“VOGLIO PIANGERE”

di Giuliano Marrucci
collaborazione Alessia Marzi
montaggio Daniele Bonazza

SIGFRIDO RANUCCI IN STUDIO
Siamo nell’era dell’internet delle cose: ci sono televisori intelligenti, lavatrici intelligenti, controlliamo il nostro sistema di riscaldamento da remoto. Ma qual è il prezzo da pagare per questa libertà e questa comodità? E se la nostra lavatrice intelligente diventasse un giorno strumento di un attacco informatico tra stati? Giuliano Marrucci.

GIULIANO MARRUCCI FUORI CAMPO
I negozi di elettrodomestici ormai sembrano succursali della NASA.

RIVENDITORE
Quello è un televisore che ha otto processori dentro, quindi, è quasi un computer veramente.

GIULIANO MARRUCCI FUORI CAMPO
C'è la lavatrice che posso controllare dall'ufficio.

RIVENDITORE 1
Uno dice: preparo la lavatrice, ora vado via. Poi io so che tanto esco alle due, quindi magari a mezzogiorno e mezzo la faccio partire, dopo un'ora e mezza io arrivo a casa ed è perfetto.

GIULIANO MARRUCCI FUORI CAMPO
Il frigo che mi aiuta a fare la spesa.

RIVENDITRICE 2
Ha tre fotocamere interne quindi ti guarda quello che c'è nel frigo e poi ti dà le ricette per i vari piatti.

GIULIANO MARRUCCI FUORI CAMPO
Il termostato intelligente.

RIVENDITORE 1
Praticamente te riesci a controllare anche da fuori se la caldaia è accesa, a che temperatura vuoi che sia la casa quando arrivi a casa.

GIULIANO MARRUCCI FUORI CAMPO
E le telecamere che funzionano anche come allarmi.

RIVENDITORE 1
Ti arriva proprio la mail quando entra qualcuno, quando si avvicina qualcuno poi dopo uno si connette e vede effettivamente cosa sta succedendo.

GIULIANO MARRUCCI
Ma non è che questa roba poi dal punto di vista della sicurezza informatica mi crea qualche problema?

RIVENDITORE 1

No, non c'è niente di particolare.

RIVENDITRICE 5
Ora è tutto connesso su internet, sono tutti dispositivi fatti con sicurezza.

GIULIANO MARRUCCI
Quindi non è che il primo hacker che passa mi entra dentro al sistema?

RIVENDITORE 3
Ti hackerano la tv e? e guardano se hai guardato Canale 5 o Rai1? Che cazzo gliene frega!

GIULIANO MARRUCCI FUORI CAMPO
Dalla gita tra i grandi magazzini torno a casa con questo oggetto, si chiama IP Camera. La attacco alla mia rete casalinga, inserisco username e password scritte nel manuale e da quel momento la posso guardare da internet ovunque sono. Il problema è che poco dopo a guardare la mia telecamera c'è anche qualcun altro, a mia insaputa.

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Siamo entrati, si vede l'immagine video e posso addirittura muovere la telecamera dove voglio io. La definizione è così buona che potrei addirittura vedere le lettere che digita e catturare un'eventuale password.

GIULIANO MARRUCCI FUORI CAMPO
Cioè, io metto la telecamera per controllare cosa succede quando sono assente e invece dalla stessa telecamera i criminali mi possono spiare. Igor Falcomatà è un esperto di sicurezza e un punto di riferimento della comunità hacker italiana. Ma a bucare una telecamera come ha fatto adesso non ci vuole la scienza, basta ad esempio un motore di ricerca come questo che si chiama Shodan, ed è una specie di Google dell'internet delle cose e che con un click di telecamere come la mia ne trova oltre 38mila in tutto il mondo.

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Nel momento in cui tu hai attaccato la tua telecamera alla tua rete interna, lei ha parlato con il router, ha chiesto di essere visibile da internet e a quel punto chiunque su internet poteva raggiungere la tua telecamera.

GIULIANO MARRUCCI FUORI CAMPO
Cioè, la telecamera si è rivolta al dispositivo che serve per andare su internet, il router, è diventata visibile a tutti e se uno mi vuole spiare e attaccare, lo può fare anche perché io ingenuamente non ho cambiato la password di fabbrica.

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
A quel punto ho provato a collegarmi alla tua telecamera con le password preimpostate in fabbrica dal produttore che tu non avevi cambiato.

GIULIANO MARRUCCI
E te come facevi a conoscerle?

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Ho cercato WiFicam default password e ho trovato la password di default.

GIULIANO MARRUCCI
Quindi è come se avessi lasciato le chiavi di casa sulla toppa insomma?

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
In sostanza sì. Il problema è che nella tua stessa situazione mi immagino che su internet ci siano centinaia di migliaia di persone.

GIULIANO MARRUCCI FUORI CAMPO
Controlliamo su Shodan. Il primo non va, il secondo nemmeno. Il terzo è un italiano. E questa volta funziona. Stiamo vedendo quello che vede lui da dentro casa. La telecamera l'ha puntata all'esterno verso il cancello.

GIULIANO MARRUCCI
Quindi la prima cosa appena ti connetti, cambia password e nome utente.

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
La base è esattamente quella, sarebbe sicuramente opportuno che i produttori ti imponessero di cambiare la password, che ti imponessero di aggiornare il firmware, purtroppo non tutti i dispositivi lo fanno.

GIULIANO MARRUCCI FUORI CAMPO
E allora proviamo a cambiare le credenziali, quindi mettiamo username REPORT e password RAI3, ma in pochi attimi le nuove credenziali appaiono anche sullo schermo di Igor.

GIULIANO MARRUCCI
Ma come hai fatto?

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Nella tua telecamera c'è una vulnerabilità che permette molto semplicemente di farsi dare le nuove credenziali impostate. Pensa che questa vulnerabilità qua è stata scoperta nel 2004.

GIULIANO MARRUCCI
E vale solo per questa telecamera?

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Il software di questa telecamera viene usato su circa 1250 modelli di telecamera.

GIULIANO MARRUCCI FUORI CAMPO
Una volta che sei entrato nella mia telecamera, oltre a spiarmi, puoi fare un sacco di altre cose.

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Posso modificare il tuo software e posso usarla come testa di ponte per arrivare a tutte le macchine che tu hai sulla tua rete interna, il tuo PC, il tuo NAS con i tuoi video.

GIULIANO MARRUCCI FUORI CAMPO
Per evitare i rischi che arrivano da stare direttamente esposti su internet, gran parte di questi prodotti in realtà comunica tramite una app specifica. Questa è quella della mia telecamera. Ma anche in questo caso...

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Eccola qui... sono le credenziali quelle nuove che Giuliano ha inserito nella sua app.

GIULIANO MARRUCCI
Cos'è successo?

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Tutto quello che tu trasmetti viene inviato senza crittografia. Se tu sei in un hotspot pubblico, in una rete wireless pubblica e c'è un attaccante lì, può catturare il numero seriale della telecamera, le tue credenziali, e da quel momento in poi può controllare la tua telecamera come se fossi te.

GIULIANO MARRUCCI
Ma è particolarmente un cesso la mia app in questo caso, o è una roba...

IGOR "KOBA" FALCOMATÀ – SIKUREZZA.ORG
Questo tipo di vulnerabilità è abbastanza diffusa anche se in questo specifico caso questa applicazione è fatta particolarmente male.

SIGFRIDO RANUCCI IN STUDIO
Vulnerabili al punto da diventare strumenti di attacchi informatici anche tra stati. Accade così che ogni giorno centinaia di migliaia di software tentano di infettare gli oggetti connessi in rete. Attraverso un worm che può colpire anche la nostra lavatrice, se è connessa, la nostra lavatrice intelligente che entra così se infettata a far parte di una rete: la "botnet", attraverso la quale si può sferrare un attacco informatico tra stati. Ecco sembra fantascienza Ma in realtà è già accaduto. Gli attacchi tra stati sono serviti a mantenere o cambiare gli equilibri di geopolitica.
Cosa diversa invece sono gli attacchi di spionaggio industriale, la cui diciamo ricaduta la puoi scoprire a distanza di anni. Dieci anni fa la Cina ha dato atto al più grande furto di dati della storia. Ha rubato i segreti di aziende americane, di aziende statunitensi in materia di energia, chimica, e grande distribuzione. Voi direte ma a noi cosa importa? Importa perché poi questo furto consentito di produrre a basso costo e di mettere sul mercato dei prodotti a prezzi stracciati mettendo in ginocchio un'economia. E poi cosa ci può importare per esempio se i cinesi rubano i segreti militari degli Stati Uniti? Ci importa perché alla fine potremmo pagare un aereo per la nostra difesa militare più del dovuto.

GIULIANO MARRUCCI FUORI CAMPO
A partire dagli anni '90 cominciano ad apparire programmi chiamati worm, che significa baco. Cercano sulla rete i dispositivi da infettare in modo automatico. I dispositivi infettati da uno stesso baco entrano a far parte di una rete, la botnet, che può essere utilizzata per lanciare un attacco DDOS. ovvero: il pc di casa diventa uno zombie che a nostra insaputa è utilizzato per bombardare di dati un punto specifico della rete, fino a mandarlo in tilt. Che è quello che è successo nel 2007 in Estonia.

MIKKO HYPPONEN – CRO F-SECURE
Dopo due giorni di scontri per strada tra governo e minoranza russa, abbiamo visto questa grande botnet mettere fuori uso i siti web del parlamento estone, del presidente, di alcuni ministeri, ma anche delle banche principali e di alcuni negozi online.

GIULIANO MARRUCCI FUORI CAMPO
Dieci anni dopo la mappa globale degli attacchi DDOS in tempo reale appare così.

CARLOS MORALES – ARBOR NETWORKS
Quello che è cambiato rispetto a 10 anni fa è che allora su internet sostanzialmente c'erano solo i computer. Creare una botnet di computer è complicato, perché spesso vengono spenti, i dischi vengono puliti, magari ci sono degli antivirus. I nuovi dispositivi consentono di creare botnet molto più grandi, perché sono estremamente insicuri, spesso non vengono spenti per lunghi periodi, e se vengono infettati nessuno se ne accorge.

GIULIANO MARRUCCI FUORI CAMPO
Uno di questi oggetti che partecipano all'attacco potrebbe essere il nostro frigorifero "intelligente" o la telecamera per controllare che nostro figlio stia dormendo tranquillo, come è successo l'estate scorsa, quando un baco di nuova generazione chiamato Mirai ha lanciato un attacco seimila volte superiore a quello che aveva colpito l'Estonia.

CARLOS MORALES – ARBOR NETWORKS
Per adesso Mirai si è limitata a mettere fuori uso per qualche ora giganti del web come Twitter o Reddit, ma attacchi di queste dimensioni rischiano ormai di mettere fuori uso tutto internet in intere aree geografiche, proprio come è successo in Estonia, e dopo anche in Libia, in Egitto, in Liberia.

GIULIANO MARRUCCI FUORI CAMPO
L'utilizzo dello spazio cibernetico per azioni di sabotaggio tra stati è ormai una realtà.
La prima vera e propria arma cibernetica è stata scoperta nel 2010 in Iran. Si chiama stuxnet, ed è stata sviluppata ad hoc da americani e israeliani per danneggiare le centrifughe responsabili dell'arricchimento dell'uranio nella centrale nucleare di Natanz. Visto che la centrale è isolata da internet, stuxnet doveva essere in grado di fare tutto da sola senza ricevere istruzioni dall'esterno e c'è riuscita per quasi due anni mettendo fuori uso circa duemila centrifughe.
A dicembre 2015 è il turno dell'Ucraina: il virus Black Energy attribuito ai russi mette ko tre gestori della rete elettrica lasciando al freddo e al buio 240 mila persone. Ma azioni di guerra come queste rimangono comunque una rarità. Mentre quello che avviene continuamente, è lo spionaggio. Soprattutto cinese.

SHANE HARRIS – THE WALL STREET JOURNAL
Alla fine dell'amministrazione Bush il Pentagono ha scoperto una serie di infiltrazioni nei sistemi informatici della difesa. In particolare si pensa siano stato rubate informazioni riservate sull'F-35, tant'è che quando un paio di anni dopo i cinesi hanno presentato il loro nuovo aereo militare, assomigliava moltissimo proprio all'F-35.
E in molti sostengono che una parte consistente dei ritardi e dell'aumento dei costi dell'F-35 siano dovuti proprio a questa attività di spionaggio, che ha costretto a riprogettare molti sistemi da capo.

GIULIANO MARRUCCI FUORI CAMPO
Will Glass è uno dei principali esperti di sicurezza cibernetica dell'americana FireEye, che da dieci anni indaga su attività di spionaggio commerciale attribuite agli hacker cinesi.

WILL GLASS - FIREEYE
A partire dal 2005- 2006, una quantità enorme di aziende americane hanno iniziato a subire infiltrazioni delle loro reti informatiche, con conseguente furto di informazioni protette da proprietà intellettuale. E indagando siamo riusciti a collegare tutti questi attacchi e risalire a un unico autore che abbiamo chiamato APT1.

GIULIANO MARRUCCI
E di che tipo di aziende stiamo parlando?

WILL GLASS - FIREEYE
Un'infinità di aziende diverse, oltre 140, dall'energia, alla chimica, la logistica, la difesa, e anche la grande distribuzione.

SHANE HARRIS – THE WALL STREET JOURNAL
È stato definito il più grande trasferimento di ricchezza della storia. Un gigantesco sforzo coordinato dal governo per far recuperare almeno parte del ritardo tecnologico cinese attraverso il furto di proprietà intellettuale americana.

WILL GLASS - FIREEYE
Per la prima volta siamo riusciti a risalire addirittura a un singolo edificio a Shanghai da cui partiva il grosso di questi attacchi. E poi abbiamo scoperto che questo edificio era la sede dell'unità 61398, che è la costola dell'esercito popolare di liberazione che si occupa di spionaggio informatico e di intercettazioni.

GIULIANO MARRUCCI FUORI CAMPO
Anche il governo americano ha il suo programma di spionaggio cibernetico, come ci spiega Bruce Schneier, il guru mondiale della sicurezza informatica che ha scavato a lungo dentro il milione di file riservati trafugati ormai quattro anni fa da Edward Snowden.

BRUCE SCHNEIER – IBM RESILIENT
Gli Stati Uniti hanno tre vantaggi enormi. Il primo, è che il grosso del traffico internet passa da qui. Tutto il traffico che dall'America Latina va verso l'Europa passa dalla Florida. E anche molto del traffico da e per l'Asia passa attraverso gli Stati Uniti. E questo ci rende più facile intercettare il grosso delle comunicazioni che avvengono nel mondo. Il secondo è che le principali aziende tecnologiche sono americane, e questo ci permette di influenzare prodotti che poi arrivano in tutto il mondo. E il terzo è che l'NSA, l'Agenzia per la Sicurezza Nazionale statunitense, e la CIA, spendono da sole più soldi per spionaggio e sorveglianza di tutto il resto del mondo messo insieme.

GIULIANO MARRUCCI FUORI CAMPO
L'intelligence americana analizza i sistemi che vuole attaccare fino a che non trova un varco nella sicurezza.

ROB JOYCE – CAPO SICUREZZA INFORMATICA NSA
Perché abbiamo successo? Perché facciamo tutto il possibile per conoscere perfettamente i sistemi che attacchiamo, fino a che non li conosciamo meglio di chi li ha progettati, e di chi li dovrebbe proteggere.

GIULIANO MARRUCCI FUORI CAMPO
Ma quando scoprono una vulnerabilità di sistema, invece di lanciare l'allarme se la tengono segreta.

BRUCE SCHNEIER – IBM RESILIENT
Il che ci permette di attaccare con più efficacia i nostri avversari, ma rende internet meno sicuro, perché basta una fuga di notizie e quelle vulnerabilità possono essere utilizzate da chiunque.

GIULIANO MARRUCCI FUORI CAMPO
È esattamente quanto è successo con WannaCry, il virus ha gettato nel panico mezzo mondo, e che impone di pagare un riscatto per riavere indietro i file rubati dai nostri computer. Era in circolazione già da marzo, ma non era riuscito a diffondersi a dovere. Fino a quando una fuga di notizie ha fatto circolare un codice di attacco sviluppato proprio dall'NSA sfruttando una vulnerabilità di Windows. Qualcuno l'ha aggiunto a Wannacry, e in poche ore è scoppiato il disastro.

GIULIANO MARRUCCI
Se l'NSA invece che tenersela per sé, l'avesse comunicata, tutto questo bordello che è successo non ci sarebbe stato?

GIUSEPPE AUGIERO - ESPERTO SICUREZZA INFORMATICA
Probabilmente sarebbe stato un virus molto più mediocre, così come era fin dall'inizio.

GIULIANO MARRUCCI FUORI CAMPO
Martedì, il gruppo di hacker responsabile della fuga di notizie dall'NSA ha pubblicato un lungo articolo dove dichiara che da giugno rilascerà altro codice trafugato per attaccare browser, router e versioni più aggiornate di Windows.

SIGFRIDO RANUCCI IN STUDIO
Tutti si lamentano, ma poi se qualcuno denuncia gli fanno passare i guai. È successo a Edward Snowden, ex informatico dell'Agenzia Nazionale di Sicurezza americana, che rivelato, diffuso dei file secretati, e aveva fatto scoprire che la Cia e i servizi segreti americani spiavano i governi di mezzo mondo. È costretto a vivere in Russia, al riparo dalle accuse dei giudici statunitensi che potrebbero costargli l'ergastolo. Julian Assange invece attraverso il suo sito Wikileaks ha pubblicato, ha reso pubblici documenti strategici dell'amministrazione statunitense e da sette anni vive chiuso in un'ambasciata ecuadoregna a Londra. Bene, poche ore fa, ha diffuso la notizia, Wikileaks il suo sito, che Microsoft, dopo aver diffuso il suo prodotto Windows 10, praticamente è stato oggetto dell'attenzione della Cia, che avrebbe brigato per renderlo più vulnerabile. L'impressione è che si voglia, si preferisca una rete debole e che noi utenti non possiamo fare altro che subire i danni collaterali di una guerra informatica tra stati dove negli ultimi tempi un certo ruolo l'ha avuto la Russia di Putin.

GIULIANO MARRUCCI FUORI CAMPO
Anton Nossik è un blogger indipendente, ed è considerato uno dei padrini dell'internet russo.

ANTON NOSSIK – GIORNALISTA
Quello che accade regolarmente da almeno una decina di anni a questa parte è che appena il governo russo individua un nemico, poco dopo viene attaccato da qualche hacker. È successo nel 2007 in Estonia, è successo l'anno dopo in Georgia, e succede continuamente a chiunque provi a fare un minimo di opposizione a Putin.
Il fatto è che la Russia non ha leggi moderne contro il cyber crimine, e questo ha favorito lo sviluppo di una comunità hacker che per dimensioni e livello di competenze non ha pari al mondo. Ma invece di metterli in prigione, gli chiedono favori in cambio di una specie di immunità. E così oggi non c'è un singolo hacker che non compia anche commissioni per conto di un qualche ufficiale delle forze dell'ordine o dei servizi di intelligence.

GIULIANO MARRUCCI FUORI CAMPO
Tra i gruppi che si presume operino in questa terra di confine tra stato e criminalità, ce n'è uno noto come apt28 che è stato accusato di aver hackerato la rete del partito democratico durante le presidenziali Usa, e di aver poi passato i documenti a Wikileaks per conto del governo russo.

JUAN ANDRÉS GUERRERO-SAADE – KASPERSKY LAB
Noi siamo sempre molto scettici su questo tipo di attribuzioni, perché vengono fatte in base ad indizi che possono essere facilmente falsati o manipolati. Non voglio dire che sia impossibile identificare l'autore di un attacco, ma sicuramente è molto più difficile di quanto ci vorrebbero lasciar credere.

GIULIANO MARRUCCI FUORI CAMPO
Per confondere le acque la CIA, ad esempio, ha costituito un'unità speciale che colleziona pezzi di software malevolo "prodotto in altri stati, compresa la Russia". Così possono lasciare le impronte digitali della Russia sulla scena di un crimine. Ma la Russia da parte sua è sospettata di essere dietro l'enorme mole di bufale circolate, in particolare su Facebook, durante la campagna presidenziale, e che avrebbero favorito l'elezione di Trump.

CRAIG SILVERMAN - BUZZFEED
Una delle bufale che ha avuto più successo durante la campagna elettorale è stata la storia del sostegno di Papa Francesco a Donald Trump. Poi c'è quella dei 3500 dollari pagati a una persona semplicemente per andare a un comizio di Trump e contestarlo. Questa storia poi è stata condivisa da due membri dello staff elettorale di Trump.
Considerate che negli ultimi tre mesi di campagna, le 20 bufale principali hanno avuto più like e condivisioni delle 20 principali notizie "tradizionali".

GIULIANO MARRUCCI
Ma chi è che fabbrica queste bufale?

CRAIG SILVERMAN - BUZZFEED
Quello che abbiamo trovato è un gruppo di 140 siti in lingua inglese tutti provenienti da un paesino della Macedonia: tutti dichiaratamente pro-Trump, e tutti pieni di notizie false al 100%. Facendo due indagini abbiamo scoperto che si trattava di ragazzini locali che pochi mesi prima avevano provato a fare la stessa cosa anche con Bernie Sanders, ma poi avevano realizzato che i sostenitori di Trump erano molto più propensi a condividere ogni genere di contenuto, e che gli avrebbero fatto guadagnare un sacco di quattrini.

GIULIANO MARRUCCI
Quindi alla fine il ruolo della Russia in tutta questa faccenda?

CRAIG SILVERMAN - BUZZFEED
Nessuno è mai riuscito a dimostrare che una di queste bufale sia partita dalla Russia. Discorso diverso invece vale per gli account Twitter. Ci sono ormai numerose prove sull'esistenza di account Twitter che si spacciano per americani, ma che in realtà pensiamo facciano parte di una campagna coordinata che parte dalla Russia.

GIULIANO MARRUCCI FUORI CAMPO
L'intelligence allora decide di puntare il dito contro un canale tv all news a cui Putin negli ultimi dieci anni ha garantito finanziamenti per oltre due miliardi. Si chiama RT, e gli è stata dedicata gran parte del rapporto che ha portato all'espulsione di 35

diplomatici russi dagli Stati Uniti. Noi siamo andati a incontrarli nella sede principale di Mosca, dove ci sono tutti gli studi e da dove trasmettono 24 ore su 24 in quattro lingue in tutto il mondo.

ANNA BELKINA – CAPO COMUNICAZIONE RUSSIA TODAY
Oggi vediamo chiaramente che tra i nostri servizi, quelli che hanno maggior successo sono proprio quelli che propongono una prospettiva completamente diversa su storie che il pubblico pensava di conoscere già.

GIULIANO MARRUCCI FUORI CAMPO
Tra gli esperti interpellati dalla tv russa c'è il defunto giornalista tedesco Udo Ulfkotte, che sosteneva fosse in corso una "jihad delle feci", fatta da donne turche che defecano sulle fragole destinate all'esportazione. Oppure l'ex star della tv americana Roseanne Barr, che sostiene che le menti delle Star di Hollywood siano controllate dalla CIA.

ROSEANNE BARR
Il controllo mentale avviene grazie ai farmaci, ti ricordi e dimentichi di nuovo le cose in continuazione, nascondi oggetti senza rendertene conto e poi li ritrovi dopo anni nei luoghi più impensabili. Ma soprattutto diventa normale tollerare cose che altrimenti sarebbero intollerabili, che è esattamente la cosa di cui un governo ha bisogno per controllare le azioni di un popolo.

GIULIANO MARRUCCI FUORI CAMPO
Karen Hudes ha lavorato per vent'anni come avvocato presso la Banca Mondiale, e sostiene che il vaticano sia controllato da una strana specie che chiama homo capensis.

KAREN HUDES
Non sono umani, tant'è che se si accoppiano con gli umani, la progenie è sterile. All'apparenza però sono del tutto simili agli esseri umani, a parte questo cranio enorme, che è il motivo per cui in vaticano vanno così tanto questi strani cappelli. Ed è il motivo per cui anche il primo ebreo, Mosè, portava uno di questi strani cappelli.

GIULIANO MARRUCCI
E in questo modo sul serio RT riesce a influenzare l'opinione pubblica americana?

VASILY GATOV – UNIVERSITY OF SOUTHERN CALIFORNIA
No, aspetta, ascoltami. In America dicono di avere due milioni di telespettatori, ma ascoltate ragazzi, potete provare a raccontarlo a Putin, di sicuro non a noi che stiamo in America. In America una tv con due milioni di spettatori sarebbe piena di pubblicità. Su RT non ce n'è neanche l'ombra. E il motivo è estremamente, estremamente semplice: in America nessuno guarda RT.

GIULIANO MARRUCCI FUORI CAMPO
Dopo le presidenziali americane invece si è deciso di rilanciare. L'Unione Europea ha creato una task force ad hoc con una decina di funzionari che di lavoro contrastano bufale e propaganda russa. E a febbraio è stato presentato al Senato italiano un disegno di legge che prevede fino a due anni di reclusione per chi diffonde bufale, e che si basa sulla "sensazione diffusa che la disinformazione prevalga sull'informazione oggettiva". Per trovare qualcuno che non si basi solo su una "sensazione", siamo dovuti venire fino a qua, la prestigiosa università di Stanford, California.

MATTHEW GENTZKOW – STANFORD UNIVERSITY

Abbiamo fatto una serie di interviste, da cui è emerso che gli elettori americani al momento del voto si ricordavano in media soltanto una delle bufale circolate durante la campagna. E abbiamo scoperto che questa bufala, per influenzare concretamente il voto, sarebbe dovuta essere 36 volte più persuasiva di uno spot elettorale tradizionale. Quindi, in soldoni, Trump sarebbe presidente anche in un mondo senza fake news.

SIGFRIDO RANUCCI IN STUDIO
Beh non sappiamo poi alla fine quanto questa cosa ci rassicuri. Insomma che cosa è successo, questo almeno ci dicono: che un gruppo di ragazzini, da un paese sperduto dei Balcani, entra a gamba tesa nella competizione elettorale di una delle più grandi democrazie del mondo e fabbrica fake news perché sono più gradite delle notizie vere. Tutto questo per guadagnare 2 euro circa ogni mille clic. Poi poco importa se c'è un elettore sprovveduto che se la beve e fa la scelta sbagliata per il proprio paese. Diciamo che fra le libertà che offre la rete c'è anche questo prezzo da pagare.