INTRODUZIONE

Gli attentati di Madrid dell' 11 marzo 2004 ci hanno dolorosamente ricordato che l'Europa è un obiettivo primario dei terroristi. Se le bombe rappresentano nel nostro subconscio collettivo la minaccia essenziale, la gamma di minacce che pesano sulle nostre società è molto più vasta.

Negli ultimi anni la Francia è entrata - senza rendersene necessariamente conto – nell'era della società dell'informazione. Tranne che sulla qualità degli uomini, la produzione della ricchezza nazionale si basa su una massa di informazioni giuridiche, finanziarie, commerciali, scientifiche, tecniche, economiche o industriali. Le minacce che pesano sul nostro strumento produttivo, si sono evolute anch' esse. Sono diventate più frequenti. L'esacerbazione della competizione internazionale trasforma le informazioni strategiche delle aziende in obiettivo di una vera e propria « guerra economica ».

D'altronde, i fondi di investimento pilotati dagli Stati, cercano di prendere i gioielli tecnologici stranieri. La tecnologia dell'informazione e della comunicazione diventa il cuore dell'economia della conoscenza, ma contiene difetti che la rendono vulnerabile alle intrusioni competitive .

Di fronte a quelle vulnerabilità che interessano tanto le aziende quanto lo Stato, quali sono state le azioni che quest'ultimo ha proposto ? Senza una guida politica decisa, sono stati fatti sforzi sparsi. Riguardo alla sicurezza dei sistemi informativi all'interno della Direzione centrale della sicurezza di informazione (DCSSI) del Segretariato generale della difesa nazionale, nel 2000 è stato creato un centro di censimento e trattamento degli attacchi informatici. Trattandosi del controllo degli investimenti stranieri nelle aziende francesi, la legge n. 2003-706 del primo agosto 2003 di sicurezza finanziaria ha rinforzato le prerogative del Ministro dell'economia.

Anche se l'intelligence economica è diventata oggetto di un importante dibattito in Francia, aprendosi a una moltitudine di iniziative,tuttavia, lo stato delle minacce che pesa sulla Francia, rimane allarmante : resta sempre urgente definire una strategia di sicurezza nazionale che comprenda sia obiettivi di difesa nazionale sia la protezione della nostra economia che la lotta contro le nuove minacce.

La nomina di un alto responsabile per l'intelligence economica è un primo passo. Tuttavia, resta necessario creare un Consiglio di sicurezza economica posto accanto al Presidente della Repubblica – come il Consiglio di sicurezza interna – responsabile della definizione di una strategia nazionale, basata sulla delimitazione di un perimetro strategico dell'economia francese. Quella politica verrà in seguito applicata da una Commissione alla tecnologia dell'informazione, della comunicazione e della sicurezza. Quella strategia deve, poi, basarsi sui fondi d' investimento con capitale pubblico e privato, destinati a condividere lo sforzo pubblico e privato allo scopo di conseguire l'indipendenza tecnologica della Francia.

La sicurezza nazionale è affare di tutti : cittadini, aziende e governi. Come ricorda Nicolas Sarkozy, -allora Ministro dell'interno - durante la quattordicesima sessione nazionale dell'Istituto di Studi Avanzati della sicurezza interna, nell' ottobre 2002 :

« Naturalmente non c'è da una parte lo Stato e dall'altra le aziende, ognuno ad assicurarsi la sicurezza per conto suo. Al contrario, per poter affrontare la cyber-criminalità, per garantire la sicurezza delle transazioni finanziarie e delle borse, ma anche per prevenire le minacce riguardo gli impianti nucleari, il trasporto di materiali pericolosi o la sicurezza di telecomunicazione, dobbiamo lavorare tutti quanti insieme. Lo Stato si assume il suo ruolo per sintetizzare, coordinare e definire le strategie ».

La forza del tessuto economico e la nostra coesione sociale si preserveranno solo a costo di uno sforzo nazionale ed europeo.

I.- LE VULNERABILITA' FRANCESI

In un'economia la cui ricchezza si basa sempre di più sul sapere, le informazioni strategiche delle aziende francesi non sembrano essere protette a sufficienza. Per di più la vulnerabilità dei sistemi informatici mettono in pericolo la forza economica del nostro paese.

1.Le minacce giuridiche

In Francia il segreto economico non è garantito a sufficienza a differenza che in America.Se gli Stati Uniti hanno saputo acquisire un diritto commerciale che protegge efficacemente e pragmaticamente il segreto economico, quest'ultimo in Francia risulta poco ben definito e quindi vulnerabile.La legge federale, denominata Economic Espionage Act oppure Cohen Act, garantisce la protezione delle aziende e delle persone contro il furto del segreto commerciale reprimendo pesantemente i trasgressori. Essa permette di sanzionare chiunque abbia l'intenzione di deviare un segreto commerciale nell'interesse economico di una persona diversa dal proprietario, sapendo che il reato nuocerà al proprietario di questo segreto. Tale dispositivo penale protegge il segreto commerciale, definito d'altronde come « ogni genere di informazione finanziaria, commerciale, scientifica, tecnica, economica, industriale, compresi modelli, piani, compilazioni, meccanismi, formule, disegni, prototipi, metodi, tecniche, processi, procedure, programmi o codici, sia in forma materiale o immateriale, sia non memorizzata, non compilata o memorizzata fisicamente, elettronicamente, graficamente o per iscritto ».

Al contrario in Francia le informazioni sensibili delle aziende sono protette solo da un insieme di testi, la cui coerenza e l'efficacia sono imperfette.

Solo l'articolo 410-1 del codice penale costituisce allo stato attuale un contributo rilevante nel contesto della sicurezza economica. Esso precisa che gli interessi fondamentali della nazione « accettano (…) la sua indipendenza, la integrità del suo territorio, della sua sicurezza, (…) e gli elementi essenziali del suo potenziale scientifico ed economico e del suo patrimonio culturale ». Questo concetto purtroppo non risulta operativo contro le minacce attuali contro il patrimonio conoscitivo francese. D'altra parte le aziende francesi-sottolinea Carayon- sono a volte vittime delle procedure giuridiche straniere.Le commissioni rogatorie internazionali (CRI) condotte sul nostro territorio da un'autorità giuridica straniera possono condurre, in modo indiretto, a una raccolta illecita di informazioni. In effetti, a volte succede che i documenti senza un collegamento con la procedura giudiziaria in corso ma comprendenti delle informazioni sensibili che possono compromettere processi industriali, siano sequestrati in occasione dell' esecuzione di una CRI contro delle società francesi.

2.Le minacce finanziarie

Il caso Saft, Eutelsat e Gemplus che sono stati obiettivo di tentativi o acquisizioni di fondi di investimento statunitense, illustrano la vulnerabilità del capitale di imprese strategiche francesi ed europee. I fondi di investimento spesso mostrano una preferenza per le società non quotate, come sono in genere le imprese tecnologiche in fase di maturazione.

Infatti i fondi di investimento sostengono la strategia di potere degli Stati Uniti.
A sostegno della loro strategia di potere, gli Stati Uniti procedono con gli investimenti diretti in società statunitensi e straniere tramite società di comodo. In pratica, si tratta di partecipazione da parte di imprese sotto il controllo delle agenzie di informazioni statunitensi al capitale di società innovative in tecnologie contenenti le applicazioni strategiche in termine di sicurezza. Il vantaggio di questa azione è molteplice perché permette :
- di promuovere la ricerca e lo sviluppo delle imprese statunitensi avendo competenze su nicchie tecnologiche per poter utilizzarle a beneficio della sicurezza nazionale;
- di garantire la sostenibilità delle PME avendo sviluppato una perizia strategica, per prevenire il rischio di acquisizione del potere da parte di una potenza straniera;
- di sostenere le PME innovative americane per stabilire la supremazia tecnologica degli Stati Uniti in relazione all'amministrazione responsabile per il sostegno dello sviluppo delle piccole e medie imprese (Small business administration).Di particolare interesse il il "modello" In-Q-Tel
In-Q-Tel è una società di capitale a rischio creata dalla CIA nel 1999.
Il suo obiettivo primario è quello di rilevare le tecnologie innovative che possono essere utilizzate dai servizi di intelligence. Una volta che si effettua il lavoro di individuazione dell'obiettivo, la missione di In-Q-Tel è quella di investire nelle società più avanzate o più promettenti nei settori selezionati.
La società di capitale a rischio funziona in relazione alle grandi organizzazioni americane di alta tecnologia, come Science Application International Corporation (SAIC).
Gli strumenti per la raccolta e le analisi dei dati (rispettivamente data mining e knowledge management) sono stati considerati essenziali dalla CIA. L'attentato a New York dell'11 settembre 2001 ha rafforzato l'interesse di In-Q-Tel da parte delle autorità statunitensi: questo evento, infatti, mise in luce i fallimenti del sistema informatico americano concentrato sulla raccolta di informazioni. Un rapporto del Congresso ha osservato che l'attività dell'azienda In-Q-Tel è giustificata e ciò che essa ha compiuto in così poco tempo è notevole.

3 Il controllo degli investimenti stranieri

Il diritto francese permette al Ministro dell'Economia di opporsi a investimenti esteri che potrebbero mettere in pericolo la sicurezza pubblica. Questo dispositivo è stato recentemente esteso a investimenti che potrebbero compromettere la difesa Nazionale.
Proprio per questa ragione il sistema francese è stato recentemente rafforzato
L'articolo L. 151-3 del Codice monetario e finanziario francese permette al ministro responsabile per l'economia, qualora constati che un investimento straniero potrebbe minare l'ordine pubblico, la salute pubblica, la sicurezza pubblica, o difesa nazionale di chiedere un autorizzazione

da imporre all'investitore.L'articolo L. 151-3 è stato recentemente modificato con l'articolo 78 della legge n 2003-706 del 1 ° agosto 2003 sulla sicurezza finanziara che ha aggiunto il tema di "difesa nazionale" all'elenco dei criteri che permette al ministro dell'Economia di sottoporre gli investimenti stranieri ad un'autorizzazione preventiva. Infatti, la nozione di pubblica sicurezza o di ricerca, produzione o commercio di armi, nel testo originale era troppo restrittiva per proteggere attività industriali che coinvolgono beni a duplice uso o l'area di componenti, che costituiscono elementi sensibili per la linea di produzione di apparecchiature strategiche.

Naturalmente la Francia non è l'unico stato ad avere una legislazione che mira a controllare gli investimenti stranieri per ragioni di difesa o di sicurezza in aziende nazionali sensibili. Con l'eccezione della Gran Bretagna,Canada e Paesi Bassi, tutti gli altri principali paesi industrializzati (compresi gli Stati Uniti, Spagna, Italia, Giappone e presto la Germania) hanno una legislazione che consente loro il controllo governativo, per motivi di sicurezza degli investimenti stranieri nel settore della difesa.
Negli Stati Uniti, la sezione 5021 dell' Omnibus Trade e Competitiveness Act del 1988, conferisce al Presidente la possibilità di bloccare o sospendere un progetto di acquisizione o fusione che potrebbe minacciare gli interessi di sicurezza nazionale. I progetti di investimento straniero sono sottoposti al Comitato per gli investimenti internazionali negli Stati Uniti (Committee on Foreign Investments in the United Sate, CFIUS).
Un periodo di revisione di 30 giorni, che può essere aumentato di 45, giorni consente di fornire un parere - tenuto segreto - al Presidente.

In Germania, non esisteva il concetto di impresa strategica. Tuttavia, operazioni di partecipazione di capitale straniero nelle società di difesa hanno evidenziato le carenze del diritto tedesco. Il governo federale ha introdotto un emendamento al suo progetto di legge per le relazioni economiche esterne, il che gli permette di controllare le operazioni finanziarie con paesi stranieri per verificare la compatibilità con gli interessi di sicurezza nazionale. Tale procedura riguarderebbe la partecipazione straniera superiore al 25% nel capitale di una società tedesca. La gestione di una tale procedura sarebbe attuata dal Ministero Federale dell'Economia e del Lavoro. Allo scopo di salvaguardare la sicurezza economica-rileva Carayon-è necessario fare riferimento all'attuale quadro europeo e internazionale .
L'Organizzazione Mondiale del Commercio (OMC), il cui obiettivo è quello di promuovere il libero commercio, prevede per gli stati la possibilità di sviluppare misure specifiche per salvaguardare gli interessi vitali della loro sovranità. Queste possibili deroghe ai principi del libero commercio possono essere osservate negli statuti del Fondo monetario internazionale o anche nell'accordo sulle misure relative all' investimento e commerciale e relative al commercio (MIC) allegato all'accordo che istituisce l'OMC.
Questo accordo contiene una clausola di eccezione, cosiddetta di sicurezza, basata sugli articoli che possono essere utilizzati XXI b) III dell' accordo del GATT del 1994, e che può essere utilizzata quando sono in gioco gli interessi vitali di uno Stato anche se questi non vengono definiti con precisione.

Analogamente, l'articolo 3 del codice di liberazione dei movimenti di capitali sviluppato sotto l'egida dell'OCSE permette le misure necessarie per mantenere l'ordine e la sicurezza pubblica e la tutela degli interessi essenziali della sicurezza.Nel contesto europeo sono vietate eventuali restrizioni ai movimenti di capitali tra gli Stati membri e i paesi terzi, in linea di principio, dal trattato che istituisce la Comunità europea.

La libera circolazione dei capitali è anche uno dei fondamenti del diritto comunitario. Tuttavia, l'articolo 58 dello stesso trattato stabilisce che il principio della libera circolazione dei capitali non impedisce che gli Stati membri possano adottare misure "giustificate da motivi di ordine pubblico o di sicurezza pubblica ".
La giurisprudenza comunitaria ha avuto cura di inquadrare l'applicazione della nozione di «motivi di sicurezza pubblica". I motivi di esenzione devono essere interpretati restrittivamente, in modo che la sua applicazione non possa essere determinata unilateralmente da ciascuno Stato membro, senza controllo da parte delle istituzioni comunitarie. Essi non possono essere invocati che in caso di minaccia reale e sufficientemente grave da pregiudicare un interesse fondamentale della società (sentenza Calfa, 1999).
La Corte di giustizia ammette che "la sicurezza pubblica" comprende tanto la sicurezza interna quanto la sicurezza esterna. Con la sentenza Richardt, pronunciata nel 1991, la Corte ha accettato la validità di autorizzazione per il transito di materiale qualificato "strategico" da Lussemburgo.

Le considerazioni economiche non possono giustificare misure restrittive se un obiettivo di sicurezza pubblica le supera ampiamente. Questo accade nel caso della necessità di garantire un approvvigionamento minimo dei prodotti petroliferi. Inoltre, la Corte di giustizia verifica il rispetto del principio di sicurezza legale.
In generale, la legislazione nazionale in materia di investimenti internazionali è compatibile con il diritto comunitario solo a due condizioni:
- gli stati membri dovrebbero essere in grado di giustificare la necessità e la proporzionalità della restrizione alla libera circolazione dei capitali di cui sono in possesso;
- gli investitori hanno bisogno di sapere con precisione quali condizioni vengono loro imposte.
Inoltre, purché le restrizioni siano basate sulla "difesa nazionale" , concetto assente, per quanto strano, in quanto tale nella legge comunitaria, occorre che il sistema nazionale sia in grado di porre in essere un concetto corrispondere a quello comunitario di "sicurezza pubblica".

4-Le minacce per la tecnologia dell'informazione e della comunicazione

Le società moderne sono sempre più dipendenti dalla tecnologia dell'informazione, anche nel loro funzionamento quotidiano. Operazioni finanziarie e commerciali sono in aumento, mentre la produzione industriale e la gestione dell'energia (compresa quella nucleare) si fondano proprio su queste tecnologie. Le nostre società sono quindi particolarmente vulnerabili ad atti di ostilità contro i sistemi informativi che ne costituiscono la base.
Allo stesso modo, i sistemi di difesa incorporano sempre di più l'informatica. Il crescente ruolo della tecnologia dell'informazione e comunicazione nell'uso degli strumenti in ambito militare causa d'altronde l' aumento delle potenziali vulnerabilità.Ebbene,usando gli stessi strumenti di comunicazione e informazione, lo stato e le aziende si trovano ad affrontare le stesse minacce.
I microprocessori sono al centro dei sistemi di informazione. Essi condizionano quindi direttamente la capacità e la velocità di calcolo, particolarmente importante per le simulazioni su larga scala, osservabile in particolare nelle applicazioni nucleari o della difesa. L'importanza strategica dei processori è chiara: per esempio il processore "PowerPC" Motorola dell' IBM è stato considerato addirittura come materiale di guerra .
Ma i microprocessori possono anche essere fonte di significative vulnerabilità per i sistemi che li incorporano . La sempre più grande integrazione delle funzioni "in silicio" porta alla costituzione di microcodici incontrollati (e difficili da rilevare) con rischi di backdoor (difetti del sistema) o di altri dispositivi di monitoraggio e controllo a distanza.
Recentemente, ha evidenziato questi problemi, la polemica sul Trusted Computing Platform Alliance (TCPA). La Microsoft e Intel contavano di poter controllare in tale modo la pirateria di software. Tuttavia, queste caratteristiche potrebbero permettere alle persone malintenzionate o ai

servizi segreti stranieri, di avere un mezzo per controllare a distanza l'attivazione di tutte o parte dei sistemi informatici senza che lo conoscano i loro utenti. Si noti che il settore dei trasformatori industriali, nonché quello di memoria o di archiviazione dati dispositivi, è oggi totalmente sotto il controllo delle società statunitensi. Né la Francia né l'Europa hanno la maggior parte delle competenze e delle industrie necessarie a sviluppare un processore competitivo senza la cooperazione con gli Stati Uniti. Questo costituisce un rilevante punto di vulnerabilità per il futuro, anche se l'Asia potrebbe offrire una potenziale alternativa: la Cina è impegnata nello sviluppo di suoi microprocessori.

I sistemi operativi costituiscono la base dei sistemi d'informazione. Anche se la concorrenza tra le imprese Apple e Microsoft è oggi in gran parte obsoleta, continuano ad essere al centro del settore delle tecnologie dell'informazione. La Microsoft ,essendo nella situazione quasi monopolistica con il suo sistema Windows, non ha più alcun reale concorrente che potrebbe essere in grado di affrontarlo. Il sistema operativo Apple riguarda oramai solo un pubblico ridotto e il sistema Unix, anche se rappresenta il 40% della quota di mercato per i server, non è mai riuscito a conquistare veramente il mercato lavorativo.

L'ascesa del potere dei software - soprattutto Linux – potrebbe fornire una nuova speranza per coloro che vorrebbero minare l'egemonia della Microsoft.

I sistemi operativi sono una delle fonti di vulnerabilità per i principali sistemi informativi: è attraverso loro che si può entrare nel sistema, utilizzando il backdoor. La Francia, come la maggior parte degli altri paesi europei, ha un'alta vulnerabilità tecnologica in questo settore, e solo l'uso dei software liberi, non protetti da legge, può costituire un possibile rimedio.

Il Controllo all' accesso è la parte più visibile della sicurezza, e senza dubbio, paradossalmente, la meno sensibile al piano di vulnerabilità tecnologica nazionale. I rappresentanti francesi sono numerosi ed efficienti in questo campo.Basti pensare a Sagem, Bull e Gemplus. Quest'ultima società, il cui capitale è ora controllato dal fondo di investimento statunitense , illustra il rischio inerente alle aziende di successo. La trasmissione delle informazioni in un mondo sempre più interconnesso, è un obiettivo primario per ottenere l'accesso non autorizzato ai dati. Le principali vulnerabilità di reti wireless sono quelle al livello di router. Tali strutture - che integrano un sistema operativo generalmente specifico per il fornitore - includono anche backdoor di servizio. Solo le due aziende – Alcatel e Cisco- condividono tra di loro il mercato mondiale.

Le reti wireless di tipo "WiFi", il cui sviluppo è attualmente molto veloce, presenteranno probabilmente delle nuove vulnerabilità. Oltre alle vulnerabilità relative alla trasmissione radio (interferenze ...), il protocollo di crittografia dei dati forniti dallo standard prescelto non risulta del tutto efficace. Poche aziende francesi sono attive in questo settore. Tuttavia, per la Francia, ci può essere ancora un' importante vulnerabilità tecnologica: la trasmissione senza fili a lunga distanza offre delle vere potenzialità sia per le applicazioni civili che per quelle militari. Le applicazioni da ufficio sono un obiettivo primario per accedere alle informazioni. La produttività aziendale dipende, in larga parte da tali software. La Microsoft è riuscita a imporre uno standard – Microsoft Office – ed i rappresentanti importanti come Adobe, sono americani. Per quanto riguarda i sistemi operativi, l'alternativa all'egemonia statunitense potrebbe venire dai software liberi. La Francia, tuttavia, fortemente presente in questo settore con i Sistemi Dassault, rimane tecnologicamente molto vulnerabile. Forse dovrebbe adottare l'idea di un' industria del software nazionale o europeo.

In definitiva lo sviluppo della società dell'informazione è accompagnato da un sensibile aumento delle minacce di fronte alle quali gli Stati sono più spesso disarmati e oggetto di precauzione riguardo ai rappresentanti privati. La Francia ha adottato diversi strumenti per affrontare questa sfida, soprattutto attraverso la creazione di piani di prevenzione e reazione ad un attacco terrorista cibernetico e avviando l'istituzione di un organo operativo il Centro per Censimento e trattamento degli attacchi informatici (CERTA). Quest'ultimo interagisce con i centri di competenza dei ministeri e delle agenzie delle controparti specializzate (RENATER per la Ricerca).

A tale proposito è necessario il controllo della Direzione Centrale della sicurezza dei sistemi di informazione (DCSSI). La cellula che ne è responsabile, è composta da sei persone, reclutate tra i migliori specialisti informatici. Tuttavia l'esiguità di questo personale risulta irrisorio riguardo al compito di responsabilità di questa cellula, competente per tutti i sistemi di informazione statali. Tutti i servizi ministeriali devono essere consapevoli dei rischi legati agli attacchi informatici e del loro dovere di proteggere i dati personali dei cittadini contenuti su server diversi.

II.- LA SICUREZZA NAZIONALE: UNA TRASFORMAZIONE DI STATO DA REALIZZARE

L'Ordinanza n ° 59-147 del 7 gennaio 1959 sull'organizzazione generale della difesa prevede nell'articolo 18 che il ministro dell'Economia , “difende l'azione dei ministri responsabili della produzione, la riunione e l'uso di diverse categorie di risorse nonché della pianificazione industriale del territorio”. Inoltre, garantisce la "connessione permanente con il Ministro dell'Interno e il Ministro della Difesa affinché si possano prendere in considerazione le essenziali necessità della difesa nel piano economico. "
Ebbene ,tali disposizioni non sono più adattate all’attuale realtà economica. Il ruolo dello Stato nell'economia è cambiato e le tecnologie dell'informazione e della comunicazione sono diventate fondamentali. A tale proposito sarebbe opportuno sostituire il concetto della difesa nazionale, come lo si concepiva 45 anni fa, con quello di sicurezza nazionale, più globale, che comprende la protezione economica e la lotta contro le nuove minacce.E' infatti necessaria una strategia globale della sicurezza nazionale .

Gli Stati Uniti si sono dotati dei mezzi per consolidare il proprio potere.Per consolidare la loro supremazia economica e il controllo delle tecnologie dell'informazione e della comunicazione, gli Stati Uniti si basano su una legislazione appropriata e le agenzie federali proteggono i loro interessi strategici, sostenendo la conquista dei mercati internazionali .
L’ attentato dell'11 settembre 2001 diede l'occasione per rafforzare i sistemi già esistenti, in particolare in termini di sorveglianza delle comunicazioni. Allo scopo di lottare contro le reti terroristiche, il Patriot Act, aumenta significativamente i poteri delle autorità americane. Per quanto riguarda il controllo delle comunicazioni, la normativa precedente prevedeva che la minaccia doveva essere chiaramente identificata perché il ministro della Giustizia desse l'autorizzazione a procedere con le intercettazioni. Il nuovo testo elimina questo vincolo. Il numero di intercettazioni può crescere automaticamente. Inoltre, il campo di controllo è stato esteso anche alla posta elettronica.
Le stesse strutture federali, si sono evolute, poiché è stato creato un nuovo ministero: il Department of Homeland Security (Dipartimento della sicurezza del territorio nazionale).
A questo ente governativo è stato dato il compito di evitare ogni genere di attacco o di una calamità che potrebbero minacciare la sicurezza nazionale sul terreno americano. E' infatti responsabile di:
- prevenire i disastri (rischio nucleare, biologico, radiologico o chimico) e prevedere eventuali

misure di emergenza;
- garantire la sicurezza dei confini marittimi, terra e aria.

- di monitorare e controllare le comunicazioni e le reti informazioni per rilevare tutte le informazioni che potrebbero essere una minaccia contro il territorio degli Stati Uniti;
- di contribuire alla ricerca e sviluppo di laboratori universitari o aziendali, sempre nella prevenzione dei rischi terroristici.
Il Dipartimento si basa su 22 agenzie federali per la raccolta e il trattamento delle informazioni.

Oltre alla possibilità di supportare l'innovazione degli Stati Uniti tramite i fondi di investimento (a volte strettamente controllati dall'amministrazione federale), gli Stati membri si sono impegnati ad un approccio proattivo al supporto per i mercati internazionali da parte delle imprese statunitensi. E 'la missione, dal 1994, del Centro Advocacy del Dipartimento del Commercio. Si tratta di un unico e centrale ufficio di coordinamento che riunisce le risorse di 19 agenzie governative degli Stati Uniti per garantire che le vendite di prodotti e servizi americani abbiano le migliori prospettive all'estero. Permette inoltre di mettere al servizio delle aziende americane tutti i dispositivi pubblici, tra cui le agenzie di intelligence, per ricevere aiuto riguardo ai loro concorrenti stranieri. Non esiste un solo spostamento, viaggio commerciale all'estero dei dirigenti di Boeing senza una precedente visita del direttore della CIA!

Alla luce di queste riflessioni ,sottolinea Carayon,la sicurezza nazionale deve basarsi sulla definizione di un ambito strategico dell'economia francese.Il presupposto per l'attuazione di una strategia di sicurezza nazionale è alla base della definizione di un "perimetro strategico" della complessiva performance della Francia ,perimetro strategico che le agenzie governative dovranno chiaramente definire.Essa deve essere parte di un quadro europeo.

Gli Stati membri e la stessa Unione europea devono impegnarsi in una strategia di potere. Devono prendersi, collettivamente, la responsabilità della loro sicurezza globale, a prescindere degli americani, e superare le dipendenze tecnologiche e normative che ostacolano il loro comune destino. Questa strategia non dovrebbe essere concepita contro gli Stati Uniti, ma volta a rafforzare il potere d'Europa, in un mondo multipolare.

In primo luogo, la sicurezza nazionale riguarda un settore pubblico più grande della sola difesa, intesa in senso stretto. Esso comprende in particolare la sicurezza o addirittura la sicurezza ambientale. Il diritto comunitario, come il diritto internazionale, consente questa espansione del concetto.

In secondo luogo, il quadro delle interconnessioni tra il settore pubblico e quello privato deve essere consolidato.

Da un lato, gli Stati membri dispongono di precise deroghe dei Trattati. Tali clausole di salvaguardia possono essere invocate per giustificare le disposizioni nazionali per la difesa dell'ordine pubblico. In generale, il diritto comunitario non impedisce l'espansione giuridica dei poteri sovrani dello Stato, ma inverte l'onere della prova. Il libero gioco del mercato è la regola, le distorsioni provocate da uno Stato membro devono essere giustificate.

D'altro canto, conviene portare tali dispositivi a livello comunitario. Il diritto comunitario si basa infatti su una filosofia contraria agli atti giuridici che possono danneggiare direttamente le operazioni di mercato.

Tuttavia, molte misure per preservare la sicurezza economica possono offendere il principio della libertà di commercio e dell'industria. Questo è il caso, per esempio, di uno Stato che interviene in una transazione privata per preservare i propri interessi strategici in aree chiave come quello farmaceutico. Così, affinché un dispositivo europeo sia il più possibile compatibile con il diritto comunitario, sarebbe auspicabile che il funzionamento del mercato . Gli europei devono accordarsi su una legislazione comunitaria. Dato il processo decisionale comunitario, occorre che la Commissione convalidi tali aspirazioni. La questione è ancora da formulare, in quanto si tratta di difendere la sicurezza economica europea e le strategie industriali che portano quindi in sé sia il potere che la coesione sociale. Questa modifica dovrebbe basarsi su un rinnovo dell'azione pubblica. Per poter essere pienamente realizzato, questo cambiamento deve basarsi su un'architettura semplice: un forte impulso politico dato da un Consiglio di sicurezza economica presso il Capo dello Stato, sulla base di una struttura che permette l'uso delle risorse pubbliche e l'uso di un fondo di investimento per il capitale misto pubblico-privato.Inoltre bisognerebbe creare un Consiglio di sicurezza economica per far fronte alle nuove sfide e le nuove minacce a cui è esposta la sicurezza interna.A tale proposito,rileva Carayon, il Presidente della Repubblica ha deciso di creare un Consiglio di sicurezza interna. Istituito con decreto n. 2002-890 del 15 maggio 2002, il Consiglio è responsabile della definizione delle linee guida della politica in materia di sicurezza interna e di definizione delle priorità. Esso garantisce la coerenza delle azioni di vari ministeri, li valuta e assicura l'adeguatezza delle risorse utilizzate.

Presieduto dal Presidente della Repubblica, il Consiglio di Sicurezza interna comprende il primo ministro, i ministri dell'Interno, della Giustizia, della Difesa, dell'Economia e delle Finanze, del Bilancio e dell'Oltremare . Il suo segretario generale, in collaborazione con i ministeri competenti e il Segretariato generale della Difesa nazionale, prepara le riunioni del Consiglio e le trascrizioni delle decisioni e monitora l'attuazione delle decisioni prese.

E'importante dare alla sicurezza economica lo stesso tipo di impulso che è stato dato due anni fa alla sicurezza interna. Creare un nuovo consiglio per tutelare la sicurezza economica diventa una questione secondaria. Una tale struttura avrebbe una portata molto più ampia rispetto al Consiglio informazioni Interdipartimentale per la difesa economica. Avrebbe autorità soprattutto politica, necessaria per superare la riluttanza, la resistenza, la compartimentazione e la lentezza dell'amministrazione.Sarebbe anche necessario porre in essere una sorta di "CEA" delle tecnologie dell'informazione, della comunicazione e della sicurezza cioè un un commissariato per le tecnologie dell'informazione, della comunicazione e della sicurezza la cui missione è quella di stimolare lo sviluppo del settore industriale e tecnologico. La sua realizzazione permetterebbe :

- di implementare le linee guida definite dal Consiglio di sicurezza economica;

- di garantire la condivisione di finanziamenti pubblici da vari ministeri e le organizzazioni correlate.

Dalla sua nascita, questa organizzazione dovrà, in collaborazione con le imprese, creare un panorama delle vulnerabilità francesi.

Un altro provvedimento che Carayon nella sua relazione ritiene utile è quello volto a creare una piattaforma industriale delle tecnologie dell' intelligence economica.Mantenere la competitività delle nostre imprese è strettamente legato alla salvaguardia della competitività tecnologica della Francia e dell'Europa. La creazione di una piattaforma industriale delle tecnologie dell' intelligence economica è ovviamente una necessità, purtroppo ancora mal percepita da parte delle autorità pubbliche.

Questo progetto di piattaforma accompagna naturalmente, la nomina di un alto responsabile dell'intelligence economica. Bisogna, infatti, dare una dimensione operativa e industriale a un tale appuntamento, non ridurlo ad un trattamento amministrativo dei fascicoli.

Inoltre questa piattaforma mostrerebbe che un partenariato pubblico/ privato è lo strumento fondamentale per superare le nostre dipendenze. Questo progetto potrebbe avere, fin dall'inizio, una dimensione franco-tedesca .

Allo scopo di consolidare il dispositivo di sicurezza economica francese Carayon ritiene necessario europeizzazione l' Adit. L'Agenzia per la diffusione dell'informazione tecnologica (ADIT) detiene oggi un primato indiscusso sul mercato francese dell'intelligence economica. Diventata nel 2003 una società nazionale al 100% di proprietà dello Stato, opera in tre aree:

-nel contesto dell' intelligence competitiva e strategica per i principali gruppi nazionali;

- nel contesto dell'intelligence territoriale per sviluppare una cultura di progetto e di rete per le PME e le PMI;

- e nel potenziamento della tecnologia dell'informazione globale a vantaggio degli operatori economici francesi.

Nel contesto dell' intelligence economica francese, l'ADIT è diventato un elemento chiave per le autorità pubbliche soprattutto per i ministeri responsabili degli Affari esteri e della Ricerca.

Le prospettive di sviluppo dell' ADIT sono ormai condizionate dalla sua capacità di intervenire su una base non più strettamente nazionale, ma europea. Nella sua dimensione attuale, non ha capacità sufficiente per fornire tutti i servizi richiesti dalle grandi aziende francesi impegnate nei mercati globali.Diventa quindi urgente includere l' ADIT in una strategia internazionale. Costruire un'alternativa credibile a quella anglosassone, su una base europea dominante, è ormai una priorità strategica.

III.- PROTEGGERE MEGLIO LE IMPRESE FRANCESI

La dematerializzazione dell'economia rende più diffuso oggi ciò che è il patrimonio di una società: i suoi uomini, naturalmente, ma anche le loro idee, la capacità, le loro reti relazionali e commerciali, i loro metodi di gestione. Le informazioni legali, finanziarie, commerciali, scientifiche, tecniche, economiche e industriali che condividiamo e scambiamo a seconda di un modello di gestione spesso diventano più orizzontali che verticali.Per questo,precisa Carayon,è necessario proteggere le informazioni economiche sensibili attraverso una nuova legge del segreto commerciale.

Secondo la legge attuale, le informazioni aziendali sensibili sono protette solo da un insieme di testi la cui coerenza ed efficacia è discutibile .Ciò significa che bisogna creare una nuova legge del segreto professionale che permetta ad una azienda, che rispetti un sistema di protezione delle informazioni, di perseguire coloro che cercano di utilizzare in modo fraudolento le informazioni sensibili. Inoltre è necessario supportare le imprese strategiche .Infatti le aziende si basano su un numero crescente di subappaltatori per fornire loro beni e servizi necessari per la loro produzione. Sempre più spesso, i grandi gruppi diventano assemblatori di pezzi, prodotti da piccole e medie industrie. Tuttavia, spesso capita che queste aziende hanno delle competenze specifiche,particolarmente cruciali. Padroneggiare le loro competenze diventa quindi una questione di carattere strategico.In altri termini le PME e PMI francesi ed europee devono essere sostenuti dalle autorità pubbliche e dai grandi gruppi industriali. Indispensabile allora diventa il finanziamento pubblico dell ' alta tecnologia. A tale proprosito il governo americano ha sviluppato da più di quarant'anni una procedura di sovvenzione sistematica delle imprese in crescita nei principali settori di alta tecnologia individuate per il mantenimento di "supremazia militare e tecnica degli Stati Uniti d'America". Il processo di finanziamento inizia con l'individuazione di progetti industriali innovativi. Tali progetti possono essere accompagnati dal programma di sostegno dell'innovazione e della ricerca delle PMI.

Il finanziamento iniziale viene svolto dalla DARPA ,o da una agenzia federale, in un paio di settimane (massimo sei mesi). L'agenzia può supportare contemporaneamente diverse decine di aziende, sapendo che solo una o due saranno in grado di raggiungere i loro obiettivi. Il fallimento del piano industriale viene generalmente considerato fin dall'inizio e non deve essere presentata nessuna denuncia ai dirigenti sfortunati, se si dimostra che essi hanno dedicato i loro sforzi per il successo del progetto. Nel frattempo, il Dipartimento della Difesa è responsabile per il finanziamento di grandi programmi di difesa.

Un altro provvedimento necessario è quello volto a rafforzare il tessuto economico delle piccole imprese innovative.L'innovazione tecnologica risulta ampiamente favorita dalla forza del tessuto economico di piccole e medie imprese innovative. Se lo stato, che agisce per ordine pubblico dei grandi gruppi industriali – che agiscono attraverso la loro attività di ricerca e sviluppo – sono ben consapevoli di questo problema, resta il fatto che questo sforzo non è ottimale. Lo Stato ed i rappresentanti economici devono concentrare la loro attenzione su alcune piccole e medie imprese che supportano le tecnologie del controllo. Senza volontà politica e industriale, il tessuto economico delle PMI non può essere rafforzato. Inoltre è opportuno assicurarsi della efficacia delle tecnologie critiche.

I grandi industriali francesi lo sanno perfettamente : al centro di molti processi industriali troviamo un piccolo numero di imprese ad alta tecnologia. Occorre garantire che queste tecnologie, spesso sviluppate da piccole e medie imprese, restino in Francia e in Europa in modo totalmente indipendente dall'estero.

Molteplici procedure consentono ai governi di identificare e contribuire a sviluppare e mantenere in Francia la padronanza delle tecnologie chiave.

L’Agenzia nazionale per la promozione della ricerca (ANVAR) – l’agenzia francese per l’innovazione – assicura, a nome della delegazione generale per gli armamenti (DGA), con la quale ha firmato un accordo- il finanziamento di progetti condotti da aziende di interesse strategico.

L’accordo tra l’Anvar e la DGA prevede, da un lato, l’istituzione di un finanziamento per supportare l’innovazione delle aziende duali o quelle interessate alla difesa e d’altra parte, una collaborazione in materia di monitoraggio tecnico – economico delle PME e delle PMI considerate strategiche. I cofirmatari si sono cosi impegnati a promuovere gli scambi delle informazioni tecnologiche, organizzare incontri tra gli esperti del settore e cercare delle opportunità a livello europeo e internazionale.
Nel 2002 e 2003, sono stati firmati 14 contratti con società innovative, per un totale di 3,6 milioni di euro. Questi programmi comprendono principalmente dei circuiti integrati, un banco di prova per un dispositivo di comunicazioni militari, un micro server integrato, un sistema di navigazione per carichi aerotrasportati e di dispositivi di sicurezza Internet.
Inoltre, dobbiamo rimanere vigili circa la sostenibilità del controllo delle tecnologie critiche. Basta ricordare l'esempio della società britannica Acorn che dopo aver ricevuto dei finanziamenti comunitari per la ricerca e lo sviluppo, è stata acquisita da Intel.

IV.- MIGLIORARE LA SICUREZZA DEI SISTEMI INFORMATIVI

L'importanza della elaborazione elettronica di dati, con un ritmo senza precedenti, ha reso necessaria la protezione dell'infrastruttura informatica, per proteggere la nostra economia.
Le nostre società si trovano ad affrontare la minaccia di pirati informatici e servizi segreti di Stati esteri .Gli Stati Uniti hanno una strategia di controllo del settore sicurezza delle informazioni. Con il sostegno finanziario del governo federale, una tale strategia consente alle aziende americane di essere in posizione dominante.
Di fronte a una simile egemonia, i mercati europei sembrano troppo rigidi per consentire lo sviluppo delle industrie nazionali.
Nonostante la sua credibilità nel contesto della crittografi la Francia potrebbe vedere scomparire gradualmente quelle sue capacità se non viene avviata una vera politica industriale.