BULETIN SPECIAL
CYBERINT

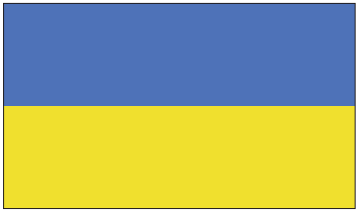

Backspace
Enter
Attack

CONTEXT **INTERNAȚIONAL**

Interferențele în alegeri ale unor actori cu relevanță geostrategică, care au utilizat inclusiv mijloace specifice spațiului cibernetic, au căpătat amploare încă din 2016, cu ocazia alegerilor prezidențiale din Statele Unite ale Americii. Principalii factorii favorizanți pentru imixtiunea în alegeri sunt reprezentați de dezvoltarea tehnologiilor IT&C și social media și intersectarea acestora cu viața politică și socială.

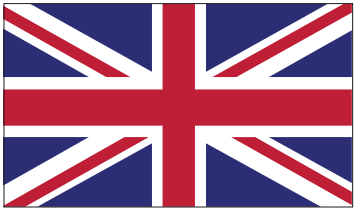
Odată cu crearea și implementarea la scară largă a acestor tehnologii au fost identificate noi vulnerabilități pe care actorii cibernetici le pot exploata, imixtiunea în procesele socio-politice la nivelul altor state, fiind unul dintre scopurile urmărite de aceștia în ultimii ani. Printre efectele urmărite se regăsesc afectarea încrederii publice în instituțiile democratice, exploatarea tensiunilor societale și influențarea rezultatului alegerilor democratice.

În ultimii cinci ani au fost identificate mai multe cazuri în care actori geostrategici s-au implicat prin folosirea unor capabilități cibernetice în influențarea rezultatului alegerilor din state de interes.



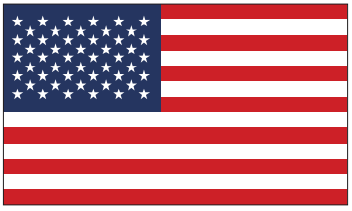
Alegerile prezidențiale din Ucraina , 25 mai 2014

Cu câteva zile înaintea derulării votului, gruparea de hackeri **CyberBerkut**, asociată în mediul specialiștilor unui actor statal, a compromis și blocat sistemul informatic al **Comisiei Centrale de Alegeri din Ucraina** și a distribuit în mod neautorizat în mediul online corespondență e-mail cu relevanță în contextul scrutinului. În cele din urmă, instituția ucraineană a repornit sistemul prin folosirea backup-urilor existente, însă ulterior a fost țința unor noi atacuri prin care s-a întârziat afișarea rezultatelor finale, încercându-se totodată afișarea unui rezultat fals.



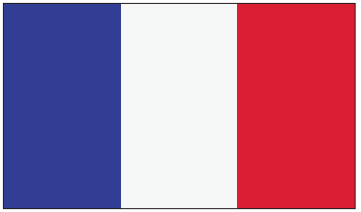
Referendumul din Marea Britanie „Brexit", 23 iunie 2016

În perioada premergătoare referendumului pe tema Brexit-ului, prin utilizarea unor *rețele de boți*, a fost derulată o campanie social-media agresivă pe *Twitter*, în cadrul căreia au fost postate și distribuite multiple mesaje pro-Brexit. În urma analizelor suplimentare ale specialiștilor în securitate cibernetică s-a stabilit că aceste conturi aparțineau organizației rusești **Internet Research Agency (IRA)**, care a încercat să influențeze rezultatul votului.



Alegerile prezidențiale din SUA, 8 noiembrie 2016

Alegerile din SUA au fost țința unor atacuri din partea actorilor cibernetici din Federația Rusă, care au derulat o campanie de subminare a încrederii publice în procesul democratic, concomitent cu denigrarea candidatului democratic Hillary Clinton. Aceste acțiuni au început din anul 2014 și au fost orientate către delegitimizarea procesului electoral, prin răspândirea de *fake-news* utilizându-se conturi special create pe rețele de socializare. O altă metodă de interferență în perioada premergătoare alegerilor a fost compromiterea infrastructurilor IT&C ale organizațiilor politice americane, *Democratic National Committee și Democratic Congressional Campaign Committee* ulterior fiind exfiltrate și distribuite neautorizat email-uri și documente menite să afecteze candidatura lui Hillary Clinton.



Alegerile prezidențiale din Franța, 7 mai 2017

În data de 5 mai 2017, cu două zile înainte de alegerile prezidențiale franceze, nouă gigabiți de date exfiltrate cu privire la campania lui Emmanuel Macron, inclusiv documente și e-mail-uri, au fost postate online pe site-ul de sharing Pastebin și ulterior pe site-ul 4Chan.
Printre documentele autentice publicate de actorii cibernetici se regăseau inclusiv documente false, special concepute pentru a crea neîncredere și dezinformare în rândul populației franceze.

Alegerile federale din Germania, 24 septembrie 2017

În anul 2015 a fost derulat un atac cibernetic persistent prin care au fost exfiltrate date (în principal corespondență electronică) de la mai multe instituții/organizații politice, inclusiv *Bundestag* (camera inferioară a Parlamentului german) și birourile de stat ale cancelarului Angela Merkel.
Pe lângă furtul de date, în anul 2016 trusturile de media rusești au realizat acțiuni de dezinformare prin lansarea de *fake news* ceea ce a condus la amplificarea problemelor existente și a tensiunilor interne.
Această acțiune este similară celei folosite în campania electorală din SUA prin intermediul rețelelor de boți, care au distribuit mesaje cu privire la fraude electorale.

CONTEXT **NAȚIONAL**

Având în vedere că, în anul 2019, în România vor avea loc două scrutine electorale (alegerile pentru Parlamentul European și alegerile prezidențiale), **există posibilitatea ca actori cu relevanță geostrategică să acționeze folosind capabilități cibernetice pentru a influența procesul electoral și, implicit, rezultatul alegerilor.**

La nivel național, **Autoritatea Electorală Permanentă** este instituția administrativ-autonomă cu personalitate juridică și cu competență generală în materie electorală și are misiunea de a asigura organizarea și desfășurarea alegerilor și a referendumurilor, precum și finanțarea partidelor politice și a campaniilor electorale, cu respectarea Constituției, a legii și a standardelor internaționale și europene în domeniu. Derularea procesului electoral este gestionată prin intermediul unui sistem informatic. Conform declarațiilor prim-ministrului României, în cazul alegerilor europarlamentare, sistemul va fi același ca și în cazul scrutinelor din anul 2016.

Sistemele informatice implicate în procesul electoral sunt dezvoltate de AEP, Serviciul de Telecomunicații Speciale (STS), precum și de companii din sectorul IT&C.

Pe baza cazuisticii și a datelor de cunoaștere disponibile, putem preconiza 5 scenarii cu privire la interferențe ale unor actori cibernetici în alegeri.

1 INFECTAREA SISTEMELOR IT&C UTILIZATE ÎN CADRUL PROCESULUI ELECTORAL

A) **Derularea unui atac cibernetic asupra Registrului Electoral Central**
B) **Derularea unui atac cibernetic asupra sistemelor informatice utilizate în cadrul proceselor de centralizare și numărare a voturilor**

EFECTE

- **afectarea disponibilității sau integrității datelor necesare pentru realizarea listelor de alegători;**
- alterarea **rezultatelor parțiale ale votului,** situație în care, prin distribuirea unor date false, s-ar putea **influența opinia publică în vederea obținerii unui rezultat favorabil unei anumite părți;**
- **perturbarea procesului electoral din punct de vedere organizatoric, prin întârzierea realizării anumitor activități;**
- **aducerea unui prejudiciu de imagine (decredibilizare), pe plan intern și extern, la adresa instituțiilor naționale implicate în procesul electoral;**
- **scăderea nivelului de încredere al populației în procesul electoral.**

RECOMANDĂRI

- **utilizarea de resursă umană suficient pregătită/specializată în administrarea sistemelor informatice utilizate în cadrul procesului electoral;**
- **testarea riguroasă a sistemelor informatice utilizate în cadrul procesului electoral, în vederea reducerii posibilității ca acestea să fie compromise/deja infectate, fapt care ar facilita accesul actorilor cibernetici și ulterior preluarea sub control;**

- utilizarea unor soluții de back-up (la intervale cât mai scurte de timp) pentru datele vehiculate;
- realizarea unui proces continuu de auditare/inspecție/control asupra sistemelor informatice utilizate în cadrul procesului electoral, chiar și în perioadele dintre scrutinele electorale;
- existența unor proceduri de verificare, auditare și păstrare a log-urilor înregistrate în perioada alegerilor.

2 INTERCEPTAREA COMUNICAȚIILOR EXISTENTE ÎNTRE MISIUNILE DIPLOMATICE ALE ROMÂNIEI ȘI AEP PRIN ATACURI CIBERNETICE

EFECTE

- afectarea integrității datelor (modificarea numărului participanților/voturilor) transmise de misiunile diplomatice către AEP;
- indisponibilizarea canalului de comunicații utilizat de misiunile diplomatice, fapt ce poate conduce la întârzierea transmiterii voturilor;
- aducerea unui prejudiciu de imagine (decredibilizare), pe plan intern și extern, la adresa instituțiilor naționale implicate în procesul electoral.

RECOMANDĂRI

- testarea riguroasă a sistemelor informatice existente la nivelul misiunilor diplomatice, în vederea reducerii posibilității ca acestea să fie compromise/deja infectate;

- utilizarea unor soluții de back-up (la intervale cât mai scurte de timp) pentru datele vehiculate;
- realizarea unui proces continuu de auditare/inspecție/control asupra sistemelor informatice chiar și în perioadele dintre scrutinele electorale;
- existența unor proceduri de verificare, auditare și păstrare a log-urilor înregistrate în perioada alegerilor.

3 REALIZAREA UNOR OPERAȚIUNI INFORMAȚIONALE DE PROPAGANDĂ ȘI DEZINFORMARE

EFECTE

- denaturarea / alterarea și transmiterea de informații de interes public către un număr cât mai mare de persoane, prin crearea de conturi false pe platformele de socializare și lansarea de afirmații false („*troli*”);
- influențarea opiniei publice sau a unui public-țintă (pentru cultivarea unei imagini favorabile unor entități, polarizarea climatului social etc.) și scăderea încrederii în structurile naționale („*fake news*”);
- asocierea unor persoane publice cu imagini sau evenimente cu caracter negativ și distribuirea acestora către anumite segmente sociale („*hate-language*”).

RECOMANDĂRI

- derularea unor campanii de conștientizare la nivelul societății civile cu privire la riscurile asociate campaniilor de propagandă și dezinformare.

4 DISTRIBUIREA DE DOCUMENTE CU CARACTER CONFIDENȚIAL/PERSONAL (LEAKS) OBȚINUTE CA REZULTAT AL UNOR ATACURI CIBERNETICE

EFECTE

- influențarea opiniei publice prin utilizarea datelor exfiltrate din cadrul unor instituții publice (ministere, Administrația Prezidențială, etc.) dar și entități private implicate în alegeri (partide politice / candidați, persoane publice, consultanți ai unor partide / candidați, companii de PR, lideri de opinie care susțin un anumit candidat etc.)
- afectarea imaginii României la nivel internațional, fapt ce ar putea aduce prejudicii la adresa intereselor naționale într-un orizont de timp ce nu poate fi estimat.

RECOMANDĂRI

- respectarea un set minim de reguli cu privire la: utilizarea și actualizarea regulată a soluțiilor de securitate cibernetică, stocarea și diseminarea datelor personale în mediul online, securitatea comunicațiilor electronice (ex. e-mail, aplicații de mesagerie), alegerea și utilizarea parolelor, actualizarea software, gestionarea permisiunilor acordate aplicațiilor.


Up
Screen
Back
Forward
Repeat
Tempo

5 ATACURI CIBERNETICE ASUPRA INFRASTRUCTURILOR IT&C ALE UNOR TRUSTURI MEDIA ROMÂNEȘTI

EFECTE

- compromiterea infrastructurilor IT&C ale trusturilor media românești;
- obținerea unor elemente de cunoaștere necesare pentru impersonarea ulterioară a platformelor web folosite de acestea (website-uri, pagini de social media, etc);
- lansarea în spațiul public a unor informații care să influențeze / altereze opinia publică;
- exfiltrarea de date confidențiale aparținând trusturilor media / persoanelor care lucrează în cadrul trusturilor, care pot fi utilizate pentru decredibilizarea acestora;
- influențarea prezenței la vot și a rezultatului alegerilor prin distribuirea de fake-news.

RECOMANDĂRI

- respectarea un set minim de reguli cu privire la: utilizarea și actualizarea regulată a soluțiilor de securitate cibernetică, stocarea și diseminarea datelor personale în mediul online, securitateacomunicațiilor electronice (ex. e-mail, aplicații de mesagerie), alegerea și utilizarea parolelor, actualizarea software, administrarea și utilizarea platformelor web, gestionarea permisiunilor acordate aplicațiilor;
- monitorizarea permanentă a mediului online în vederea identificării platformelor web care impersonează și raportarea acestora către organismele și autoritățile cu competențe.

romania2019.eu

www.sri.ro