Rassegna stampa

Centro Studi C.N.I. 22 maggio 2016

Waypress
media monitoring

CYBERSECURITY

ARCHEOLOGI

ECONOMIA

L'inchiesta

Le manovre Nato sul fronte della cyberguerra

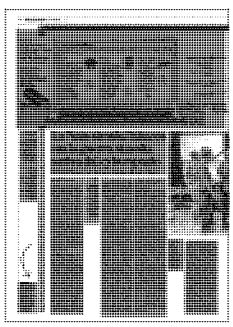
CAROLA FREDIANI

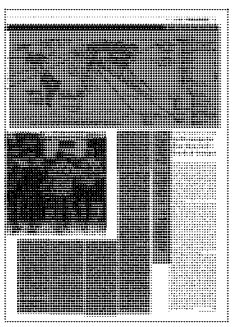
È il più sofisticato gioco di guerra informatica e di dissimulazione, quello organizzato tutti gli anni a Tallinn dalla Nato. Oltre 500 persone di una ventina di Paesi dell'Alleanza atlantica in competizione tra loro per contrastare, decifrare e attribuire un cyberattacco simulato in un ambiente virtuale. «Lavoravamo sotto pressione, abbiamo dormito poco», commenta Emanuele Gentili, ad dell'azienda TigerSecurity Pro e parte del team italiano guidato dal ministero della Difesa che ha partecipato all'edizione dello scorso aprile. «Ma - aggiunge - abbiamo trovato il malware, il software malevolo, nei sistemi compromessi, lo abbiamo decodificato e siamo risaliti ai server di comando».

Locked Shields - la più grande esercitazione di cyberdifesa al mondo - è organizzata fin dal 2010 dalla Nato in Estonia. Quest'anno l'Italia è arrivata settima. Prima una sorprendente Slovacchia.

Più o meno negli stessi giorni di questa maestosa simulazione internazionale, ad aprile, la spicciola realtà faceva capolino sui sistemi industriali dell'Europa.

CONTINUA ALLE PAGINE 12 E 13





LA STAMPA

La Nato simula l'attacco ma la guerra stavolta arriva dal cyberspazio

In Estonia maxi esercitazione: l'Italia soltanto settima

CAROLA FREDIANI
SEGUE DALLA PRIMA PAGINA

Il fornitore di energia elettrica tedesco Rwe, che gestisce la centrale nucleare di Gundremmingen, non lontano da Monaco di Baviera, comunicava infatti di aver trovato delle infezioni - tecnicamente un paio di worm - su alcuni dei suoi pc, che fortunatamente non erano collegati a Internet. Il malware - vecchio, non mirato specificamente alla centrale, e il cui obiettivo era rubare credenziali di accesso degli utenti - ci era arrivato tramite chiavetta Usb. Se quindi quel tipo di infezione non era particolarmente preoccupante, era tuttavia poco incoraggiante la facilità con cui era stata veicolata. Del resto furono proprio delle chiavette Usb che inizialmente nel 2009 veicolarono Stuxnet - la prima vera arma digitale – in Iran (vedi box).

L'attacco in Europa

Ma l'Europa lo scorso 23 dicembre ha messo a segno anche un suo primato, registrando un cyber-attacco a una utility dell'energia ucraina, Prykarpattya Oblenergo, che ha tolto la corrente per alcune ore a 230 mila residenti della regione di Ivano-Frankivsk. A oltre tre mesi dall'attacco, i diversi esperti che lo hanno analizzato concordano su un fatto: è stato progettato ed eseguito molto bene. Per farla breve, gli attaccanti hanno prima infettato dei dipendenti dell'azienda via mail (attraverso le macro di allegati Word), quindi si sono mossi nella rete aziendale fino a ottenere le credenziali dei sistemi di controllo industriale - che in quel caso gestivano la rete elettrica. E mentre staccavano una serie di sottostazioni, mandando in blackout migliaia di ucraini, si premuravano perfino di bloccare le linee telefoniche dell'azienda - e le segnalazioni dei clienti - ingolfandole con finte chiamate.

«Dopo l'attacco alla centrale, i suoi tecnici per due mesi sono andati avanti comunicando attraverso carta e telefono. Tra l'altro i sistemi di protezione che avevano non sono molto diversi da quelli usati in Occidente», commenta Andrea Rigoni, advisor Nato e codirettore del progetto CyberDefence in Georgia.

L'intelligence ucraina ha subito puntato il dito contro Mosca, anche in considerazione delle tensioni geopolitiche tra i due Paesi. Ma come accade spesso in questi casi le prove per l'attribuzione di un attacco sono esili e spesso contraddittorie. E dare la caccia all'attaccante è un po' come muoversi in un labirinto di specchi, con la complicazione che i cacciatori - le aziende di sicurezza - hanno a loro volta una collocazione geografica se non geopolitica ben definita.

Per capirci: nella sola Russia ci sarebbero almeno 14 gruppi diversi dediti ad attacchi cyber mirati e persistenti, scrive l'Istituto americano per la tecnologia delle infrastrutture critiche. Alcuni hanno ricevuto dai ricercatori nomi fantasmagorici, da Epic Turla a CosmicDuke. Il più noto e il più attivo, attribuito alla Russia se non direttamente al suo governo, si chiama Apt28 (o Sofacy). Apt sta per Advanced persistent threat, minaccia persistente avanzata: un tipo di attacco che punta a target specifici, prolungato nel tempo, che cerca di esfiltrare dati o in casi più rari sabotare sistemi. Dietro spesso ci sono degli Stati.

Spie digitali

I primi a fare un rapporto dettagliato che svelava l'identikit di un simile gruppo sono stati gli analisti di Mandiant - società oggi parte della compagnia statunitense FireEye, forti legami col governo Usa - quando nel 2013 pubblicarono il report intitolato Apt1. Nel documento esponevano l'attività di un gruppo di cyberspionaggio cinese riconducibile, anche fisicamente, all'unità 61398 dell'esercito della Repubblica popolare.

Nel 2014 è stata invece la volta di un report FireEye sulle spie digitali di Apt28, che venivano ricondotte al governo russo. «È un gruppo sponsorizzato dallo Stato, che colpisce soprattutto organizzazioni dell'Est Europa, in particolare ministeri degli Esteri. Il suo obiettivo è raccogliere intelligence utile per il governo di Mosca», commenta Yogi Chandiramani, direttore commerciale per Europa e Mediterraneo della stessa FireEye. Sulle finalità di questo Apt28 concordano diversi analisti. Alla società di cybersicurezza russa Kaspersky - autrice di numerosi rapporti su gruppi di cyberspionaggio, e considerata vicina al governo del suo Paese - lo chiamano Sofacy. «È un gruppo longevo negli anni. Hanno molti strumenti e risorse, se individui un loro malware nel tuo network dopo poche ore tornano con un altro tipo di software malevolo. E il loro obiettivo è lo spionaggio a lungo termine», racconta Vicente Diaz, ricercatore di punta di Kaspersky.

Ma se sull'analisi le diverse società spesso concordano, è sulla attribuzione di attacchi specifici che aumentano le divergenze. Chandiramani ad esempio riconduce il pesante e distruttivo attacco del 2015 alla tv francese Tv5monde proprio ad Apt28; Diaz invece si mostra scettico. Da notare che all'epoca si era addirittura parlato di Cyber Califfato, poi è invece subentrata la pista russa. E questo è solo un esempio del groviglio in cui si muovono anche i più navigati analisti quando devono districare simili assalti informatici.

Torniamo a questo punto al blackout ucraino. Il malware usato in quel caso si chiama BlackEnergy3, appartiene a una famiglia di strumenti che sarebbero stati usati da un gruppo Apt (chiamato proprio BlackEnergy) promosso a sua volta dal governo russo, almeno secondo il già citato Istituto per la tecnologia delle

infrastrutture critiche. Dunque attribuzione chiara? Diaz di nuovo è scettico, perché «sappiamo poco su chi lo ha effettivamente usato». La ragione sta anche nel tipo di software malevolo adottato. BlackEnergy è un kit di strumenti impiegato da anni da diverse organizzazioni criminali, venduto nell'underground russo dal 2007, spiega un rapporto della società di sicurezza finlandese F-Secure. La sua modularità e popolarità lo hanno diffuso tra gang diverse, molte delle quali lo usano per rubare credenziali bancarie. «L'uso di BlackEnergy per attacchi di natura politica è una intrigante convergenza fra attività criminali e spionaggio», scrive F-Secure.

Processo bidirezionale

La sovrapposizione di criminali e spie, o quanto meno dei loro strumenti, è un processo bidirezionale. Da un lato gli Stati comprano vulnerabilità informatiche anche dai mercati neri; dall'altro, «quando un certo strumento, un malware in mano a gruppi statali viene scoperto dai ricercatori, allora viene condiviso con cybercriminali, confondendo gli analisti», commenta Chandiramani. Anche perché definizioni e report provano a incasellare realtà variegate, dalle appartenenze fluide, specie se si scantona nell'ambito della cybercriminalità.

«Apt è un espressione usata da voi giornalisti; noi siamo un gruppo di russi, attivi da sette anni, anche se non lavoriamo per il governo. Vendiamo vari strumenti e 0day e abbiamo una percentuale dalla condivisione di alcune risorse», ci scrive un hacker russo individuato attraverso il suo sito web, da cui vende vari tipi di malware e 0day. Il sito è collegato a un account Twitter che allude a un'appartenenza a Sofacy, ma non è stato possibile verificare tale legame. «Non tocchiamo dati di carte di credito o siti bancari. Diciamo che il nostro è più un hobby. Abbiamo attaccato siti in Germania, Stati Uniti, Svezia, anche se in quest'ultimo Paese ci interessava solo l'azienda dell'energia Vattenfall». La bizzarra conversazione - avvenuta a metà tra inglese e russo, e analizzata con l'aiuto dal ricercatore dell'università di Trento Luca Allodi, conoscitore dei forum della cybercriminalità russa - cita un episodio poco noto, che sarebbe avvenuto poco tempo prima. A parlare per la prima volta di un possibile cyber attacco subito in Svezia da Vattenfall, una grossa compagnia energetica del Nord Europa, è a metà aprile una testata norvegese, citando, senza nominarle, fonti Nato. Nello stesso periodo l'intelligence svedese accusa la Russia di aver mandato in tilt, con un attacco informatico, il sistema di controllo del traffico aereo nei suoi aeroporti per alcuni giorni, nel novembre 2015. Inizialmente era stata data la colpa a una tempesta solare. È probabile che l'hacker con cui abbiamo parlato si sia intestato un attacco fatto da altri. Ma è anche possibile che l'attacco non sia mai avvenuto, poiché nessuno ha avuto modo di verificarlo davvero.

500

persone

Quelle che ogni anno partecipano al gioco di guerra informatica e di dissimulazione organizzato dalla Nato a Tallinn, in Estonia

20

Paesi

In competizione tra loro per contrastare, decifrare e attribuire un cyber-attacco simulato in un ambiente virtuale

Sherlock Holmes dei virus

La questione della corretta identificazione degli autori di cyberattacchi è così delicata che a fine aprile la Darpa, l'agenzia per la ricerca avanzata della Difesa Usa, ha pubblicato un bando per un progetto di ricerca solo su questo.

Quello che possono fare nel mentre gli Sherlock Holmes dei virus è cercare di stare ancorati a frammenti di evidenze, da incastrare in un puzzle. Così si inizia da un pezzo di malware, dalla mail che lo ha veicolato, si cercano altre vittime.

«Anche se cresce la pratica tra gli Apt di nascondersi dietro strumenti e attacchi di basso livello, che sembrino casuali, per non destare sospetti», commenta Diaz, che poi prova a elencare i gruppi più dinamici e potenti sulla scena attuale. «Nel 2015 Sofacy è stato sicuramente uno dei più attivi. Ma non va dimenticato Equation Group».

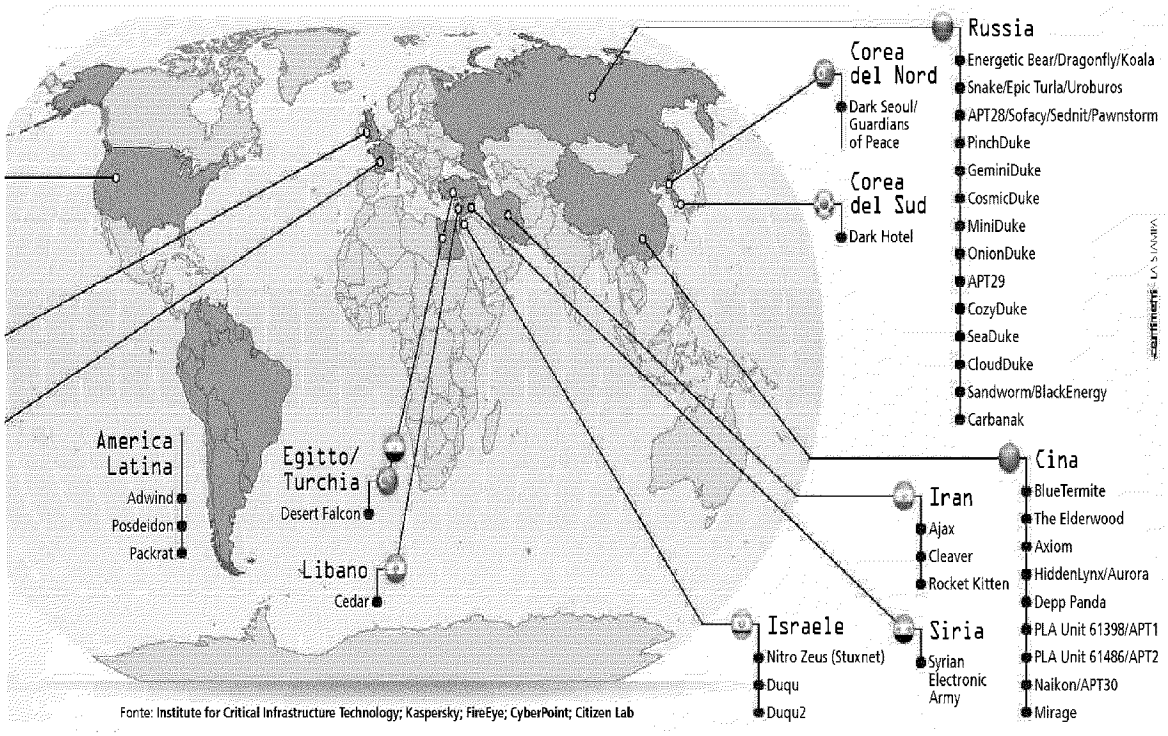
Equation Group sarebbe una sorta di unità d'élite di cyberspionaggio individuata proprio da Kaspersky nel 2015, e tracciata da alcuni fino all'americana National Security Agency. Del resto le potenze in campo sono queste: Usa, Russia, Israele, Cina, Francia, Uk e - dato in ascesa - lo stesso Iran. Sulla Corea del Nord restano opinioni contrastanti. Mentre per quanto riguarda la Cina, «dopo l'accordo del 2015 fra Obama e il presidente cinese Xi Jinping per limitare il cyberspionaggio, abbiamo registrato meno movimento da parte dei gruppi di quel Paese», rileva Diaz. Il che, aggiunge il ricercatore, rischia quasi di essere un problema, dal momento che hacker di Stato «disoccupati» potrebbero riciclarsi tra le file della cybercriminalità.

23
dicembre
Il giorno dello scorso anno in cui l'Europa ha registrato un cyber-attacco a una utility dell'energia ucraina

230
mila
I residenti della regione ucraina di Ivano-Frankivsk rimasti senza corrente dopo il cyber-attacco

14
gruppi
Quelli che in Russia si dedicano ad attacchi cyber mirati e persistenti secondo l'Istituto Usa per la tecnologia delle infrastrutture critiche

SICUREZZA DIGITALE



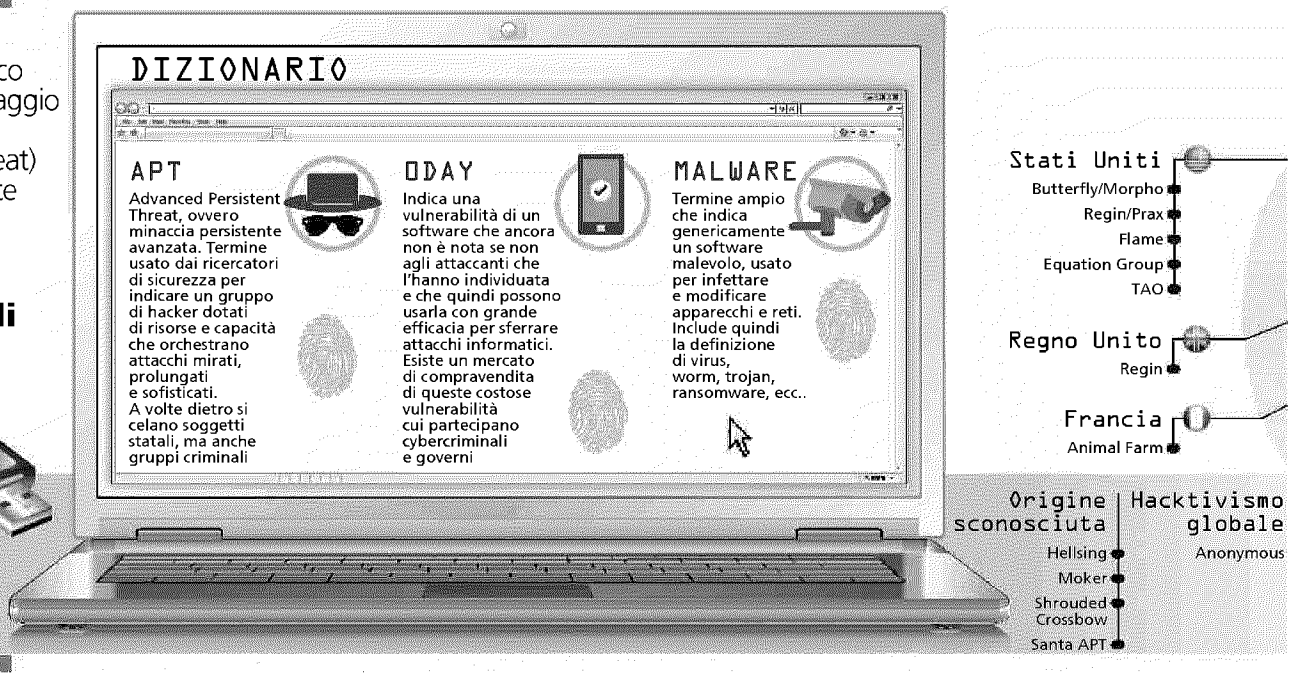
Fonte: Institute for Critical Infrastructure Technology; Kaspersky; FireEye; CyberPoint; Citizen Lab

Gruppi di cyber attacco e cyber spionaggio (Advanced persistent threat) attivi di recente

Il mercato globale dei prodotti e servizi di cybersicurezza è stato stimato sui

77 miliardi
di dollari
per il 2015

Fonte: Report 2015 del Congresso Usa



A Tallinn
Alcuni sfidanti durante l'ultima esercitazione di guerra informatica tra Stati organizzata dalla Nato in Estonia

7°
posizione
Conquistata quest'anno dall'Italia nella più grande esercitazione di cyberdifesa al mondo organizzata fin dal 2010 dalla Nato in Estonia

Ai lettori
Assieme all'Italia che funziona c'è anche un'Italia che non va. Segnalateci tutto ciò su cui a vostro avviso vale la pena di indagare scrivendo a: inchieste@lastampa.it

Il congresso «Cia»

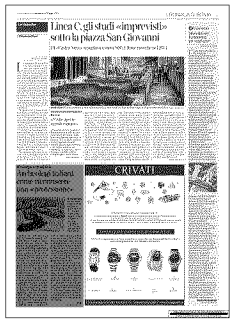
Archeologi italiani, come riconoscere una «professione»

Crustumerium Gli scavi della necropoli della città latina Crustumerium (IX- VI secolo avanti Cristo), nella zona Nord di Roma nei pressi di Settebagni, nella Riserva naturale della Marcigliana

Definizione (finalmente!) della figura professionale dell'archeologo. Ma più in generale si è discusso delle recenti riforme che riguardano il lavoro degli archeologi: la Riforma Franceschini del MiBACT, il nuovo Codice degli Appalti e l'Archeologia Preventiva, e il mini Jobs Act delle Partite IVA. E inoltre il volontariato in archeologia e i rapporti con le guide turistiche. Sono i temi del secondo congresso della Confederazione Italiana Archeologi, che si è svolto ieri a Palazzo Massimo a 12 anni di distanza dalla fondazione. Al Congresso hanno partecipato tra gli altri Rita Paris, Direttrice del Museo Nazionale Romano di Palazzo Massimo, Giuliano Volpe, Presidente del Consiglio Superiore dei Beni Culturali, i rappresentanti delle imprese di settore, Emiliana Alessandrucci, Presidente del CoLAP e Cristian Perniciano, Presidente della Consulta delle Professioni. Resta centrale la problematica della definizione della figura professionale dell'archeologo: esiste una legge a firma Madia, Ghizzoni, Orfini (legge 110/2014) ancora in attesa dei decreti attuativi; è stata inviata alla Direzione Generale Educazione e Ricerca del MiBACT la definizione proposta dall'associazione.

La Confederazione presenterà nei prossimi giorni la propria domanda di riconoscimento al Ministero dello Sviluppo Economico, al fine di essere inserita tra le associazioni che regolano le professioni che non hanno albo, come stabilito dalla legge 4/2013. A fine giornata è stato rinnovato il Direttivo Nazionale dell'associazione con l'elezione di 25 nuovi membri che si riuniranno nei prossimi giorni per eleggere il nuovo Presidente.

R. C.



OLTRE L'EUROSCETTICISMO

L'Europa disgregata e le risposte dell'economia

di **Luca Ricolfi**

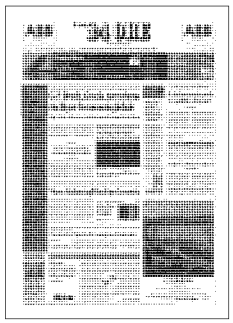
Sono ormai passati più di sedici anni da quando, nel marzo 2000 a Lisbona, il Consiglio Europeo ebbe a proclamare che l'Europa ambiva a «diventare l'economia basata sulla conoscenza più competitiva e dinamica del mondo, in grado di realizzare una crescita economica sostenibile con nuovi e migliori posti di lavoro e una maggiore coesione sociale».

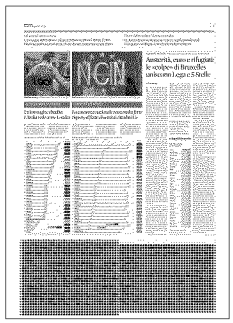
Quelle parole, pronunciate nel cuore dell'ultimo lungo periodo di crescita ininterrotta del Pil mondiale (il dodicennio 1995-2007), suonano oggi vagamente fuori luogo e fuori tempo. Nel periodo che ci separa dai sogni di Lisbona l'economia della Cina è cresciuta a un tasso medio annuo che sfiora il 10%, l'India al 7%, l'Africa oltre il 5%, l'America latina oltre il 3%. Quanto alle economie moderne, più o meno «basate sulla conoscenza», la crescita media ha superato di poco il 2%, ma con una chiarissima e netta gerarchia fra le varie aree dei Paesi Ocse: i Paesi extraeuropei sono cresciuti al 2,9%, i Paesi europei senza euro al 2,5%, i Paesi europei dell'Eurozona all'1,5% scarso, un ritmo che confina pericolosamente con un regime di stagnazione.

Il nucleo dell'Europa, quello che ha fondato la Comunità europea e promosso la nascita dell'euro, pare diventato l'area «meno dinamica del mondo». Su questo insuccesso economico dell'Europa si sono innestati i due grandi drammi che, da qualche anno, vanno stabilmente in scena nelle nostre vite: la crisi della Grecia e l'ondata migratoria. Due drammi che una classe dirigente europea divisa e confusa non pare minimamente in grado di affrontare.

Se questo è quel che è successo e sta succedendo, non possono stupire più di tanto i risultati del dossier sull'opinione pubblica europea, curato dalla Fondazione David Hume, che Il Sole 24 Ore pubblica oggi. Quel che colpisce, tuttavia, non è solo la forza delle correnti euroscettiche, ma quanto lontana nel tempo sia la loro origine. Un'occhiata alla traiettoria dell'euroscetticismo mostra nitidamente che la svolta nell'opinione pubblica non è avvenuta negli ultimi anni, sotto la pressione della crisi economica e dei flussi migratori, ma risale grosso modo agli anni della dissoluzione dell'impero sovietico.

Continua ▸ pagina 3





L'EDITORIALE. Dal sogno velleitario di Lisbona 2000 al rischio di rottura del 2016

LA RINASCITA PASSA DALL'ECONOMIA MA SERVE UNA VISIONE CONDIVISA

di **Luca Ricolfi**

▸ Continua da pagina 1

Se il primo decennio dell'Unione europea (dal 1979 al 1989) è stato un periodo di consenso crescente alle istituzioni comunitarie, i 25 anni successivi, pur fra qualche oscillazione, sono stati anni di crescita dei sentimenti antieuropei, soprattutto nelle loro espressioni e varianti di destra.

E alla crescita dei sentimenti si è accompagnata l'ascesa di decine di partiti più o meno xenofobi e populisti, più o meno antisistema, ma sempre invariabilmente accomunati dall'ostilità nei confronti della costruzione europea, degli immigrati, della burocrazia di Bruxelles.

Sulle cause generali di questa evoluzione (o involuzione) dell'opinione pubblica europea c'è un relativo accordo fra gli studiosi, ma si tratta di un accordo generico e non privo di sfumature e contrasti (vedi in proposito l'interessante analisi di Daniel Gros, pubblicata sul Sole 24 Ore il 19 maggio). Nessuno nega che la globalizzazione, la crisi economica, le ondate migratorie, le divisioni dei politici europei su tutte le materie calde (dalla politica economica alla questione delle frontiere) abbiano avuto un ruolo significativo nel disamorare le opinioni pubbliche dei vari paesi, ma nessuno sa ancora con ragionevole certezza quale sia stato l'ingrediente, o il cocktail di ingredienti, che ha avuto il ruolo decisivo nello smantellare il sogno europeo.

L'INSUCCESSO
Quella che avrebbe dovuto essere l'area più dinamica del mondo è oggi molto vicina a una vera stagnazione

LA CLASSE POLITICA
I dirigenti europei sanno di aver fallito ma non sembrano capire che cosa è successo, perché e come uscirne

Quale che sia stato il mix che ha fatto deflagrare la crisi europea, almeno un punto pare incontrovertibile: la classe dirigente europea, la stessa che 16 anni fa aveva baldanzosamente enunciato la strategia di Lisbona, non pare altrettanto disponibile ad enunciare una diagnosi, un bilancio, un resoconto disincantato. Sanno di aver fallito, perché è solo nel cuore dell'Europa che l'economia non è ancora uscita dalla crisi, ma non paiono interessati ad interrogarsi su che cosa non abbia funzionato. Eppure è di questo che i popoli europei avrebbero un disperato bisogno, per poter pensare il futuro, un futuro che non sia fatto solo di incertezza.

Se, a dispetto del permanente lamento per la crisi, il resto del mondo ha ripreso a crescere e l'Europa ancora balbetta, è inevitabile chiedersi: perché?

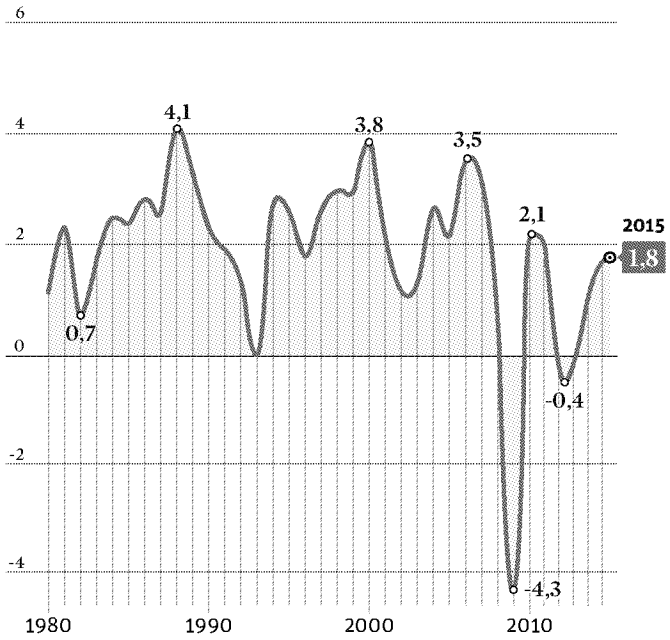
Sappiamo che le risposte a questa domanda sono numerose e divergenti. C'è chi invoca minore austerità, e pensa che ancora un po' di debito faccia bene all'economia. C'è chi vorrebbe mettere in comune il debito pubblico europeo. C'è chi, tutto al contrario, crede che solo con bilanci in ordine potremo tornare a crescere. C'è chi pensa che la chiave di tutto siano gli investimenti pubblici. C'è chi si aspetta che la salvezza venga dai tedeschi, quando si decideranno a fare debito e aumentare i salari. C'è chi fa notare che le tasse sono troppo alte, e chi sottolinea che il welfare europeo è divenuto insostenibile. Per non parlare della crisi dei migranti: c'è chi vorrebbe rimandarli a casa, e chi vorrebbe tenere le porte sempre aperte; c'è chi vorrebbe proteggere le frontiere esterne dell'Unione, e chi pensa che l'imperativo numero uno sia salvare vite umane in mare.

Il guaio è che tutte queste opinioni non dividono solo o tanto cittadini e studiosi, ma dividono innanzitutto i politici europei. E la divisione crea paralisi, frustrazione, senso di impotenza. Sentimenti che un'uscita del Regno Unito dall'Europa non potrebbe che rafforzare.

Ecco perché i contrasti e i silenzi dei nostri governanti sono inquietanti. Possiamo non sapere quale sia la diagnosi giusta. Ma almeno un paio di cose le sappiamo. La prima è che la disgregazione dell'Europa non è la soluzione. La seconda è che una diagnosi condivisa, che permetta di formulare una politica coerente, è la condizione minima per restituire un po' di speranza ai popoli europei.

Il tracollo che ha lasciato il segno

Andamento storico del Pil dell'intera Unione europea (dollari internazionali PPP del 1990): variazioni percentuali per la Ue come risulta dai progressivi allargamenti



Fonte: Fondazione Hume per Il Sole 24 Ore, 2016 (su dati GGDC Total Economy Database)