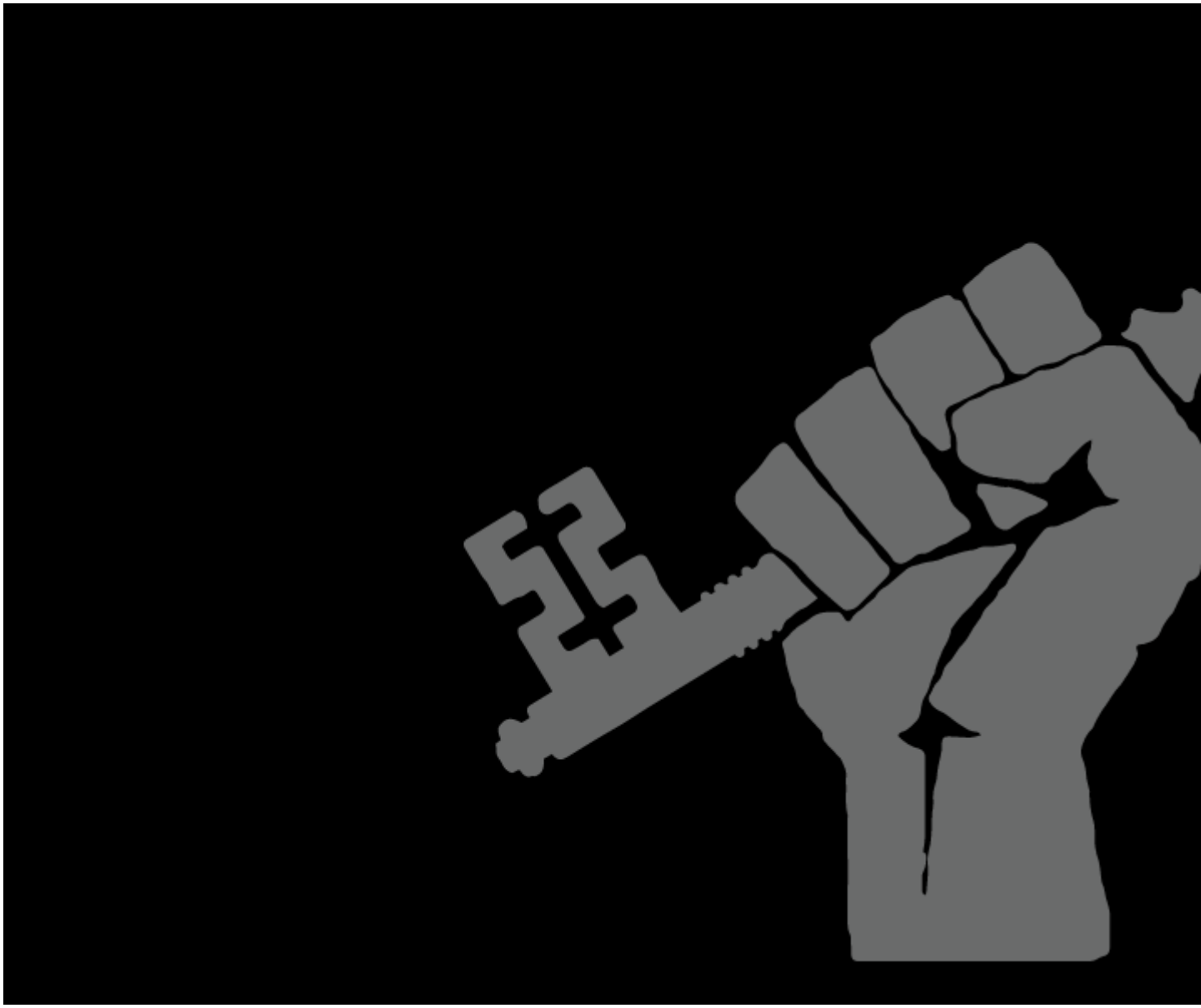
I funzionari dell'amministrazione Biden in arrivo dovrebbero cambiare rotta sulla crittografia

Di Joe Mullin
4 febbraio 2021



Per avere privacy e sicurezza nel mondo digitale, la crittografia è un ingrediente indispensabile. Senza di essa, siamo tutti a rischio di sfruttamento da parte di governi autoritari, polizia di vasta portata, società ficcanaso e criminali online.

Ma da alcuni anni, le forze dell'ordine federali hanno prestato fede alla "sicurezza informatica", mentre in realtà cercano di renderci tutti meno sicuri . Funzionari come l'ex procuratore generale William Barr, il direttore dell'FBI James Comey e numerosi altri hanno affermato che la crittografia

diffusa rappresenta un grave pericolo per le indagini a causa del rischio di "oscuramento" e hanno invitato le aziende tecnologiche a progettare sistemi sicuri che consentano al governo per accedere ai contenuti dei dati crittografati su richiesta. Ma semplicemente non è possibile combinare sistemi protetti e crittografati con una speciale "backdoor" per consentire alle forze dell'ordine di accedere, indipendentemente da come lo chiami .

Non ci sono chiavi d'oro né proiettili magici. È ora che le forze dell'ordine e i funzionari dell'intelligence lo riconoscano e lo dicano pubblicamente. Sfortunatamente, il personale chiave che è già stato selezionato per la nuova amministrazione del presidente Biden non ha una storia stimolante su questo argomento.

Cominciamo con il direttore dell'FBI Christopher Wray, che continua dall'amministrazione Trump come parte di un mandato standard di dieci anni. Ha affermato più volte che alle forze dell'ordine dovrebbe essere concesso un accesso eccezionale alle conversazioni crittografate e ha descritto la "crittografia predefinita controllata dall'utente" come una "vera sfida per le forze dell'ordine".

Avril Haines, che è stato confermato come il nuovo direttore dell'intelligence nazionale, faceva parte di un gruppo di esperti sponsorizzato dal Carnegie Institute for Peace per avviare un dibattito più "pragmatico e costruttivo" sulla crittografia. Il del gruppo Carnegie è rapporto stato pubblicato nel 2019 e per i sostenitori della crittografia e della privacy è stato deludente . Invece di riconoscere le realtà tecnologiche della crittografia, ha puntato su una serie di domande importanti e ha offerto una variante di uno schema di "deposito delle chiavi" per i dispositivi crittografati, un approccio screditato che è stato proposto e giustamente rifiutato per decenni .

Lisa Monaco, nominata del presidente Biden per il vice procuratore generale, è stata anche una coautrice del rapporto Carnegie. Il procuratore generale Merrick Garland, anch'esso ancora non confermato, non ha una chiara registrazione sulla crittografia, ma ha una lunga storia come procuratore federale.

Indipendentemente dal background dei funzionari, una nuova amministrazione presidenziale è un'opportunità per un nuovo percorso. Abbiamo già inviato il nostro promemoria di transizione al team di Biden , raccomandando al nuovo presidente di adottare una politica formale a favore della crittografia e rinnegando qualsiasi tentativo di indebolire la sicurezza digitale, inclusa l'introduzione di backdoor di crittografia. Questi funzionari chiave devono ripudiare le loro dichiarazioni fuorvianti secondo cui l'indebolimento della crittografia e della sicurezza informatica è necessario per la sicurezza pubblica. Non lo è e non lo è mai stato.