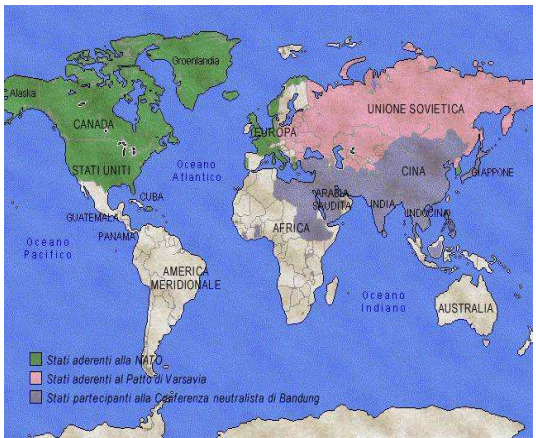
I due schieramenti nel 1980.
- NATO
- Altri alleati degli Stati Uniti
- × Gruppi armati anticomunisti
- Patto di Varsavia
- Paesi socialisti allineati con l'URSS
- Altri alleati dell'URSS
- × Gruppi armati comunisti
- Cina Popolare e suoi alleati
- Non allineati
- × Altri conflitti



SPIONAGGIO

Gran parte della guerra fredda si svolse soprattutto attraverso, o contro, “nazioni surrogate” e per mezzo di spie e traditori che lavoravano sotto copertura. In questi conflitti, le potenze maggiori operavano in buona parte armando o sovvenzionando i surrogati. La guerra fredda comprese anche un conflitto nascosto, portato avanti attraverso atti di “ESPionage” (“spionaggio” in inglese dove “ESP” sta per “percezione extrasensoriale”). Oltre alle eliminazioni fisiche di agenti da entrambe le parti, la Guerra Fredda fu evidente nelle preoccupazioni riguardanti il possibile uso di armi nucleari e il fatto che la loro semplice esistenza fosse un deterrente sufficiente alla guerra**.**

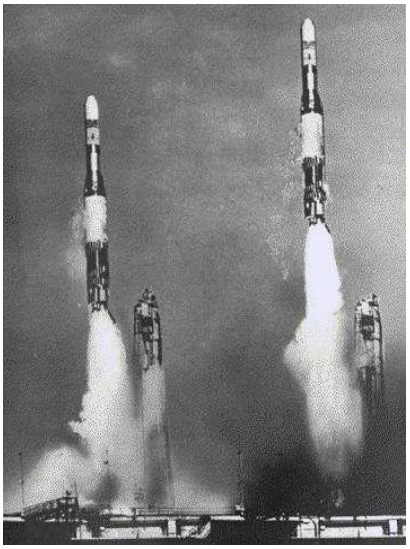
Gli eserciti delle nazioni coinvolte raramente presero parte alla guerra fredda in scontri diretti. Infatti, le maggiori potenze mondiali non entrarono mai in conflitto armato le une contro le altre. La guerra venne combattuta principalmente dai servizi segreti quali CIA (stati uniti) SIS (inghliterra), BND (Germania Ovest), Stasi (Germania Est) e KGB (Unione Sovietica). La guerra tra agenti, nello spionaggio tra obbiettivi civili e militari potrebbe aver causato la maggior parte delle vittime della Guerra Fredda. Gli agenti erano inviati nei paesi “avversari” sia dell’Est che dall’Ovest e le spie reclutate anche sul posto o costrette al servizio. Nel caso fossero state scoperte, venivano uccise immediatamente o scambiate con altri agenti.



Molte spie vendevano informazioni al nemico per denaro, ma tante altre erano mosse da sinceri motivi ideologici e ideali e in particolare dall'antifascismo e vedevano nel comunismo russo l'unico modo per combatterlo efficacemente. Gli aerei spia e altri apparecchi di ricognizione venivano immediatamente abbattuti al momento dell'individuazione. Durante la crescente minaccia della dominazione sovietica durante la Guerra Fredda, tanti autori documentavano un budget di 60-300 milioni di rubli spesi annualmente dallo stato sovietico per reclutare oltre agli scienziati, sensitivi, medium e individui dotati di capacità psicocinetiche e telepatiche arruolandoli con mansioni di "controspionaggio psichico" e di ricerca sulle applicazioni nella sicurezza nazionale. Questi erano gli scopi principali del KGB. Si è evidenziato che le conoscenze sovietiche in questo campo erano maggiori a quelle occidentali. Alcune organizzazioni temevano che i sovietici potessero guadagnare un aposizione di vantaggio nello spionaggio internazionale utilizzando personale "atipico", come ad esempio spie psichiche che avrebbero potuto leggere a distanza le intenzioni politiche ei leader statunitensi, o dei documenti segnalati "top secret" sulla locazione strategica di truppe e armamenti Usa.

LA CORSA AGLI ARMAMENTI

Nel conflitto strategico tra Stati Uniti e Unione Sovietica uno degli elementi principali fu la supremazia tecnologica come l'invenzione di armi d'inaudita potenza (Bomba H) o il progresso in campo spaziale. La guerra fredda si concretizzò di fatto nelle preoccupazioni riguardanti le armi nucleari; da entrambe le parti veniva l'auspicio che la loro semplice esistenza fosse un deterrente sufficiente a impedire la guerra vera e propria. In effetti non era da escludere che la guerra nucleare globale potesse scaturire da conflitti su piccola scala, e ognuno di questi aumentava le preoccupazioni che ciò potesse verificarsi. Questa tensione influì significativamente non solo sulle relazioni internazionali, ma anche sulla vita delle persone in tutto il mondo.



Durante tutta la guerra fredda gli arsenali nucleari delle due superpotenze vennero costantemente aggiornati ed ingranditi fino ad arrivare agli ultimi anni del conflitto (1979-1989), nei quali vennero negoziati una serie di accordi, denominati accordi START, che portarono a sostanziali riduzioni del numero di ordigni. Ma la contrapposizione tra una corsa al riarmo apparentemente irrefrenabile e continui tentativi di controllo degli armamenti negoziati tra USA ed URSS o nell'ambito dell'ONU fu costante.

Furono necessarie molte attenzioni e una buona dose di diplomazia per sedare sul nascere alcuni conflitti armati, al fine di prevenire una "guerra calda" che avrebbe rischiato di estendersi e intensificarsi.

L'EVOLUZIONE DELLA GUERRA FREDDA A OGGI

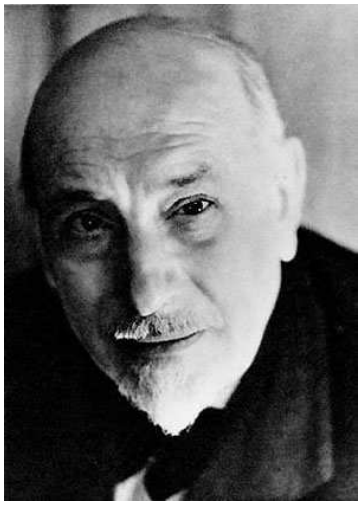
Oggi, il controllo dello spazio elettronico può assicurare l'egemonia mondiale. La nuova Guerra Fredda si combatte sul web: da una parte c'è Washington, con i suoi alleati occidentali, dall'altra Pechino, che ha scelto il cyber spionaggio per rovesciare l'antica supremazia americana. Un conflitto non convenzionale, affidato agli

strumenti più sofisticati che la moderna tecnologia mette a disposizione dell'intelligence. Hacker e cracker: sono loro i soldati del nuovo millennio, essi sono capaci di penetrare in siti protetti, rubare o distruggere informazioni riservate. L'ultimo attacco ha puntato in alto: i pirati informatici sono riusciti a copiare molti terabyte di dati relativi al design dei sistemi elettronici del «Joint Strike Fighter», il super bombardiere che rappresenta il più costoso progetto militare degli Stati Uniti.
La mole di sabotaggi, attacchi o incidenti informatici su reti classificate e non di istituzioni o enti governativi è in continua crescita. Il problema, d'altra parte, è intrinseco all'inevitabile progresso della società moderna: «si è creata una dipendenza da Information Technology e, dunque, un aumento della vulnerabilità dei singoli paesi, ovvero una crescita della potenzialità della minaccia». L'avvento di nuove tecnologie ha creato altre forme di potere. «Lo sviluppo di internet ha segnato l'inizio di un nuovo capitolo della storia del terrorismo. Sono nati i cosiddetti Tvo (Terroristic Virtual Organization), organizzazioni virtuali i cui membri reali sono dislocati sull'intero globo e possono condurre azioni terroristiche in tempi molto rapidi, dopo avere ricevuto l'ordine di procedere. E la domanda a cui i singoli paesi, la Nato, l'Unione europea, tutti gli organismi internazionali devono dare risposta è se un cyber attacco rappresenti davvero, e sempre, un atto di guerra.

Gli Stati membri dell'Alleanza atlantica hanno concordato sulla necessità di una maggiore collaborazione: a questo scopo, su impulso di sette paesi tra cui l'Italia, è stato creato il Cooperative Cyber Defence Centre of Excellence, il cui obiettivo è quello di addestrare i tecnici della Nato contro possibili «minacce informatiche». Un gruppo di 30 esperti opera a Tallin, in Estonia. E la scelta non è stata certo casuale: proprio le istituzioni pubbliche e private di questo paese furono colpite nel mese di maggio del 2007 da un attacco che per tre settimane paralizzò le infrastrutture informatiche nazionali.
Gli Stati Uniti hanno ammesso più volte di essere stati sotto attacco informatico. Fonti del Pentagono e dei servizi di intelligence hanno chiamato in causa la Russia e la Cina. A scopo difensivo è nato il Joint Functional Component Command for Network Warfare, il team di super hacker ed esperti informatici provenienti dalla agenzie di difesa e forze armate. L'obiettivo è quello di provare a contrastare l'attuale supremazia di cyber esperti d'Oriente, cinesi e indiani soprattutto; il timore è che molto presto gli hacker di Pechino sapranno essere in grado di condurre un attacco capace di bloccare completamente tutte le centrali elettriche americane.

Luigi Pirandello

Cenni biografici



Luigi Pirandello nasce ad Agrigento in una tenuta paterna detta "il Caos", da Stefano Pirandello, garibaldino durante la spedizione dei Mille, e da Caterina Ricci-Gramitto, sposata nel 1863, sorella di un suo compagno d'armi, di famiglia tradizionalmente antiborbonica. Frequentata la scuola nella città natale fino al secondo anno presso l'Istituto Tecnico, dal 1880 lo troviamo a Palermo dove frequenta gli studi liceali e dove la famiglia si era trasferita dopo un dissesto finanziario. Conseguita la licenza liceale si iscrive contemporaneamente sia alla Facoltà di Legge che a quella di Lettere dell'Università di Palermo e nel 1887 si trasferisce alla Facoltà di Lettere dell'Università di Roma, dalla quale è costretto, dopo un diverbio con il preside della Facoltà e docente di Latino Onorato Occioni, ad allontanarsi. Si iscrive, allora, all'Università di Bonn dove si reca con una lettera di presentazione del Professore di filologia romanza Ernesto Monaci. A Bonn all'inizio del mese di gennaio 1890, conosce a una festa da ballo in maschera Jenny Schulz-Lander, alla quale dedica il suo secondo volume di poesie, dal titolo Pasqua di Gea, una ragazza di cui si innamora e che rivestirà una parte importante nella sua vita anche sul piano spirituale, in quanto gli rimarrà per sempre dentro l'amarezza di un amore non realizzato, l'unico vero della sua giovinezza. Si laurea nel 1891 con una tesi su Suoni e sviluppi di suono della parlata di Girgenti. Nello stesso anno rientra in Italia e si stabilisce a Roma con un assegno mensile ottenuto dal padre. Nel 1894 sposa Maria Antonietta Portolano, figlia di un socio del padre, e l'anno seguente nasce il primo figlio, Stefano. Dopo le prime opere di poesia, scritte in Germania, a Roma comincia a collaborare a giornali e riviste con articoli e brevi studi critici e nel 1897 accetta l'insegnamento presso l'Istituto Superiore di Magistero femminile di Roma. Nel 1897 e nel 1899 gli nascono i figli Rosalia e Fausto. Il 1893 è un anno particolarmente difficile, perché un allagamento nella miniera di zolfo del padre, nella quale aveva investito la dote patrimoniale della moglie, provoca il dissesto finanziario suo e del padre insieme ai primi segni della malattia mentale della moglie, che si aggraverà sempre di più fino ad essere ricoverata in ospedale. Nel 1901 pubblica il romanzo L'esclusa e nel 1902 Il turno; nel 1904 ottiene il primo vero successo con Il fu Mattia Pascal. Nel 1908 diventa ordinario dell'Istituto superiore di Magistero, risolvendo in parte i suoi problemi economici, e pubblica due importanti saggi: L'umorismo e Arte e Scienza, che scateneranno un contrasto molto vivace con Benedetto Croce che si protrarrà per molti anni. Nel 1909 pubblica il romanzo I vecchi e i giovani e l'anno seguente rappresenta i suoi primi lavori teatrali: La morsa e Lumie di Sicilia.. Nel frattempo continua a scrivere e pubblicare novelle che assumeranno il titolo generale di Novelle per un anno. Il 1915 è uno degli anni più tristi della vita di Pirandello sia per l'entrata in guerra dell'Italia e per il figlio Stefano che parte volontario per il fronte, dove abbastanza presto verrà fatto prigioniero, sia per la morte della madre, verso la quale nutriva un sentimento non solo di amore filiale, ma anche di partecipazione ai suoi intimi segreti dolori, causati da un carattere troppo 'vivace' del marito. Col 1916 comincia la vera stagione teatrale pirandelliana con Pensaci, Giacomino!, Liolà e La ragione degli altri, alle quali seguiranno Così è, se vi pare (1917), Il berretto a sonagli, Il piacere dell'onestà, La patente, Il giuoco delle parti, Ma non è una cosa seria, Tutto per bene, La Signora Morli uno e due, fino ai Sei personaggi in cerca d'autore, del 1921, opera rappresentata da Dario Niccodemi, scatenando violenti contrasti nel pubblico alla prima ma altrettanti consensi già dalla seconda messa in scena, Enrico IV del 1922, Vestire gli ignudi (1922), Ciascuno a suo modo (1924), ecc. Nel 1926

pubblica l'ultimo romanzo, Uno nessuno centomila e fonda a Roma, insieme al figlio Stefano, Orio Vergani e Massimo Bontempelli il Teatro d'arte, nel quale debutterà Marta Abba, giovanissima interprete che diverrà musa ispiratrice di alcune commedie, scritte appositamente per lei, con la quale Pirandello stabilirà un rapporto d'affetti che durerà per tutta la vita. Nel 1934 riceve a Stoccolma il premio Nobel per la Letteratura. Muore nel 1936, il 10 dicembre e le sue ceneri verranno tumulate in una roccia nella tenuta del Caos nella quale era nato 68 anni prima.

I quaderni di Serafino Gubbio

Il romanzo e il suo contesto storico

I quaderni di Serafino Gubbio operatore sono sette e scandiscono le pagine di un diario immaginario, scritto a cose già avvenute. Chi scrive è un operatore cinematografico, Serafino Gubbio, soprannominato Si gira, il quale vuole vendicarsi delle macchine che lo hanno ridotto a una mano che gira una manovella, scrivendo, dal suo punto di vista, le vicende della troupe impegnata nella produzione di un film per la casa cinematografica Kosmograph. Il racconto, si apre con l'arrivo a Roma di Serafino, ospite la prima notte di uno strano tipo di filosofo, Simone Pau, in un ospizio di mendicità. Sono memorie che seguono il percorso di un individuo vittima della macchina da presa, mentre prende coscienza della sua alienazione. Della troupe fanno parte l'attrice Varia Nestoroff, figura esemplare delle nuove dive dello schermo, il regista Nino Polacco, amico intimo di Serafino, e altri attori ed addetti. L'incontro con la Nestoroff riporta alla mente di Serafino momenti del passato: è una donna fatale che ha tragicamente sconvolto la vita felice di due giovani, Giorgio Mirelli, morto suicida, e la sorella Duccella, da lui conosciuti nella paradisiaca "casa dei nonni" vicino a Sorrento. Un'altra vittima è Aldo Nuti, che aveva abbandonato la fidanzata Duccella per seguire la diva. Una storia che si complica nella tragedia finale, raccontata nel settimo quaderno: il film sta per essere terminato, si sta preparando la scena finale dell'uccisione della tigre, feroce e innocente incarnazione della natura. Nella gabbia, dentro la quale è stata ricostruita la giungla, vengono fatti entrare Nuti e Gubbio, l'uno con il fucile, l'altro con la macchina da presa. Attori e tecnici assistono alla scena finale attorno alla gabbia: appena entra la tigre, "si gira". Ma ecco che accade l'imprevisto che trasforma la scena di finzione in scena reale: Nuti, anziché colpire la tigre, volge l'arma contro la Nestoroff che sta assistendo alla scena e la uccide, mentre la tigre si avventa su di lui e lentamente lo sbrana. È qui il punto centrale del romanzo: Serafino è talmente alienato dalla macchina che, impassibile come un automa, continua a girare la scena, in una sorta di raggelante identificazione con la macchina. Il sesto romanzo pirandelliano nasce alla vigilia della prima guerra mondiale, nel 1914 e viene pubblicato per la prima volta su di una rivista letteraria, "Nuova Antologia", e poi in un volume nel 1916 con il titolo "Si Gira"; successivamente, nel 1925, riveduto e corretto appare con un nuovo titolo: "I quaderni di Serafino Gubbio operatore". Sono gli anni del Futurismo, che al netto rifiuto della tradizione univa l'esaltazione della vita moderna e dei suoi aspetti più caratteristici: la velocità, le macchine, le nuove metropoli e i complessi industriali. Tali principi vennero elaborati per la prima volta dal poeta italiano Filippo Tommaso Marinetti, che nel Manifesto del futurismo del 1909 sostituiva alla vittoria di Samotracia, quale nuovo ideale estetico, l'immagine della "automobile in corsa con il suo cofano adorno di grossi tubi simili a serpenti dall'alito esplosivo" mentre, nel 1912 il Manifesto tecnico della letteratura futurista, redatto da Boccioni, Balla, Russolo, Carrà e Severini, era dettato a Marinetti dall'elica turbinante di un aeroplano. Nell'ambito della situazione politica, culturale ed economica italiana, il futurismo rappresenta quindi la fase più clamorosa della subordinazione della letteratura all'industria

capitalista, l'esito estremo delle correnti letterarie spiritualistiche, nazionaliste che presupponevano la negazione dei valori umani: valori che non l'industrializzazione in sé svalorizza ma l'industrializzazione capitalista. La negazione del passato della storia, l'odio contro ogni forma espressiva tradizionale, il disprezzo della bellezza classica a vantaggio di una nuova bellezza meccanica, sono gli elementi mediante i quali i futuristi intendono negare all'arte ogni diritto di rappresentare l'uomo nelle sue reali aspirazioni individuali e sociali. Il mito della macchina, del progresso meccanico, rappresenta la costante di una letteratura incapace di osservare realisticamente questo progresso nel quadro generale del progresso sociale. Il tema delle fabbriche, delle macchine, dell'elettricità è certamente uno dei prediletti dei futuristi, ma non si tratta solo di una scelta di contenuti: i futuristi affermano, e realizzano, l'antropomorfizzazione della macchina, la vedono in sembianze e le attribuiscono sentimenti umani: la mitragliatrice è paragonata ad una bella donna, poi ad un tribuno, quindi ad un trapano, a un laminatoio, a un tornio elettrico, a un cannello ossidrico. Ma, d'altra parte, nel futurismo è anche l'uomo a trasformarsi in macchina, sono i suoi sentimenti ad essere espressi con termini presi dalla fraseologia dell'industria: l'uomo ansima come dynamo, i nervi sono paragonati a cavi dell'alta tensione, l'anima grida come un cuore d'acciaio, si protende come un elemento di macchina. Nella struttura e nelle proporzioni del racconto futurista il funzionamento meccanico della nuova civiltà non deve venire intralciato dall'elemento umano; l'uomo non sarà che una rotella nel gigantesco corpo della macchina. E' il ripudio del neoclassico a favore del moderno. Pirandello invece nutre per le macchine una profonda diffidenza. È proprio sulla insistita polemica vita/macchina che si aprono i Quaderni di Serafino, ridotto dalla sua professione ad essere esclusivamente "una mano che gira una manovella". L'alienazione di un uomo depauperato di vita e di creatività nel farsi servitore di macchinari è il nucleo intorno a cui ruotano le riflessioni di questo io narrante, più interessato a seguire il suo filo teorico/meditativo che a raccontarci la storia di amore e morte presa a pretesto di narrazione. Siamo, con la prima edizione del romanzo, nel 1915: le macchine che incombono nella nostra vita sono quelle belliche, in una atmosfera pervasa da fremiti futuristi. Il presagio di Pirandello è quello di una Terra devastata dalla follia distruttiva dell'uomo/macchina e ancor di più, il presentimento che, forse, proprio questo esito apocalittico possa essere l'unica via rigeneratrice dell'essere uomo: "mi domando se veramente tutto questo fragoroso e vertiginoso meccanismo della vita, che di giorno in giorno sempre più si complica e s'accelera, non abbia ridotto l'umanità in tale stato di follia, che presto proromperà frenetica a sconvolgere e a distruggere tutto. Sarebbe forse, in fin dei conti, tanto di guadagnato. Non peraltro, badiamo: per fare una volta tanto punto e a capo".