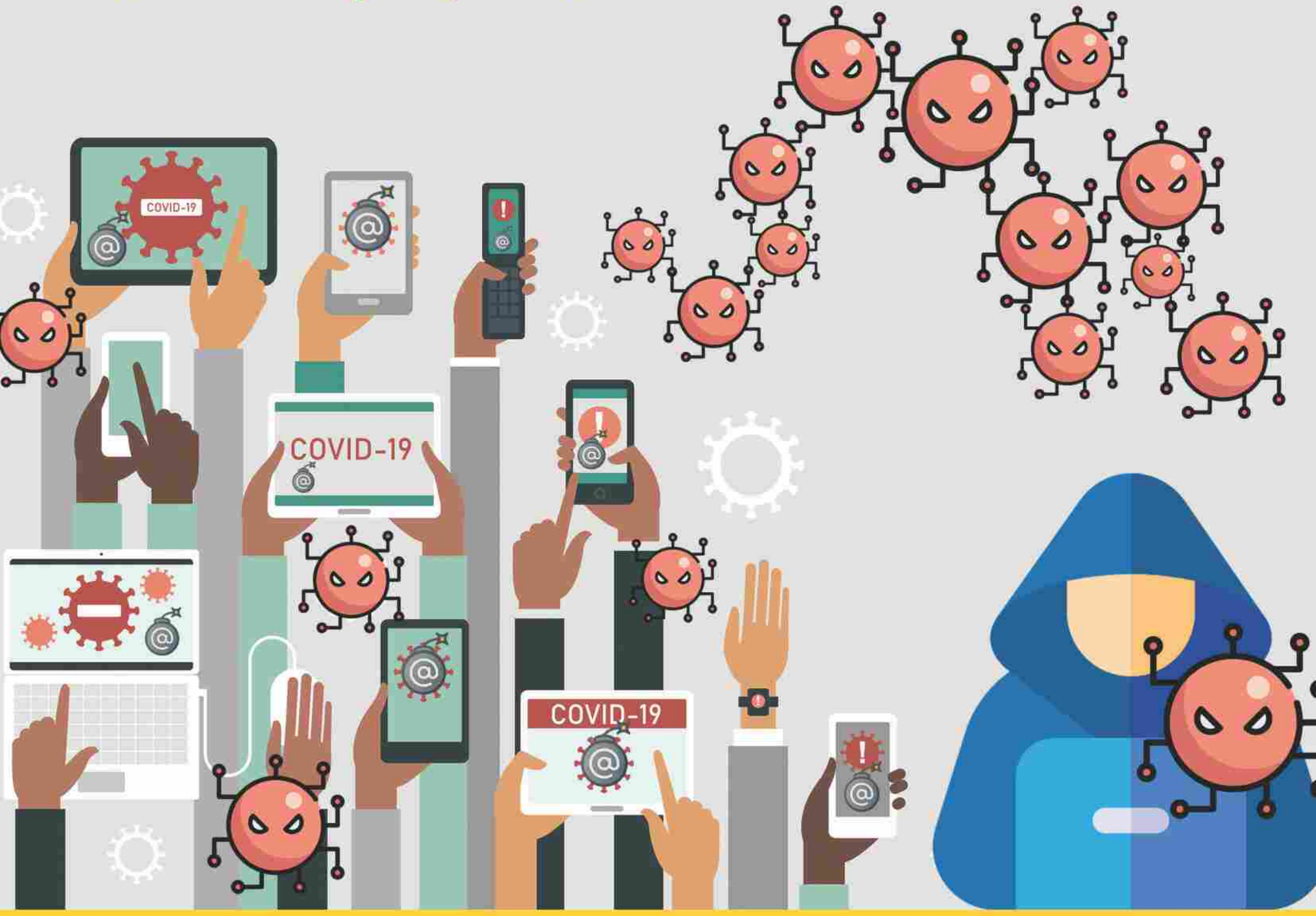
Cybersecurity Trends

Ediție Specială, Aprilie 2020

Ce volume vous est offert par :

MIRAT DI NERIDE
Cyber Sécurité

- **Context și impact**
- **Ghid de apărare cibernetică pentru cetățeni și companii**



«Ciber-COVID#19», cel mai mare val de atacuri cibernetice din istorie. PROTEJAȚI-VĂ!

O publicație binevenită, în contextul unui val de atacuri fără precedent

Autor: **Patrick Ghion**

Ca întreaga Europă, țara noastră este ținta unui val de atacuri cibernetice fără precedent în ceea ce privește numărul, amploarea, varietatea și, mai ales, calitatea celor mai periculoase dintre ele.

În afară de phishing și de formele cunoscute de escrocherii digitale, regăsim ransomware de generație nouă, atacuri împotriva sistemelor și software-urilor folosite cel mai des, precum și un număr impresionant de *zero-days** și de mutații accelerate de *Advanced Persistant Threats***.

Mai rău, aceste atacuri afectează nu doar cetățeni din toate categoriile sociale și de vârstă, ci și toate companiile, de la cele mai mici la cele mai mari. Toate instrumentele digitale folosite în viața de zi cu zi, de la smartphone-uri la tablete și calculatoare și până la servere și cloud, toate sunt sub asediu.

De exemplu, e de ajuns să ne raportăm la statisticile oficiale ale Confederației pentru a înțelege proporția prejudiciilor: de la 14 denunțuri referitoare la incidente/atacuri grave în prima săptămână a lunii ianuarie 2020, *Centrul Național pentru Securitate Cibernetică* a înregistrat, în prima săptămână din aprilie, aproape 240 de anunțuri (1), adică un salt de mai mult de 1700%.

Operațional încă de anul trecut, Centrul de Competență Regional de Luptă împotriva Criminalității Cibernetice pentru Elveția de vest activează în cadrul Poliției Cantonului Geneva. Principiul generat de noua strategie de protecție a Elveției în materie digitală are ca obiectiv punerea la comun a competențelor avansate la nivelul întregului canton. Prin această schimbare de paradigmă, se prefigurează o eră colaborativă fără precedent în istoria Elveției, unde fiecare canton constitutiv al Confederației are propria poliție și propriul organ de poliție judiciară, cu câte un compartiment specializat, competent în materie de spațiu digital.

În acest context, odată cu noile responsabilități extra-cantonale care revin de acum Poliției Cantonului Geneva, este acordată o atenție specială importanței fundamentale a parteneriatelor public-private, pe care această poliție le-a cultivat de-a lungul anilor, cu rezultate extraordinare.

Cu aceeași situație se confruntă toate statele din Europa: tot personalul specializat este deja angrenat, astfel încât suntem în imposibilitatea de a mobiliza forțe suplimentare pentru a aduna, regrupa și sintetiza toate alarmele împrăștiate în rândul populației și al companiilor.

Din punctul nostru de vedere, această broșură adresată tuturor, veritabil ghid de prevenție și de apărare digitală cu o structură clară, organizată pe categorii de atacuri și de ținte, redată într-un stil limpede și sintetic și însoțită de nenumărate referințe online, apare exact la momentul potrivit.

Pentru noi este o îndatorire și o onoare să figurăm printre partenerii internaționali principali ai acestei publicații, care va apărea în trei limbi.

Pentru inițiativă și asumarea voluntară a muncii pe care o presupune aceasta, îi mulțumim călduros partenerului nostru de tradiție, Swiss Webacademy, organizatoare a triadei de congrese internaționale Cybersecurity-Dialoguri, materializate în revista Cybersecurity Trends, precum și tuturor celor care au contribuit la această ediție specială, în primul rând fondatorului și redactorului-șef, Laurent Chrzanovski, dar și întregii sale echipe. ■

BIO

Căpitanul Patrick Ghion lucrează pentru Poliția Cantonului Geneva de 20 de ani. Fost responsabil al brigăzii de luptă împotriva criminalității informatice, Patrick Ghion este astăzi șef al Secției de criminalistică al Poliției judiciare de stat din Geneva, alcătuită din 4 unități de brigadă, printre care și cea de luptă împotriva criminalității informatice. Înainte de a se alătura forțelor de ordine, a lucrat în cadrul mai multor bănci elvețiene și, o vreme, a fost și instructor de scufundări în Asia. Tatăl a doi copii, principalele sale hobby-uri sunt scufundările subacvatice și pilotarea avioanelor.

(1) www.melani.admin.ch/melani/fr/home/ueber_ncsc/meldeeingang.html
*zero-days = formă inedită de atac ce vizează o vulnerabilitate informatică și care nu a fost dezvăluită sau pentru care nu există niciun patch
**Advanced Persistant Threats = tipuri de piratare informatică ce sustrage informații constant și vizează adesea o entitate sau un sector specific.

O vom scoate la capăt?

Autor: **Nicola Sotira**

GLOBAL CYBER SECURITY CENTER

În acest moment, pare aproape „normal" să vorbim de măsuri de urgență, de pandemii, de COVID-19. O situație de urgență care a început să se manifeste public în Italia în 30 ianuarie, când doi turiști chinezi au fost testați pozitiv.

Începând cu acel moment, cifrele au început să crească, iar noi trebuie să regândim totul într-o nouă lumină. Așa cum indică foarte clar și raportul MIT din 17 martie, pentru a pune capăt acestei pandemii, trebuie să ne schimbăm obiceiurile, modul de lucru, felul în care facem mișcare, cumpărături, felul în care învățăm, socializăm și mai ales modul în care călătorim.

S-ar putea ca unele din aceste transformări să devină permanente?

Până de curând, *smart working* nu părea să vizeze decât anumite nișe în piața muncii. Acum, este adoptat la scară largă, spre marea satisfacție a companiilor, mai ales a celor care operează în sectorul serviciilor.

Am descoperit că acest lucru e posibil, că ziua noastră de lucru poate fi punctată de întâlniri pe platforme de colaborare digitale, fără însă a afecta calitatea muncii.

Însă ce se va alege de școli, de universități? Să ne amintim de imaginile văzute la știri, cu săli de clasă pline și amfiteatre insuficiente.

Acest subiect a devenit anacronic azi și nu vreau să amintesc nici măcar de aspectul întreținerii costisitoare a unităților școlare, care trebuie în continuare efectuată, sau chiar de construirea de spații noi. În această situație, școlile au lansat sesiuni online, iar tema studiului online a fost integrată complet. S-a zis cu sălile de clasă arhipline: fiecare poate urmări lecțiile de acasă și poate interacționa cu profesorul prin intermediul chat-ului sau al formularelor online.

Centrele de analiză a calității aerului și imaginile din satelit indică o diminuare a poluării, alt element care ne face să reflectăm la modul în care un model de creștere diferit poate combina dezvoltarea și durabilitatea de mediu.

Sectorul digital se dovedește tot mai util și permite schimbarea regulilor jocului, în producție, în ciclul de viață al companiilor, dar și în gestionarea timpului liber în vremuri în care socializarea fizică este redusă din rațiuni precum cea din aceste momente.

În plus, în cadrul acestei urgențe, multe state au reglementat eliberarea de prescripții medicale digitale, iar medicamentele pot fi solicitate prin e-mail și chiar prin WhatsApp.

Folosim Big Data și tehnici de predicție în domeniul sănătății, se vorbește și despre utilizarea aplicațiilor pentru urmărirea împrăștierii pandemiei, luăm în calcul implementarea sistemelor de telemedicină, avem deci dovada că tot ceea ce făcea subiectul unor discuții fără sfârșit înainte de tragedie poate în mod real și concret să se fie implementat!

Lumea s-a schimbat în mai multe rânduri, iar această pandemie va continua să ne schimbe viețile. Va trebui să ne adaptăm cu toții la un nou mod de a trăi după această experiență.

Însă la fel ca în cazul oricărei schimbări, trebuie să învățăm să apreciem aspectele pozitive pentru a construi o legătură și pentru a accelera o veritabilă metamorfoză digitală, care va fi în mod obligatoriu însoțită de o protecție a tuturor aspectelor legate de securitate și de viață privată, singura modalitate în care poate fi garantată o îmbunătățire autentică a calității vieților noastre.

Tot ce putem spera este ca gravitatea acestei tragedii să forțeze toate statele nu doar să-și regândească aspectele sociale care au generat inegalități, dar și să le determine să implementeze schimbări pozitive a căror continuare să merite și după traversarea acestei perioade de urgență. ■

BIO

Nicola Sotira este Director de Securitate a Informației a Grupului Poste Italiane și Director General al Global Cyber Security Center (fundația Grupului). Are peste 25 de ani de experiență în domeniul securității cibernetice, dobândită în numeroase companii internaționale, în timpul mandatelor sale. Înainte de a se alătura Grupului Poste Italiane, Nicola Sotira a fost Sales Director UC & C & Security Practices la Westcon Group Italy și Vice-President Sales Italy pentru Clavister AB. Profesor la Universitatea La Sapienza din Roma din 2005, predă în cadrul programului de Master in Network Security și este membru al Association for Computing Machinery din 2004. Promotor al inovației tehnologice, a colaborat cu numeroase start-up-uri din Italia și din străinătate. Membru al Italia Startup din 2014, participă la dezvoltarea și conceperea de servicii mobile. În plus, este colaborator al Oracle Security Council.

Cum exploatează infractorii cibernetici situatia creată de COVID-19, munca la distanță și cum putem riposta

BLOCKAPT

Autor: Marco Essomba

BIO

Marco Essomba este fondatorul și directorul tehnic al BlockAPT. Această companie de top în materie de securitate cibernetică, cu sediul în Regatul Unit, furnizează organizațiilor o platformă de apărare cibernetică avansată și inteligentă. Platforma BlockAPT permite organizațiilor să supravegheze, gestioneze, să automatizeze și să reacționeze (MMAR) la amenințările cibernetice, 24 de ore din 24, 7 zile din 7. Pasiunea, expertiza și cunoștințele lui Marco acumulate în decursul a 15 ani în procesul de elaborare de soluții de securitate digitală au culminat cu dezvoltarea acestei platforme unice, BlockAPT. Concepută de-a lungul timpului ca o trusă de instrumente atât pentru companiile mici, cât și pentru cele mari, cu scopul de a le facilita rezolvarea problemelor de securitate, platforma BlockAPT conține informații asupra amenințărilor, gestionarea vulnerabilităților, a dispozitivelor și a atitudinii proactive în legătură cu răspunsurile la incidente, pentru a sprijini lupta împotriva atacurilor cibernetice.
LinkedIn: https://www.linkedin.com/in/marcoessomba/
Twitter: https://www.linkedin.com/in/marcoessomba/
Website-ul companiei: https://www.blockapt.com

Introducere

Infractorii cibernetici sunt întotdeauna pregătiți să exploateze evenimentele cele mai mediatizate, folosind ingineria socială. Epidemia de coronavirus (COVID-19) ilustrează perfect modul în care infractorii cibernetici creează sisteme de fraudă sofisticate, cu unicul scop de a-i face pe utilizatori să acceseze link-uri generate ad hoc și să descarce malware, folosind tehnici de phishing. Dintre numeroasele tipuri de atacuri, phishing-ul continuă să reprezinte o amenințare importantă pentru indivizi și organizații, de la cele mai mari la cele mici. Phishing-ul rămâne un instrument foarte eficient, pentru că permite relativ ușor vizarea a milioane de utilizatori prin intermediul căsuțelor de e-mail, mesajelor transmise pe smartphone-uri și pe paginile rețelelor sociale, folosindu-se de coronavirus pentru a disemina false apeluri la acțiune.

Coronavirusul a obligat milioane de utilizatori să lucreze de acasă. Numeroase organizații au fost prinse pe nepregătite și au trebuit să implementeze rapid soluții de acces la distanță, adesea inadecvate și cu un grad scăzut de siguranță. Acest fenomen generează probleme importante pentru organizații ai căror angajați sunt vizați în mod direct de tot felul de escrocherii „COVID-19" care au ca obiectiv utilizarea de software pentru accesul la distanță, vulnerabile, și transformarea lor în mijloace de obținere a accesului neautorizat la sisteme securizate și la date sensibile.

Mai mult, acum că tot mai multe organizații își pun infrastructurile critice la dispoziția tuturor angajaților, la distanță, infractorii cibernetici sunt în permanentă căutare de noi metode de a accesa aceste sisteme cu reavoință.

COVID-19 – un punct de atac ideal pentru a pirata calculatoarele indivizilor și ale IMM-urilor

Infractorii cibernetici caută să compromită dispozitive centrale și să sustragă informații sensibile, folosind tehnici de atac comune precum phishing-ul, exploatarea software-urilor care nu au instalate cele mai recente patch-uri și recurg chiar la atacuri bazate pe forță brută: toate mijloacele sunt bune dacă ajută la obținerea accesului neautorizat la sisteme. Dată fiind lipsa de expertiză și de competențe în materia securității cibernetice, ne așteptăm ca în special IMM-urile să fie nepregătite. Majoritatea dețin soluții inadecvate pentru a-și proteja angajații împotriva unor atacuri diverse cum ar fi phishing-ul. De aceea, riscul la care sunt expuse acest tip de organizații este mult mai ridicat ca de obicei, antrenând sustrageri importante de date care ar putea conduce la prejudicii mai mari decât furtul în sine, cum ar fi creșterea valorii poliței de asigurare împotriva atacurilor cibernetice.

Miza întăririi securității cibernetice devine și mai importantă, pentru a le permite angajaților să-și continue munca la domiciliu într-un mod productiv. Având în vedere natura foarte variată a amenințărilor cibernetice pe care persoanele răuvoitoare le pot exploata, ar trebui ca fiecare organizație să-și implementeze un sistem de apărare solid, care să îndeplinească funcțiile de supraveghere a dispozitivelor, gestionarea lor, automatizarea și reacționarea la atacuri *(MMAR framework: Monitoring, Management, Automation and Response)* pentru a garanta că amenințările sunt descoperite și neutralizate rapid.

Cum putem să ne apărăm și să rămânem protejați împotriva atacurilor cibernetice în contextul COVID-19

Ținând cont de creșterea numărului de atacuri cibernetice în contextul coronavirusului, angajații și organizațiile ar trebui să fie mai vigilenți și să dea dovadă de o capacitate de apărare mai bună. Desigur, nicio soluție nu poate să ne protejeze complet de una singură împotriva arsenalului de care dispun infractorii cibernetici. Cu toate acestea, aplicarea unei strategii de apărare pe mai multe niveluri este întotdeauna o metodă foarte eficientă, așadar efectuarea de controale de securitate atât la nivelul rețelei și al punctelor de acces, cât și la nivelul companiei și al angajaților *(endpoints)* este esențială.

La nivelul primei linii de apărare, sunt cruciale controalele constante de securitate a traficului de rețea *in* și *out*. La nivelul celei de-a doua linii de apărare, trebuie instituită o metodă de protecție împotriva malware-ului pentru dispozitivele de acces și de stocare, folosind analiza clasică a malware-urilor în combinație cu analiza comportamentală. Astfel, chiar dacă un sistem e compromis, atacul poate fi detectat și întrerupt înainte ca răul să se producă. În al treilea rând, formarea orientată spre creșterea gradului de conștientizare pe tema securității joacă un rol important în cadrul strategiei de securitate globală a unei organizații. Crescând gradul de conștientizare, organizațiile își pot reduce considerabil gradul de expunere la riscurile de atac prin metoda phishing. Compromisul între securitate și comoditate constă în faptul că angajații nu vor putea detecta și evita în mod sistematic toate atacurile particularizate și sofisticate (nici chiar cele de tip phishing). Și totuși, formarea combinată cu o soluție de securitate globală și solidă de apărare în profunzime, oferă protecția cea mai ridicată, iar atacurile de tip phishing nu îi vor mai avea pe angajați pe post de țintă facilă.

În plus, o soluție de protecție a terminalelor, atât a laptopului cât și a desktop-ului, este esențială pentru garantarea protecției aparatelor împotriva malware și ransomware. Utilizarea unei autentificări în mai mulți pași pentru accesarea tuturor sistemelor externe este indispensabilă. Aceasta permite nu doar asigurarea unei rezistențe semnificative împotriva atacurilor bazate pe parole, care sunt și cele mai frecvente, dar constituie și un mijloc util de disuasiune împotriva atacurilor de bază. Sfaturile practice de mai jos sunt obligatorii atunci când lucrați de acasă:

- Asigurați-vă că laptopul sau desktopul este echipat cu cele mai recente versiuni de antivirus sau de protecție a punctelor de acces.
- Fiți cu precădere vigilenți în ceea ce privește atacurile de tip phishing legate de coronavirus și software-urilor de acces la distanță.
- Asigurați-vă că nivelul de autentificare solicitat pentru conectarea la sistemele de acces la distanță și de videoconferințe este unul ridicat.
- Asigurați-vă că, în măsura în care este posibil, toate sistemele externe care necesită o parolă utilizează autentificarea în doi pași, suplimentar față de clasica parolă.
- Dacă vă conectați la Internet dintr-un loc străin, cum ar fi Internet-café-urile, folosiți un VPN pentru a vă asigura că traficul este criptat și protejat împotriva supravegherilor exterioare.

Concluzie

Coronavirusul a obligat milioane de utilizatori să lucreze de acasă. Infractorii cibernetici sunt în permanentă căutare de mijloace rapide și eficiente de compromitere cu reavoință a sistemelor. Indivizii și organizațiile trebuie să dea dovadă de o capacitate mai mare de a se apăra împotriva numeroaselor atacuri personalizate. Instalarea regulată a patch-urilor, utilizarea unei autentificări în doi pași, implementarea unei soluții actualizate de protecție a punctelor de acces și efectuarea permanentă de acțiuni de conștientizare a rolului securității sunt de departe măsurile cele mai eficiente pentru a fi cu câțiva pași înaintea infractorilor cibernetici. În fine, o apărare solidă trebuie să facă parte din arsenalul global de securitate a administratorilor de rețele și de securitate. Combinația dintre supravegherea dispozitivelor, gestionarea, automatizarea și reacționarea la atacuri *(MMAR framework: Monitoring, Management, Automation and Response)* este fără îndoială cea mai bună metodă de a garanta descoperirea și neutralizarea rapidă a amenințărilor. ■

Pentru o igienă tot atât de necesară în lumea digitală ca în lumea fizică

Autor: **Mohamed Saad, Președinte al Asociației Utilizatorilor de Sisteme de Informații din Maroc (AUSIM)**

Pentru prima noastră activitate în parteneriat cu revista Cybersecurity Trends, rezultat al congresului public-privat „Cybersecurity Dialogues", ne-ar fi făcut o deosebită plăcere să fi prezentat Asociația, realizările sale, bogăția schimburilor interumane care a culminat cu prezența noastră în acest număr, printre altele grație prietenului și partenerului nostru comun, Didier Spella.

Însă, ținând cont de circumstanțe, este de datoria noastră să abordăm subiectul de actualitate care este totodată probabil cel mai mediatizat subiect de după al Doilea Război Mondial, eveniment la care, desigur, niciunul dintre noi nu a fost martor.

„Dar chiar un război?" veți întreba unii. „Da", ar răspunde alții. Această criză sanitară fără precedent, care s-a răspândit cu viteza luminii, punând sub izolare populații întregi, este pe cale să câștige teren și să provoace pierderi de miliarde de dolari... însă este mai ales în curs de a distruge o mare parte din confortul și plăcerile vieții.

Trebuie să ne sprijinim instituțiile în demersul de protejare a oamenilor, prin punerea la dispoziția colegilor noștri a instrumentelor necesare pentru munca la distanță, pentru a încuraja statul acasă și pentru a ne proteja la maximum de contactul cu ceilalți. Apoi, trebuie să ne asigurăm că activitatea instituțiilor nu se oprește, cu ajutorul instrumentelor IT și al altor dispozitive digitale, pentru a permite mediului de business să supraviețuiască, întrucât acest lucru are un impact asupra întregii economii naționale.

Devotată acțiunilor sale și modelelor de bună practică pe care le promovează, AUSIM este în proces de lansare a unor webinare despre Planurile de Continuitate a Activității, inclusiv în contextul protejării sănătății umane, dar și al securității IT și criminalității cibernetice, un alt flagel care se extinde odată cu proliferarea fenomenului de muncă la distanță.

Și tema securității digitale va fi abordată, întrucât este o temă „relativ nouă" în modul nostru de lucru și în cultura noastră. Tema reprezintă o urgență, acum mai mult ca niciodată, fiindcă pandemia a lăsat cale liberă infractorilor cibernetici, cu o creștere lunară a ratei atacurilor cu peste 500% la nivel global începând cu luna februarie. Alt fenomen nemaiîntâlnit.

În acest context, pentru AUSIM este o plăcere de a se alătura efortului colectiv pe care-l reprezintă publicația de față, care apare în patru limbi și are ca obiectiv furnizarea către un număr cât mai mare de oameni a instrumentelor pentru înțelegerea lumii digitale, pentru ca, apoi, să fie capabili să folosească ghidul de amenințări cibernetice care ne pândesc încă de la începutul pandemiei.

Viața trebuie să meargă mai departe, în primul rând prin impunerea de măsuri sanitare necesare pentru salvarea omenirii și, apoi, prin crearea unui spirit de întrajutorare, între oameni dar mai ales între instituții.

AUSIM promovează izolarea ca fiind una dintre măsurile cele mai eficiente

BIO

Mohamed Saad este actor în lumea Tehnologiilor informației încă din 1991, Evanghelist Digital, Președinte al AUSIM și Director al Polului de Resurse al Bursei din Casablanca, membru fondator al Isaca-Casablanca, filiala marocană a ISACA, Vice-președinte al CCAM (Clubul Marocan pentru Continuitatea Activității), membru al PMI. A absolvit INSEA și deține un MBA, certificări CISA, PMP, CRISC, ISO 27001. Mohamed Saad este autorul mai multor articole despre guvernanța IT, riscurile în IT, managementul portofoliului aplicației, standarde și referințe IT și multe altele.

pentru oprirea răspândirii acestui flagel, iar acest lucru este confirmat de opinia majorității experților, cercetătorilor și virusologilor.

Slavă Domnului, țara noastră a luat măsurile necesare la timp pentru limitarea și reducerea impactului și răspândirii virusului, însă cu toții trebuie să dăm dovadă de civism, de responsabilitate și de respect față de recomandările autorităților și instituțiilor de control și supraveghere.

Încă de pe acum, e rândul fiecăruia dintre noi să luăm măsuri de igienă digitală și să profităm de acest moment unic pentru a ne crește doza de maturitate în securitate digitală, fie ea individuală sau la nivel de companie, din sfera vieții noastre private, ori a activităților noastre profesionale sau chiar din sectorul public.

Într-un moment în care mulțumirile și recunoștința noastră se îndreaptă în primul rând către personalul medical și paramedical și către agenții care veghează asupra siguranței cetățenilor, ținem să subliniem și rolul vital al celor care, precum inițiatorii acestei reviste, depun eforturi pentru ca ziua de mâine să fie mai bună. Și așa va fi, cu voia lui Dumnezeu. ■

* Puteți urmări primul webinar în întregime (Webinar AUSIM: PCA et télétravail pour gérer la crise) la adresa: http://www.ausimaroc.com/webinar-ausim-pca-et-teletravail-pour-gerer-la-crise/

O mobilizare fără precedent

Cybersecurity Trends

Autor: Laurent Chrzanovski, fondator și redactor-șef al Cybersecurity Trends

Pregătind, pe final de martie, volumul Cybersecurity Trends Italie, ne-a venit ideea să trimitem articolul pe care l-am scris, împreună cu un mic ghid pentru utilizatori ai spațiului digital, către mai mulți specialiști care lucrează în instituții de stat, dar și privați, specializați în apărare cibernetică, pentru a aduna păreri, sfaturi, date și, nu în ultimul rând, critici constructive.

Toți acești experți români, elvețieni, francezi, marocani, italieni și englezi, care luptă în prima linie împotriva pandemiei de atacuri cibernetice 24/7, în creștere exponențială în ultimele două luni, ne-au ajutat în permanență, sacrificându-și, într-un efort colectiv de divulgare pozitivă, puținele ore libere pe zi care le-au mai rămas.

Rezultatul a urmat în același spirit, însă ține și de micile minuni care se înfăptuiesc doar în vremurile cele mai grele. Remarcând lipsa de personal care să se ocupe de informarea publicului larg altfel decât prin brief-uri despre atacuri punctuale, mai multe instituții și asociații profesionale din țările menționate ne-au rugat să planificăm, să concepem și să editățm această ediție, în limbile acestor state: franceza, engleza și româna.

Astfel, în 6 aprilie, directorii tuturor acestor entități au primit pe e-mail cererea oficială necesară pentru obținerea aprobării cu privire la parteneriate și pentru a permite specialiștilor să conceapă prezentările și lucrările pe care le puteți consulta aici. În aceeași zi, Ambasada Elveției în România a acceptat ca publicarea acestor trei versiuni lingvistice să se facă sub egida sa, prin Înaltul Patronaj al Ambasadorului Arthur Mattli.

Suntem în 15 aprilie, toate textele au fost transmise, iar traducerea lor este pe final sau sunt chiar în curs de paginare. O viteză de reacție nemaiîntâlnită, la înălțimea mizei pe care o reprezintă, și anume salvarea prin prevenție a unui număr cât mai mare de locuri de muncă, prin protejarea companiilor, dar și a vieții noastre private.

Le mulțumim din inimă tuturor instituțiilor și organizațiilor partenere, tuturor autorilor textelor care alcătuiesc acest număr și zecilor de specialiști care ne-au sprijinit.

Lucrarea de față nu are pretenția de a fi exhaustivă. În schimb, își propune să genereze cât mai multe pretexte pentru reflecție, grație multitudinii de puncte de vedere pe care le-am identificat și numeroaselor trimiteri la resurse mai detaliate disponibile online.

Să profităm cu toții de acest moment dificil pentru a înțelege în sfârșit lumea digitală, contribuțiile sale indispensabile la viața de zi cu zi, dar și pericolele și numărul enorm de capcane care ne amenință. Reziliența va da roade în curând, în lupta cu coronavirusul. Însă o reziliență digitală matură a fiecăruia dintre noi va da roade pe termen scurt, mediu și lung.

Să contribuim, deci, împreună, pentru a opri atât boala cât și cohorta sa de viruși digitali! ■

*Toate numerele, inclusiv proaspătul număr 1/2020, sunt disponibile online pe site-ul ad hoc creat de Poșta Italiană și GSEC: www.cybertrends.it/rivista/

II. Cum am ajuns aici? Pe teren și în viețile noastre.

Vocabularul strategic uitat

Autor: **Olivier Kempf**

Articolul original, rezervat abonaților, a apărut de curând în publicația bilunară La Vigie (nr. 139 din 1 aprilie 2020, pp. 4-6).
Pentru mai multe informații: www.lettrevigie.com
Îi prezentăm mulțumirile noastre lui Olivier Kempf pentru amabilitatea sa și pentru acordul de reproducere, traducere și publicare în exclusivitate a textului său în diferitele versiuni lingvistice în care apare Cybersecurity Trends.

Toți cei care urmăresc subiectul susțin că pandemia actuală constituie un punct de cotitură și că vor mai fi unul înainte și unul după. Este prea devreme pentru a distinge cu precizie caracteristicile acestei „zile de după".

Cu toate acestea, încep să se prefigureze câteva indicii: să constatăm totuși cu precauție că afacerile geopolitice își reintră în cursul firesc, pe ici, pe colo, iar anumiți actori, profitând că atenția e îndreptată spre numărul victimelor, își relansează discret activitățile.

Vom reveni asupra acestui aspect. Pentru moment, haideți să analizăm o parte a vocabularului strategic care a fost uitat, cu bună știință sau nu, din neglijență sau din reconfigurarea priorităților.

Surpriza strategică

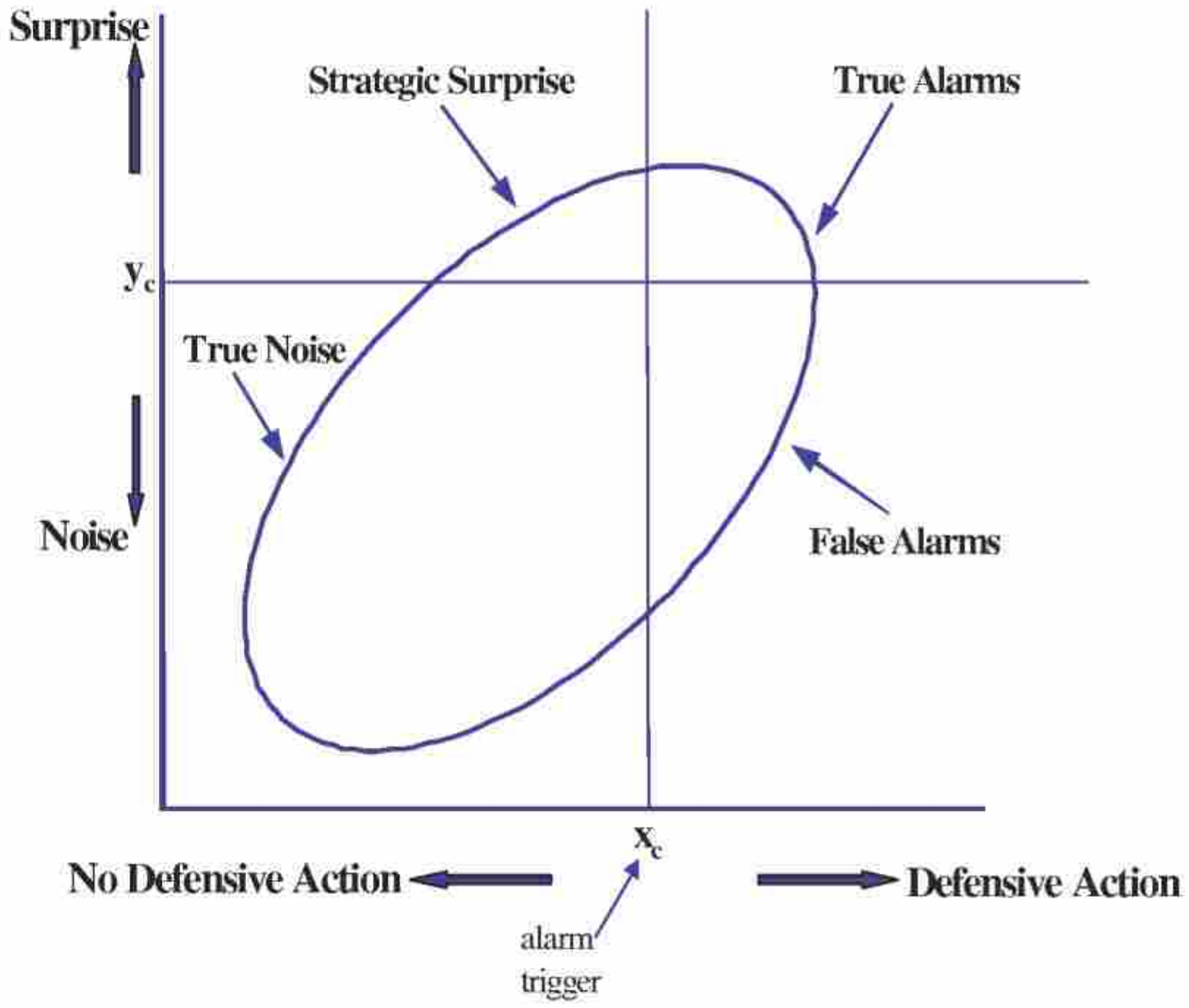
Amintiți-vă: termenul a fost foarte la modă după seria de atentate din 2001. Pe atunci, toți am lucrat pe această temă, am întocmit analize mai mult sau mai puțin inteligente, apoi am trecut la alte expresii, venite de peste ocean: GWOT, MENA, COIN sau A2AD, de pildă. Apoi ne-am luat angajamentul că am învățat lecția și nu vom mai fi surprinși.

De altfel, am anticipat următoarea surpriză strategică, prin faptul că am investit mult în apărare cibernetică. Bineînțeles, situația din Crimeea din 2013 ne-a alarmat puțin, însă din punct de vedere tactic am putea spune că am inventat cu acea ocazie conceptul (foarte puțin convingător) de hibriditate.

Însă am rămas într-un cadru convenit, iar strategi străluciți țineau discursuri despre chestiuni de operațiuni multi-domenii.

BIO

Biografie: după o carieră militară în care, în afara operațiunilor, a fost responsabil cu afacerile internaționale și de transformare, generalul (r) Olivier Kempf este consilier pentru companii și organizații în materie de strategie digitală și de securitate cibernetică (în cadrul Truchement consultants). Autor al „Introducerii în strategie cibernetică" (Economica, 2015), este directorul La Vigie, publicație de sinteză strategică pe care a fondat-o în 2014 și care apare bilunar, dar se ocupă și cu întocmirea de diverse studii pentru clienții săi.



Conceptul de surpriză strategică: imagine © Joseph Lampel, Zur Shapira, Judgmental Errors, Interactive Norms, and the Difficulty of Detecting Strategic Surprises, in Organization Science Vol. 12 No. 5 (2015), fig. 1

Desigur, aceste chestiuni sunt importante (introducerea domeniului spațial în strategie, evoluții tehnologice, luptă colaborativă) și nu se pune problema trecerii lor cu vederea. Însă ele aparțin teoriei strategice militare și nu marii strategii.

Or, un concept este pertinent dacă se adaptează atât strategiei militare (la nivelurile sale strategice, operative sau tactice) cât și marii strategii.

Conceptul de surpriză aparține fără îndoială acestei categorii. Ar trebui să fie așadar obsesia strategului. Este necesar să admitem că, în această privință, am eșuat.

Cu toate acestea, probabilitatea unei pandemii era bine cunoscută. Iată un nou caz, cel al surprizei care nu era chiar o surpriză, dar care totuși ne-a luat prin surprindere. În anii 2000 am avut câteva exemple: mai întâi SARS, dar și H5N1. Or, tocmai succesiunea acestor două crize a determinat lipsa de pregătire pe care o constatăm acum.

În 2003, SARS a fost o surpriză care a generat o mobilizare foarte amplă. În 2009, cu ocazia H1N1, reacția a fost una viguroasă, însă epidemia a fost mai puțin virulentă decât ne-am așteptat.

A urmat apoi o dezbatere cu privire la pagube și la reacția disproporționată: această dezbatere n-ar fi trebuit să existe, pentru că autoritățile au reacționat în context de incertitudine și nu cunoșteau virulența amenințării. Faptul că li s-a reproșat ulterior că au cheltuit prea mult nu a constituit deloc o reacție strategică, ci a reprezentat mai degrabă un comportament de comentator de fotbal, de după meci.

Apoi am lăsat lucrurile să curgă timp de zece ani, fapt care ne-a adus în situația actuală: deodată, această pandemie apare ca o surpriză strategică.

Are caracter strategic în privința consecințelor sale, fiindcă cealaltă caracteristică a surprizei strategice (în afară de caracterul surprinzător) este caracterul strategic în relație cu consecințele.

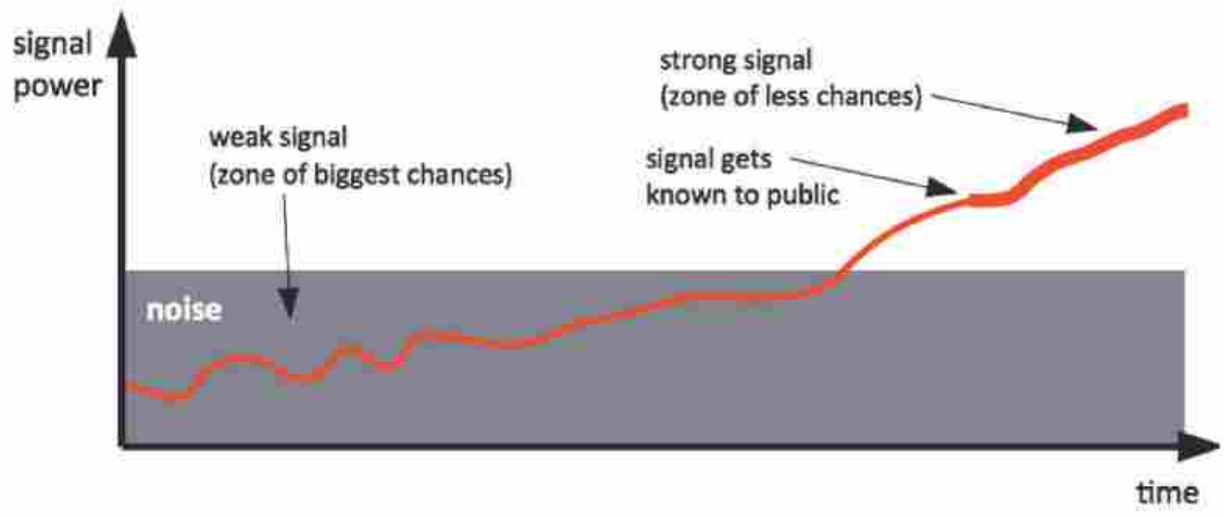
Semnale slabe

Altă expresie moștenită după 11 septembrie este noțiunea de semnale slabe. Nu este cazul acum să revenim asupra teoriilor lui Rumsfeld care, la vreme, vorbea despre „necunoscuții necunoscuți" (unknown unknowns), și nici asupra practicii de ascultare efectuate de serviciile de informații; o informație nu e valoroasă decât în corelare cu capacitatea de ascultare a decidentului.

Însă în acest caz, constatăm că semnalele nu au fost deloc slabe, ci puternice. Să ne amintim de criteriile evocate în planul de reacție la o pandemie de gripă, enunțate de către Secretariatul General al Apărării și Securității Naționale în 2009: *„Semnalele de alarmă care ar putea justifica folosirea acestei fișe sunt următoarele: semnale subite venite din surse concordante de undeva din lume, despre o extindere amplă a bolii, cu un mare număr de cazuri de sindrom gripal (mai mare de o sută), cu suspiciunea de extindere rapidă (grad ridicat de contagiune), cu o rată a mortalității anormal de ridicată și/sau de o gravitate clinică sau biologică ce necesită o spitalizare mult mai frecventă decât gripa sezonieră".*

Nu trebuia să fii mare profet: încă din 5 februarie, La Vigie semnala prezența virusului, deci aproape cu o lună înainte de măsurile luate de guvern.

Concluzia: dacă nu doar semnalele puternice rămân neauzite, oare câte din cele slabe sunt percepute? În fond, acestea din urmă nici nu există.



Utilitatea de a înțelege semnalele slabe înainte ca șansele de a combate fenomenul să se reducă © Robert Eckhoff, Mark Markus, Markus Lassnig, and Sandra Schön, No Outstanding Surprises when Using Social Media as Source for Weak Signals? First Attempt to Discuss the Impact of Social Media Sources to Detect Surprising Weak Signals. In: Proceedings of The Ninth International Conference on Digital Society (ICDS) in Lisbon, Portugal, 2015,Ifig 1

Strategia mijloacelor

Am evocat chestiunea alinierii mijloacelor cu scopurile și căile, trebuie astfel să evocăm și strategia mijloacelor pentru a desemna modul de mobilizare a aparatului industrial pentru obținerea resurselor de care au nevoie armatele.

Or, această criză ne învață că o strategie civilă are nevoie și de o strategie a mijloacelor.

Analogia este valabilă sub toate aspectele: este util să avem stocuri, de muniție și carburant, de măști medicinale, de ventilatoare și de teste, însă avem nevoie și de o strategie industrială pentru a permite o suveranitate a producției: industria apărării pe de o parte, industriile chimice și sanitare pe de altă parte.

Trebuie amintit, în acest context, gradul semnificativ de devalorizare în ultimele decenii a noțiunii de „politică industrială": politica economică de încredere în procesul de globalizare le-a transformat multora entuziasmul în tristețe.

Noțiunea de inteligență economică capătă puțină popularitate, după 2-3 ani, grație deciziilor radicale ale lui Donald Trump. Fără îndoială, în scurt timp, noțiunea de industrie strategică va fi la modă.

Defensivă și inovare

Bineînțeles, nu există un război împotriva virusului. Formula poate constitui eventual o metaforă, dar este greu de acceptat când ne vedem

în situația de a folosi vocabularul de război pentru a susține o mobilizare națională care nu a fost încurajată cu predilecțe înainte.

Complementar, apelurile la „armată", ivite pe ici-pe colo, ne demonstrează că în mentalul colectiv nu există nici cea mai vagă idee despre vulnerabilitatea reziduală a mijloacelor militare, efect al celor trei decenii de optimizări, cum li se spunea pe atunci. Regizarea unui apel la armate are rolul mai mult de a îngrijora decât de a liniști.

Cu toate acestea, există un front, iar nimeni nu poate tăgădui acest lucru: frontul spitalelor. Trebuie remarcată capacitatea de inovare, cu mijloacele care sunt la îndemână: amenajarea de urgență a sălilor de reanimare, fabricarea de măști sau de echipamente, de medicamente în regim de urgență. În această privință, am putea crede că asistăm la inventivitatea formidabilă a armatelor (și a serviciilor de sănătate ale acestora) din timpul Primului Război Mondial.

Măști de scufundări (snorkel) folosite în spitalele franceze, belgiene și canadiene © radiocanada

Apărarea (contra-atacuri menite să neutralizeze atacul, încetinire, control) necesită și adaptare în ceea ce privește durata.

Dreptul la libera circulație

Cine nu cunoaște cele trei principii ale strategiei, la care Foch ținea atât de mult? Unul dintre ele este dreptul la libera circulație.

Odată cu izolarea, populația e privată de acest drept, însă cu scopul împiedicării liberei circulații a virusului (se vorbește așadar de libertatea de contagiune).

Este foarte curios și paradoxal cum singura noastră strategie de apărare constă în imobilizare pentru oprirea extinderii. Însă logica este consecventă: această pandemie a căpătat o dimensiune globală din pricina exacerbării fluxurilor, cauzate de globalizare. În mod rațional, încetarea fluxurilor va permite încetinirea extinderii virusului.

Reziliență

Reziliența: alt cuvânt foarte la modă, împrumutat din psihologie de către cei care activează în sectorul strategic. Însă deși la origine termenul semnifică o capacitate individuală de a trece peste obstacole, acum este aplicat la ansambluri colective.

Trebuie remarcat că nu se vorbește despre națiuni, ci de „reziliența populațiilor", pentru a explica felul în care vor putea acestea să treacă peste atacurile teroriste, fiind de la sine înțeles că atacurile erau menite să declanșeze frică, să modifice opinii colective și să contribuie la apariția unor politici noi.

În mod ciudat, iată că virusul (pe care nu îl vom cataloga ca inamic) nu a stârnit frică, în primă fază. Din contră, l-am bagatelizat: „o banală gripă", care nu avea să ne împiedice să mai mergem la teatru, așa cum am fost sfătuiți de forurile de conducere.

Apoi, situația s-a agravat și am început să vorbim despre război și, imediat după, despre reziliență. Fiindcă, chiar dacă francezii par mai puțin tulburați decât cu ocazia atentatelor din 2015, suferă din plin de efectele pandemiei: în afară de izolare, bilanțul victimelor este deja (în Franța) de ordinul miilor de morți.

Sigur că o gripă sezonieră, sinuciderile sau alcoolul cauzează multe decese. O persoană cinică ar putea susține că, în final, această situație nu ar afecta echilibrul țării într-atât, iar reziliența ar fi asigurată, însă pagubele economice produse ar fi mai însemnate, iar, din acest punct de vedere, reziliența este mai puțin evidentă.

Convalescența va dura cu siguranță mult mai mult. Operațiunea Reziliența (mobilizarea mijloacelor militare împotriva Covid-19 în Franța) nu va fi suficientă. ■

Militari francezi angrenați în operațiunea reziliența © Europe1

Sub egida :

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

În parteneriat cu :

Cu sprijinul :

COVID-19 sau când guvernele ar avea multe de învățat de la securitatea cibernetică, în materie de gestionare a crizei

Autor: **Laurent Chrzanovski**

Situația actuală: politica haosului și ideologia „fiecare pentru sine”

Gestionarea europeană a COVID-19 (Coronavirus) este catastrofică. Planuri naționale de urgență cu măsuri tot mai restrictive care apar într-un ritm năvalnic, închiderea granițelor, izolarea indivizilor, populații sub stare de asediu și panicate, într-o oarecare măsură.

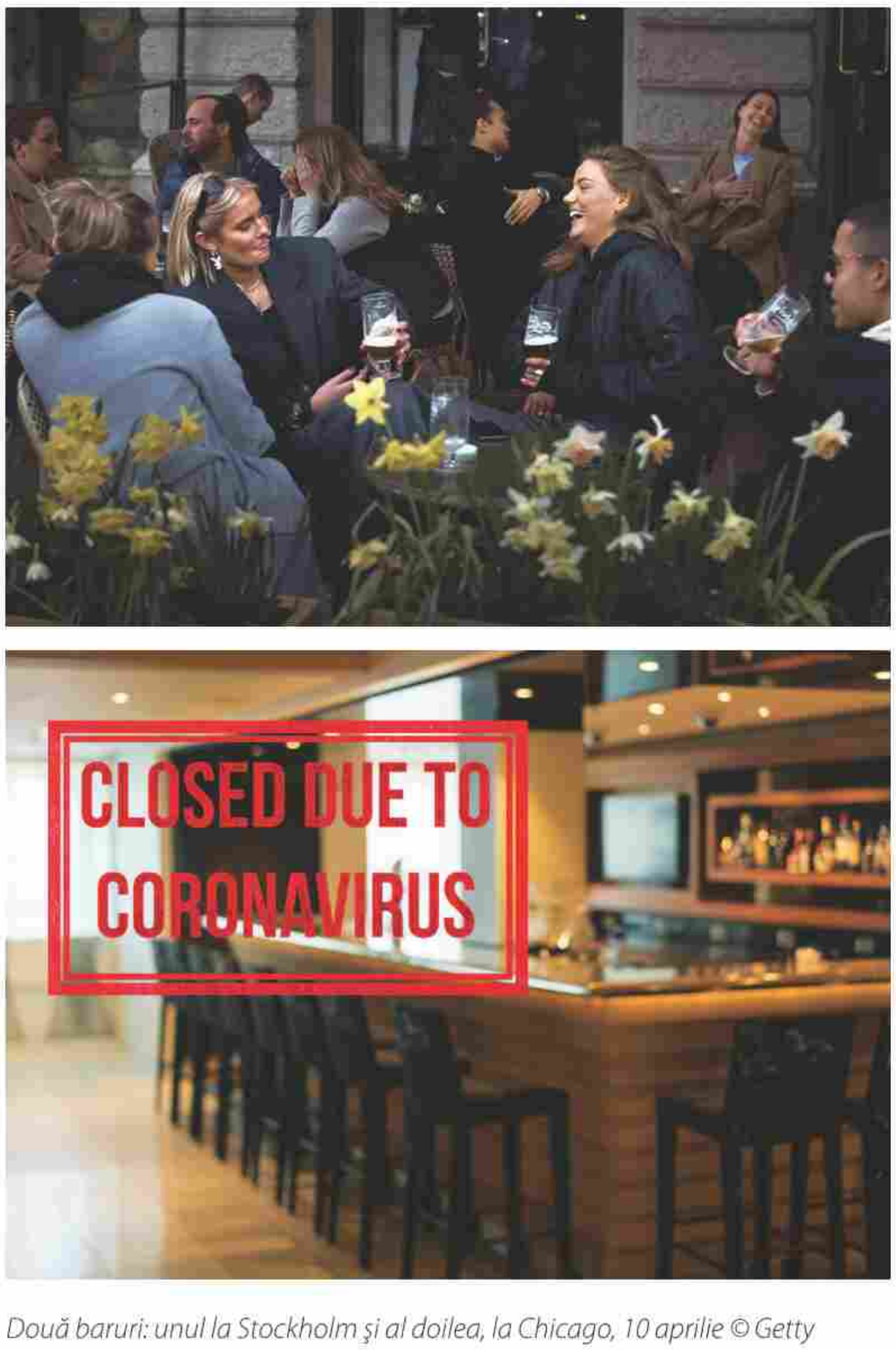
Toate acestea dublate de un cinism politic arareori întâlnit. Urgența este triplă în cazul guvernelor: de a lupta în mod eficient împotriva extinderii virusului, de a face ca economia să funcționeze cât mai bine și de a nu pierde popularitate electorală.

Politica haosului: Korczowa – Krakovets, punct de trecere a frontierei dintre Polonia și Ucraina, 28 martie 2020. În plină criză COVID-19, zeci de mii de cetățeni ucraineni au inundat acest punct pentru a se întoarce în țară înainte de închiderea granițelor. © Novynarnia

BIO

Cu un doctorat în Arheologie Romană obținut la Universitatea din Lausanne, o diplomă de cercetare postdoctorală în istorie și sociologie la Academia Română, Filiala Cluj-Napoca și o abilitare UE în a coordona doctorate în istorie și științe conexe, Laurent Chrzanovski este co-director de doctorate la școala doctorală la Universitatea Lyon II Lumière și susține regulat cursuri post-doctorale în cadrul mai multor universități importante din UE; fiind de asemenea, profesor invitat la Universitățile din Fribourg, Geneva și Sibiu.
Laurent Chrzanovski este autor/editor a 18 cărți și a peste o sută de articole științifice. În domeniul securității, este membru al „Roster of Experts” al ITU, membru al think-tank-ului „e-Health and Data Privacy” sub egida Senatului Italian, și manager al congresului anual „Cybersecurity in Romania. A macro-regional public-private dialogue platform”.

În *think-tank*-urile liderilor europeni, aceste trei fronturi, fiecare cu necesități clare și precise, sunt complet contradictorii. Rezultatul e vizibil, trăim într-un haos în care fiecare stat aplică legi de urgență, măsuri sanitare și aprobă folosirea de tratamente diferite, situație descrisă recent și de Giorgio Agamben: „Niciodată în istorie n-am mai asistat la acest spectacol, tipic religiilor în vremuri de criză, de opinii și de indicații diferite și contradictorii, variind de la poziția eretică minoritară (reprezentată de asemenea de oameni de știință prestigioși) a celor care neagă gravitatea fenomenului, la discursul ortodox dominant care confirmă această gravitate și care, cu toate acestea, diferă adesea radical în ceea ce privește metoda de abordare. Iar, ca întotdeauna în astfel de cazuri, anumiți experți sau așa-zișI experți reușesc să câștige considerația conducătorului, care, la fel ca în vremurile conflictelor religioase care dezbinau creștinismul, îmbrățișează în funcție de propriile interese o anumită teorie și impune măsurile aferente acesteia." (1)



Două baruri: unul la Stockholm și al doilea, la Chicago, 10 aprilie © Getty

Cetățenii sunt lăsați pradă unei explozii de informații alarmiste, dublate de fake news. Din ce în ce mai des, aceștia sunt abandonați în starea exprimată perfect de Noam Chomsky: „Oamenii de rând nu știu ce se întâmplă și nu sunt nici conștienți că nu știu ce se îmtâmplă".

Colaborarea europeană și internațională, singura metodă prin care s-ar putea înfrunta cu adevărat epidemia, este aproape inexistentă, așa cum a subliniat-o în mod magistral și Yuval Noah Harari: „Cred că cel mai rău lucru îl reprezintă dezbinarea pe care o vedem în lume, lipsa de cooperare, de coordonare între state. Și lipsa de încredere, atât interstatală cât și între cetățeni și guverne. (...) Lipsa de leadership și de cooperare mă sperie cu adevărat. Oamenii ar trebui să înțeleagă că răspândirea epidemiei în fiecare țară amenință întreaga lume, pentru că dacă nu este limitată la timp, virusul va evolua. O evoluție rapidă a virusului reprezintă probabil unul dintre cele mai rele scenarii legate de acest tip de epidemie". (2)

Mai rău, în țările care au închis granițele și în care, ca măsură de sănătate publică, a fost instituită carantinarea (izolarea) totală a cetățenilor, asistăm la o veritabilă lovitură de stat dictată de incapacitatea de a identifica și izola focarele de infecție în teren, din lipsă de teste. Această situație dă naștere unei psihopatologii în care părintele, vecinul, prietenul devin circumspecți și se creează o barieră în jurul fiecăruia, așa cum explică Michel Onfray: „Or, ce reprezintă izolarea dacă nu chiar îndemnul de a clădi frontiere pentru fiecare locuitor francez? Frontiera națională nu este adecvată, iar frontiera care ne desparte de cel de lângă noi e prezentată ca unică soluție. (...) Tratatul de la Maastricht tușește, scuipă și dă semne de embolie." (3)

Democrațiile confruntate cu tentația supravegherii în masă

Aceste măsuri nu sunt singurele care să ne determine să reflectăm asupra viitorului, cu precădere asupra celui digital, întrucât deja multe dintre guverne ne folosesc „smartphone-urile" pentru a ne controla localizarea, așa cum a prezis Slavoj Žižek: „Epidemia provocată de

coronavirus justifică și legitimează măsuri de control și de reglementare a populației de neconceput până acum într-o societate democratică occidentală; închiderea completă a Italiei nu este oare o fantasmă totalitară? Deloc surprinzător, China (care a utilizat deja masiv noile tehnologii în scopul instituirii controlului social) se dovedește țara cea mai bine pregătită pentru înfruntarea epidemiei catastrofice – cel puțin judecând după ceea ce pare a fi situația actuală. Oare asta înseamnă cumva că, cel puțin sub anumite aspecte, China înfățișează viitorul nostru?" (4)

Yuval Noah Harari, în ultimul său eseu, merge mai departe, susținând posibilitatea ca supravegherea legată de coronavirus instituită în multe state democratice să fie apoi folosită în mod obișnuit: „Pentru a pune capăt epidemiei, populații întregi vor trebui să respecte anumite linii directoare. Există două modalități principale prin care acest lucru se poate înfăptui. (...) Pentru prima dată în istoria umanității, tehnologia permite acum supravegherea în permanență a tuturor. Acum cincizeci de ani, KGB-ul nu putea urmări 240 de milioane de cetățeni sovietici 24 de ore din 24, nici nu putea analiza în mod eficient toate informațiile culese. KGB-ul se baza pe persoane agenți și analiști și pur și simplu nu putea pune câte un agent să urmărească fiecare cetățean. Însă de acum, guvernele se pot baza pe receptori omniprezenți și pe algoritmi puternici în loc să se bazeze pe apariții în carne și oase. (...)

Multe măsuri de urgență pe termen scurt vor deveni măsuri obișnuite. Este un lucru firesc în cazul situațiilor de urgență: ele fac ca procesele istorice să avanseze rapid. Decizii care, în vremuri normale, ar fi necesitat ani de deliberări sunt luate în câteva ore. Sunt implementate tehnologii premature și chiar periculoase, fiindcă riscurile de a nu face nimic sunt mai mari. Experimente sociale la scară largă le demonstrează utilitatea în multe state. Ce se întâmplă când toată lumea lucrează de acasă și comunică doar la distanță? Ce se întâmplă când școlile și universitățile funcționează online? În vremuri normale, guvernele, companiile și conducerea școlilor n-ar accepta niciodată asemenea experimente. Dar nu trăim vremuri normale. În vremuri de criză, avem două alegeri importante de făcut. Prima o constituie varianta supravegherii totalitare versus cea a responsabilizării cetățenilor. A doua o constituie tentația de izolare naționalistă versus solidaritatea mondială". (5)

Securitatea cibernetică: un domeniu global cu actori în dialog permanent

Atenția noastră începe să se orienteze acum spre securitatea cibernetică și spre o coordonare exemplară a acesteia, în comparație cu majoritatea alegerilor sanitare și de securitate guvernamentale.

Motivul e simplu: în plus față de daunele economice legate strict de consecințele virusului (pe care diverse surse le consideră simptome ale unei recesiuni mult mai grave decât criza din 2007), ar trebui adăugate daunele suplimentare produse de infracționalitatea cibernetică.

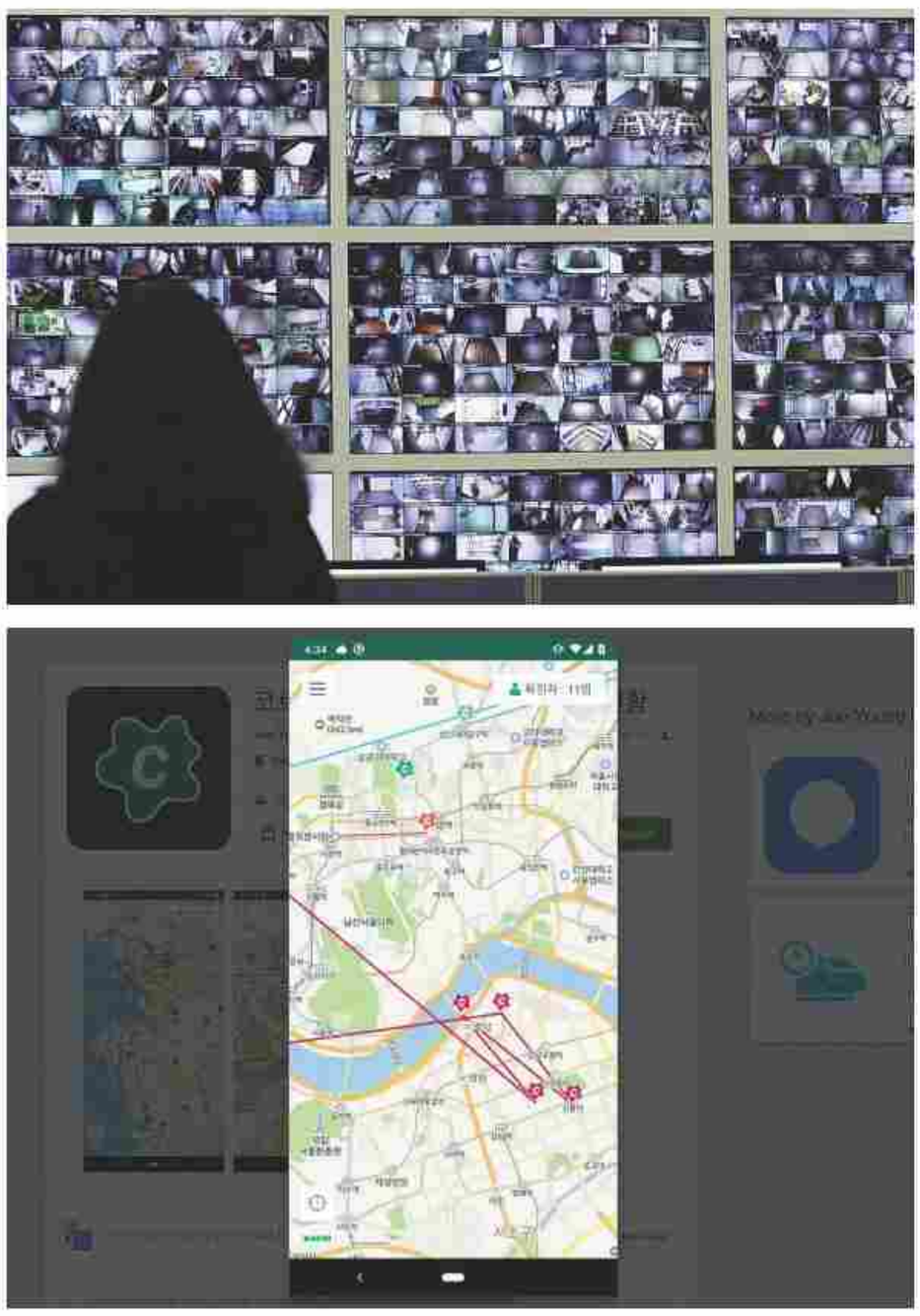
Pentru a oferi o dimensiune metaforică la ceea ce se întâmplă în lumea digitală, dacă în momentul redactării acestui text, COVID-19 ar fi fost un virus multimedia unic, numărul victimelor sale (asimptomatice, simptomatice, care se pot vindeca și care nu mai pot fi vindecați) ar fi avut cu cel puțin 4 zerouri mai mult decât persoanele care au contractat boala. Mai rău, acest virus nu ar ataca un singur sistem (precum sistemul respirator, în cazul virusului real), ci fiecare parte interioară și exterioară din corpul nostru ar fi în pericol.

Această mobilizare globală a tuturor sectoarelor, într-un veritabil parteneriat public-privat, care reprezenta obiectivul (foarte optimist) setat pentru 2020 de către Microsoft într-un raport din 2012, capătă formă sub ochii noștri.

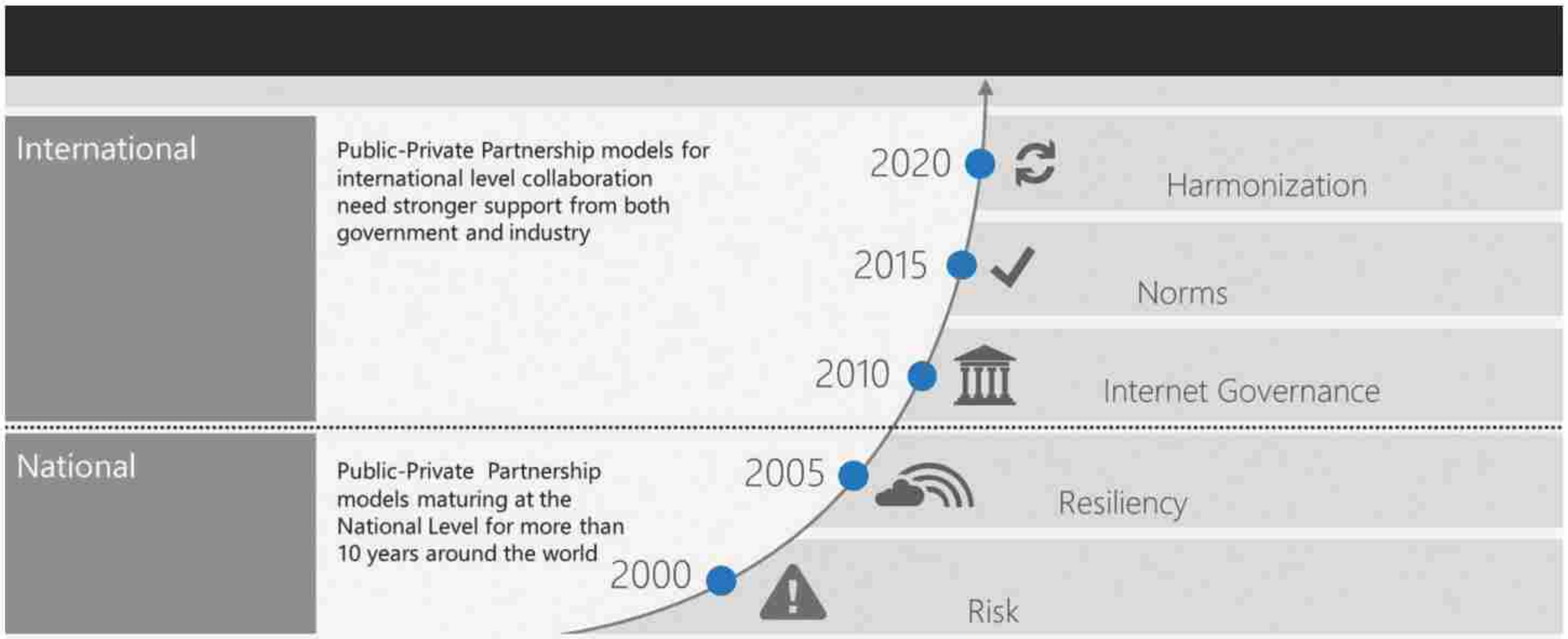
Apariția acestei mișcări este pur economică și, în același timp, legată de strategia statelor mai avansate și a companiilor de securitate. Orice eveniment problematic, chiar și unul „minor" (inundații la scară mică, greve în sectoare vitale), este imediat urmat de tentative multiple de atacuri cibernetice, iar acest lucru se întâmplă de cel puțin 10 ani.

Astfel, chiar dacă virusul ar fi fost limitat în Wuhan, ar fi fost succedat de un tsunami de atacuri. Într-adevăr, orice eveniment major care se produce în China sau în Statele-Unite are un impact economic, politic și... cibernetic global. Așa încât, încă de la primele cazuri comunicate la începutul lui februarie, experții în securitate digitală din toate țările s-au mobilizat.

Pe măsură ce pandemia se extinde, cel mai negru dintre scenarii se desfășoară – exploatarea de către grupări infracționale a mediatizării



Supraveghere în timp real, Coreea de Sud © The Conversation
Aplicații ale guvernului sud-corean care afișează itineriariile și locurile în care se află persoanele infectate © Businessinsider



Evoluția pe care o spera Matt Thomlinson în Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace
© Microsoft, 05.10.2012

pandemiei, urmărindu-i îndeaproape evoluția și adaptându-se rapid: atacuri la scară largă, strategii multiple, folosind toate mijloacele și toate limbile pentru a ajunge la toate tipurile de utilizatori și la toate instrumentele posibile (hard, soft, cloud) – pentru date tehnice, a se vedea raportul detaliat al grupului Insikt, *„Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide"* (6).

Aceste operațiuni fuseseră deja aplicate, dar cu mai puțin succes – tocmai pentru că n-au existat reacții guvernamentale atât de puternice și de incoerente la nivel mondial – în primul val al epidemiei de Ebola (2002-2003), așa cum explică foarte bine François Mouton și Arno de Coning în introducerea la studiul lor foarte recent legat de ce se petrece în lumea virtuală.

Diferența față de gestionarea epidemiilor: veritabile parteneriate public-private (PPP) internaționale și chiar mondiale

Pentru a face față unei game foarte largi de atacuri ce vizează minori și adulți deopotrivă și care încearcă să se insinueze în toate activitățile private și profesionale, marea diferență între gestionarea pandemiei virale *umane* și a *pandemiei cibernetice virale* constă în faptul că factorul politic este absent în cazul celei din urmă.

Entitățile însărcinate cu lupta împotriva atacurilor și cu limitarea pagubelor cauzate cetățenilor, companiilor și, nu în ultimul rând, instrumentelor digitale din instituțiile publice sunt agențiile specializate ale diferitelor state. Coerența, rigoarea, calificarea profesională excelentă și interacțiunea interdisciplinară constată a celor care se ocupă, în toată lumea, de urgența digitală actuală sunt, prin comparație, diametral opuse față de ce vedem pe frontul „fizic" și uman.

Ca întotdeauna, remarcăm proactivitatea unor țări care sunt în prima linie în ceea ce privește publicarea imediată nu doar a noilor vulnerabilități ale materialelor și ale aparaturilor (precum și a patch-urilor dezvoltate de producătorii respectivi), dar și a descrierii, mai întâi generaliste, apoi, cât mai repede posibil, tehnice, a diferitelor tipuri de ransomeware, viruși și „zero-days", cum ar fi **Singapore**, care deține, din punctul nostru de vedere, cel mai dinamic sistem CERT din lume în privința colectării, trierii și diseminării de informații, de o excelentă claritate și sinteză a elementelor-cheie. (8)

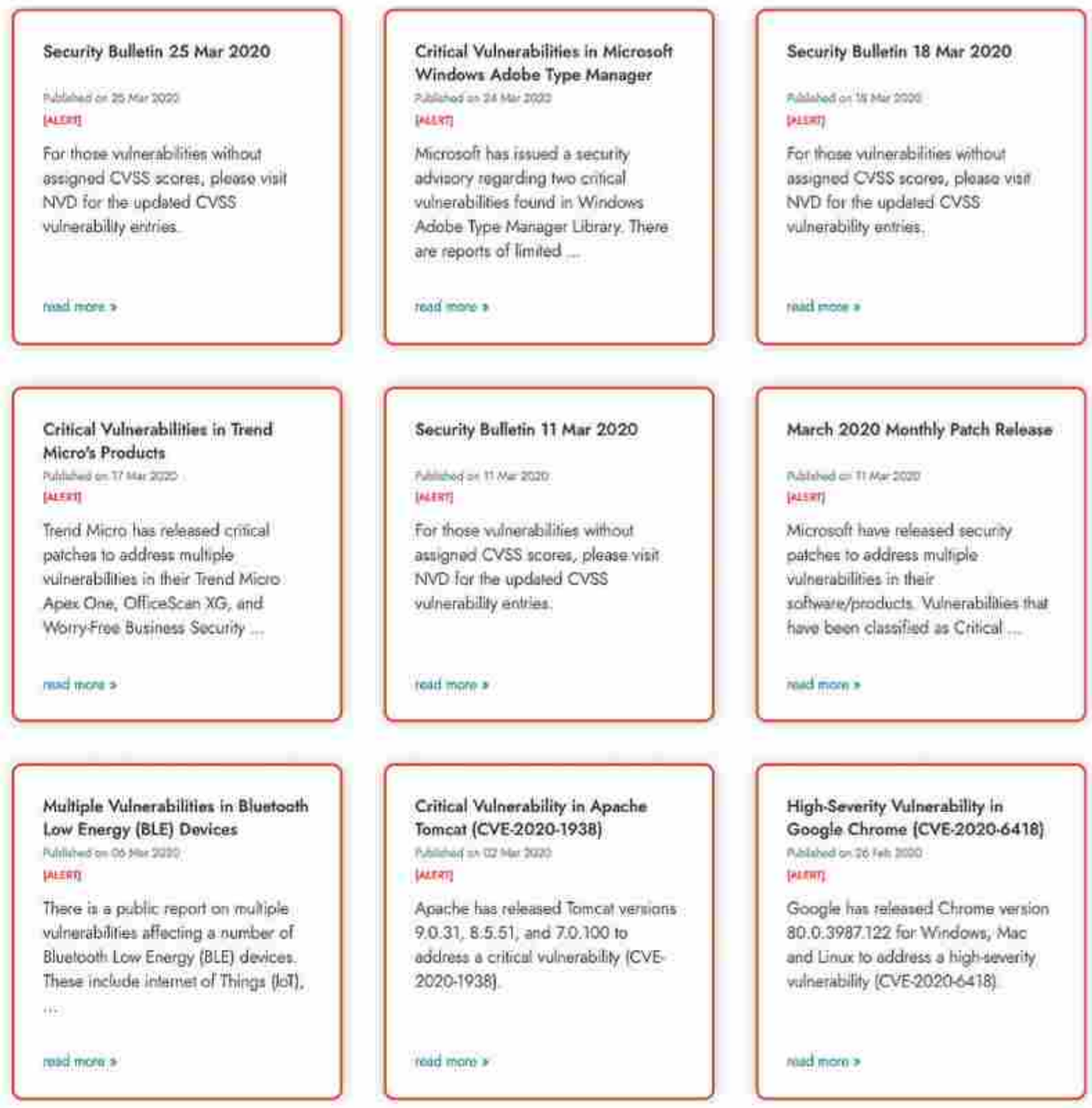
Este de menționat nu doar faptul că SingCert face parte integrantă din departamentul de securitate cibernetică al serviciilor de informații ale statului, dar și că încorporează un număr record de colaborări cu alte state sau cu companii private, mari și mijlocii. Un model de eficiență.

Situația - Cybersecurity Trends

În plus, eficiența acestei mici țări asiatice a uimit planeta și pe plan sanitar. Învățând din experiența gestionării virusului SARS, amintim că Singapore este, înaintea unor state precum Taiwan sau Hong Kong, țara care a gestionat cel mai bine criza și care a reușit să limiteze extinderea virusului uman, fără izolarea populației și fără închiderea creșelor, școlilor și firmelor.

La celălalt capăt al lumii, Statele Unite ale Americii și-au multiplicat eforturile și au reușit să facă un salt cuantic în materie de calitate pe care puține țări europene l-au atins: pentru a evita nenumărate căutări și consultări de site-uri web publice și private, ONG-ul **Staysafeonline** a pus la dispoziție de o lună o „Bibliotecă de resurse despre securitatea cibernetică în contextul COVID-19" (10), foarte utilă și actualizată constant. Extrem de clară, biblioteca cuprinde trei secțiuni: rapoartele de urgență și sfaturile emise de instituțiile de stat, rapoartele companiilor de securitate și articole specializate alese pe sprânceană și selectate din cele mai bune reviste din domeniul cibernetic. Comunicatele de presă succinte se găsesc în fluxul de informații speciale consacrat fiecăreia din cele patru ținte principale: copii, adulți, angajați, companii.

Explicația e simplă: platforma Staysafeonline este creată de **National Cybersecurity Alliance**, un grup de lucru foarte puternic care cuprinde Department of Homeland Security și aproape toate companiile specializate în securitate, companii mari și mijlocii, precum și asociații de white hats și universități. Această alianță este considerată în prezent ca ecosistemul PPP (de parteneriat public-privat) cel mai eficient din lume, cu excepția parteneriatelor cibernetice pe nișe dedicate



Pagina „news" a SignCert și o grădiniță din Singapore, 24 martie © Axios

Pagina bibliotecii de resurse de securitate în contextul COVID-19 © Staysafeonline

(infrastructuri critice, industrii sau sectoare private precum aviația, băncile, producătorii/furnizorii de electricitate etc.).

Un singur exemplu pentru ilustrarea frontului care se construiește în lupta împotriva atacurilor în masă

Pentru a face față asediului asupra tuturor obiectelor conectate și asupra utilizatorilor acestora din toată lumea, răspunsul cel mai impresionant a venit miercuri, 25 martie. Co-fondatorul celebrului congres DefCon, Marc Rogers, a creat **COVID-19 Cyber Threat Intelligence (CTI) League**, la care au aderat deja 400 de experți de nivel înalt din mai mult de 40 de state, aleși prin cooptare și pe bază de voluntariat.

Liga CTI a semnat deja protocoale de colaborare cu numeroase state, în principal cu Canada, sau direct cu agențiile de inteligență cibernetică din aceste state. Lăsând la o parte softurile de tip malware și „zero days" sofisticate, care sunt supravegheate și disecate de către membrii grupului în timp real, Rogers a justificat crearea acestui grup de elită plecând de la o remarcă: „n-am mai văzut niciodată un asemenea volum de phishing. Descopăr literalmente mesaje de phishing în toate limbile lumii." Grație ideii sale de a-i coopta pe cei mai buni, de la experți tip white hat la responsabili în securitate cibernetică ale marilor multinaționale și specialiști din societăți de securitate, după doar două zile, Rogers a declarat că n-a mai văzut niciodată o deschidere atât de mare din partea agențiilor de stat și a tras concluzia: „N-am mai văzut niciodată un asemenea nivel de cooperare, sper că se va menține și după, este un lucru foarte frumos." (11) Rezultatele Ligii (care nu-și dorește publicitate) vor avea fără îndoială efecte rapide și eficiente, fără ca utilizatorul de rând să-și dea măcar seama.

Sectorul privat, în lucru 24/24 și 7/7

În plus față de eforturile colective menționate, există și companii specializate, care propun zilnic rapoarte detaliate noi, întocmite de echipe active în toată lumea. Nu este necesară înșiruirea lor într-o listă, pentru că n-ar putea fi exhaustivă, iar cea mai bună modalitate de a afla și de a accesa ultimele informații disponibile pentru toți este de a citi articole oferite de reviste specializate online, ca de exemplu textele excelente de Montalbano, Pilkey, Lakshmanan (14) sau, în italiană, articolul remarcabil al lui Salvatore Lombardo (15) cu sfaturi și link-uri utile. ■

Note:

(1) Giorgio Agamben, Rifl$_{essioni}$ sulla peste, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste) (quote : author's translation)

(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

(3) Michel Onfray, Berezina, in Les Observateurs, 17.03.2020 (https://lesobservateurs.ch/2020/03/17/michel-onfray-berezina/) (quote : author's translation)

(4) Slavoj Žižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plaît ! in Le Nouvel Observateur, 18.03.2020 (quote : author's translation) (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)

(5) Yuval Noah Harari, Il mondo, dopo il Coronavirus, in Ottimisti e Razionali, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/) (quote : author's translation)

(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

(8) https://www.csa.gov.sg/singcert

(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html

(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/

(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049

(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

(14) Ravie Lakshmanan: Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

(15) Salvatore Lombardo: L'allarme: Coronavirus, in aumento attacchi cyber, phishing e malspam: consigli per difendersi, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

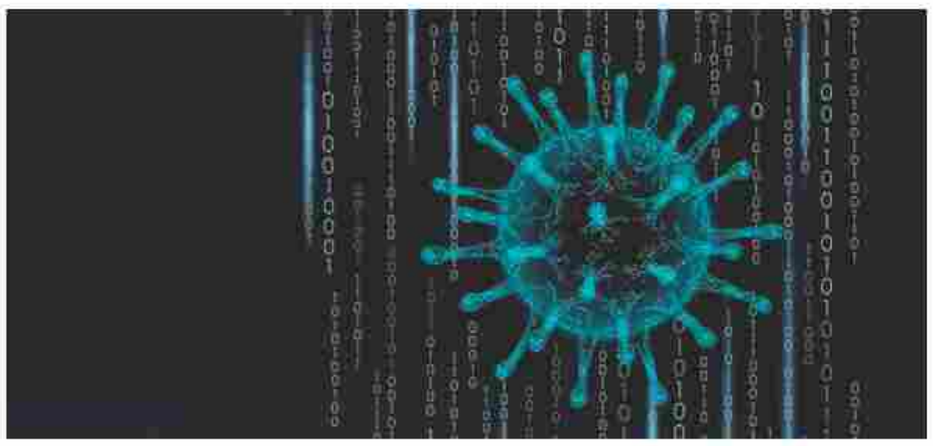
III. Impactul digital al COVID#19: un tsunami de atacuri. Explicații.

COVID-19 și securitatea cibernetică

Autor: Marc-André Ryter

Din situația generată de COVID-19 se vor putea desprinde lecții în multe domenii, de la primirea turistică la gestionarea crizelor, inclusiv în ceea ce privește capacitatea de producție autonomă minimală necesară fiecărei țări. Sperăm ca aceste lecții să fie transpuse în măsuri concrete.

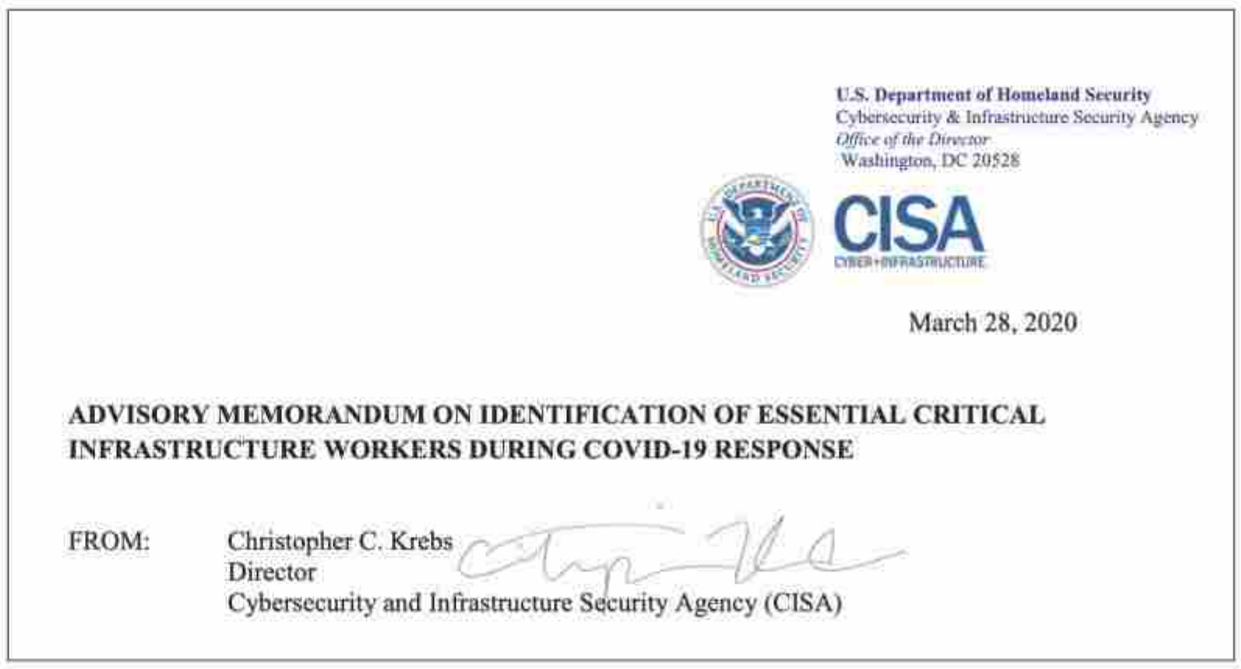
Este firesc să ne întrebăm cum a fost posibil ca guvernele să fie luate prin surprindere în asemenea măsură, din moment ce, de aproape două decenii, apar frecvent, cu un impact deloc neglijabil asupra populației. Ne referim aici în special la epidemia de SARS în 2002-2003, urmată de cea de gripă porcină H1N1, apoi de cea de Ebola în 2014. Și nu sunt singurele.



Ne interesează similitudinile și legăturile dintre această criză și securitatea cibernetică. În primul rând, trebuie menționat mediul instabil și generator de riscuri. Într-un asemenea mediu, complexitatea, nevoia crescută de securitate, controlul informației, controlul produselor și al comportamentelor și securitatea manipulării datelor sunt parametri care trebuie gestionați. Atât în spațiul virtual cât și în prezent, trebuie găsite soluții flexibile, rapide, coordonate și eficiente. Criza sanitară actuală determină aceleași provocări ca în cazul spațiului virtual: o competiție globală, necesitatea de a inova rapid și necesitatea de a integra sectorul public și cel privat.

Legătura dintre cele două domenii rezidă în riscurile care le amenință. Înainte de toate, fragilitatea rețelelor și fiabilitatea lor. Rețelele sunt puse la grea încercare în ceea ce privește dependența lor de numeroși parteneri externi. Riscul de perturbare a comportamentului din cauza unor sisteme disfuncționale este la fel de ridicat în sectorul sanitar ca în celelalte domenii ale vieții publice. Utilizatori răuvoitori din spațiul digital devin foarte repede capabili să profite de noile vulnerabilități temporare. Atacurile se dublează ca număr și sunt dezvoltate în mod specific în funcție de temerile populației. Manipulările și fake news se întețesc, la fel și fraudele de toate tipurile. Această dezinformare poate avea un impact important asupra societății și asupra comportamentului oamenilor, deci și asupra infrastructurilor critice.

Reacțiile încetinite nu fac decât să agraveze situația. Interpretarea semnalelor slabe și puternice este adesea lacunară, fapt ce încetinește



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

CISA
CYBER+INFRASTRUCTURE

March 28, 2020

ADVISORY MEMORANDUM ON IDENTIFICATION OF ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS DURING COVID-19 RESPONSE

FROM: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

Crește numărul paginilor care conțin sfaturi și metode de prevenție pe site-ul Department of Homeland Security dedicat infrastructurilor critice (CISA – www.cisa.gov). Mai sus, antetul ultimei adrese din 28 martie semnate de directorul Agenției.

BIO

Expert în politici de securitate, colonelul Marc-André Ryter lucrează pentru statul-major al armatei elvețiene. A urmat o formare de bază în științe politice înainte de a se specializa în studii de securitate. A absolvit Colegiul de Apărare NATO de la Roma. Urmărește și studiază evoluțiile tehnologice care se pot dovedi adecvate pentru forțele armate, cu scopul de a estima consecințele acestora asupra doctrinei militare.

procesul de trecere de la analiza informațiilor la acțiune. Această reacție este complicată și mai mult de managementul producției de tip *just in time* pe care se bazează economia. Companiile și instituțiile publice nu mai dispun decât de cele de imediată necesitate, atât din punct de vedere cantitativ cât și calitativ. Nu mai există nici stocuri, nici rezerve. Reziliența sistemelor economice și sanitare trebuie îmbunătățită. Situația actuală ne arată adevărata proporție a dependențelor noastre, în special în privința surselor de informații și a canalelor de schimb de date. Există un mare decalaj între realitate și percepția populației.

Munca la distanță reprezintă o măsură importantă adoptată de guverne pentru a face față răspândirii COVID-19 și ne demonstrează gradul mare de dependență de rețele, de capacitatea lor de transmitere a datelor și deci de buna lor funcționare. Din cauza muncii la distanță, volumul schimburilor de date a crescut exponențial, iar, împreună cu acesta, și vulnerabilitățile corelate.

Crizele precum cea pe care o trăim lasă cale liberă pentru breșe noi și numeroase, în favoarea infractorilor cibernetici. Aceștia profită de starea de slăbiciune și de temerile populației. Pe de o parte, își întețesc atacurile prin mijloace cunoscute, adesea sub forma unor e-mailuri aparent oficiale care adoptă un ton prin care fac apel la calm. Pe de altă parte, infractorii cibernetici organizează fraude masive de toate soiurile, dar în special legate de vânzarea unor bunuri foarte căutate.

Protecția datelor este esențială. În timpul crizelor, fenomenul colectării de date ia amploare și este practicat atât de privați, cât și de autorități. Controlul și protecția trebuie asigurate, la fel și utilizarea și în cele din urmă ștergerea datelor atunci când nu mai sunt utile. Amenințările deja existente, cum ar fi atacurile clasice, de tip ransomware, pot avea consecințe dramatice atunci când blochează de pildă funcționarea unui spital.

După modelul crizei COVID-19, înțelegerea necesității absolute a securității în spațiul digital este obligatorie.

Country or State	Traffic Change	DL Speed Change
France	↑ 38.4%	↓ 13.9%
Italy	↑ 109.3%	↓ 35.4%
Japan	↑ 31.5%	↑ 9.7%
Spain	↑ 39.4%	↓ 8%
United Kingdom	↑ 78.6%	↓ 30.3%
USA - California	↑ 46.5%	↑ 1.2%
USA - Michigan	↑ 37.9%	↓ 16.1%
USA - New York & New Jersey	↑ 44.6%	↓ 5.5%

Creșterea traficului în martie 2020 și reducerea vitezei © Fastly
https://www.fastly.com/blog/how-covid-19-is-affecting-internet-performance

Doar această securitate face posibilă protejarea împotriva acțiunilor infractorilor cibernetici și, mai ales, asigurarea unei funcționări corecte a rețelelor și garantarea disponibilității informațiilor indispensabile. Gestionarea și controlul crizelor trebuie să se bazeze pe un spațiu digital sigur. Trebuie evitate consecințele negative pe termen lung prin dezvoltarea cooperării între toți actorii, în vederea asigurării coerenței și similarității măsurilor luate.

Această necesitate de securitate, această cooperare între actori și îndatorirea de a împărtăși și de a promova un pachet de cunoștințe de bază legate de apărare către un număr cât mai mare de persoane, toate constituie pretexte pentru acest volum special, vital în aceste momente deosebite. Grație calității și diversității lucrărilor de față, avem certitudinea că acestea vor constitui un punct de plecare valoros pentru o examinare amănunțită a momentului ieșirii din criză care, mai devreme sau mai târziu, se va întrezări. ■

BLOCKAPT

An automated, intelligent cyber defence platform

- **Integrated web-based security** – reduce financial and reputational risks.
- **Active monitoring of web-based attacks** – monthly threat reports.
- **Automated security alerts** – preventative approach to threats.

FREE 60 DAY TRIAL WEBSITE SECURITY

www.blockapt.com

info@blockapt.com

BlockAPT Platform

- Deep integration
- Unified security ecosystem

Monitor – Deep integration with a single pane of glass view.

Manage – Automated threat intelligence, vulnerability management, device and incident response management on one platform.

Automate – Single command & control of your devices with automated playbooks to manage responses – 24/7.

Respond – Incident response management integrated into your change control processes to prevent future cyberattacks.

Cybersecurity Trends

Cuprins

Cuvânt înainte

3 **Răspândirea COVID-19 și atacurile cibernetice: o dublă amenințare pentru societate**
Autor: Arthur Mattli, Ambasador al Confederației Elveției în România

I. Cuvinte introductive ale partenerilor

Despre importanța de a repoziționa elementul uman ca actor al securității cibernetice
5 **și de a reda o semnificație pozitivă acestui comportament**
Autor: General Marc Watin-Augouard, Fondator al FIC; Director, Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

7 **Intensificarea atacurilor cibernetice în contextul pandemiei de COVID-19**
Autor: General Anton Rog, Director, Centrul Național Cyberint din cadrul Serviciului Român de Informații

8 **O publicație binevenită, în contextul unui val de atacuri fără precedent**
Autor: Patrick Ghion, șef al Secției de criminalistică al Poliției judiciare de Stat din Geneva

9 **O vom scoate la capăt?**
Autor: Nicola Sotira, Director de Securitate a Informației, Grupului Poste Italiane; Director General, Global Cyber Security Center

10 **Cum exploatează infractorii cibernetici situația creată de COVID-19, munca la distanță și cum putem riposta**
Autor: Marco Essomba, fondatorul și directorul tehnic, BlockAPT

12 **Pentru o igienă tot atât de necesară în lumea digitală ca în lumea fizică**
Autor: Mohamed Saad, Președinte, AUSIM; Director, Polului de Resurse al Bursei din Casablanca

13 **O mobilizare fără precedent**
Autor: Laurent Chrzanovski, fondator și redactor-șef al Cybersecurity Trends

II. Cum am ajuns aici? Pe teren și în viețile noastre.

15 **Vocabularul strategic uitat**
Autor: Olivier Kempf

18 **COVID-19 sau când guvernele ar avea multe de învățat de la securitatea cibernetică, în materie de gestionare a crizei**
Autor: Laurent Chrzanovski

III. Impactul digital al COVID#19: un tsunami de atacuri. Explicații.

25 **COVID-19 și securitatea cibernetică**
Autor: Marc-André Ryter

28 **Limitările planurilor actuale de apărare cibernetică și nevoia de a regândi lumea digitală**
Autor: Didier Spella

33 **Recursul la emoții în spațiul digital: între strategie discursivă și manipulare**
Autor: Laura Ascone

38 **Când izolarea asociată cu dezinformarea conduc la internări în spital**
Autor: Octavian Oancea

40 **Securitatea perimetrală, VPN și Zero Trust în pandemie de Coronavirus**
Autor: Cătălin Pătrașcu

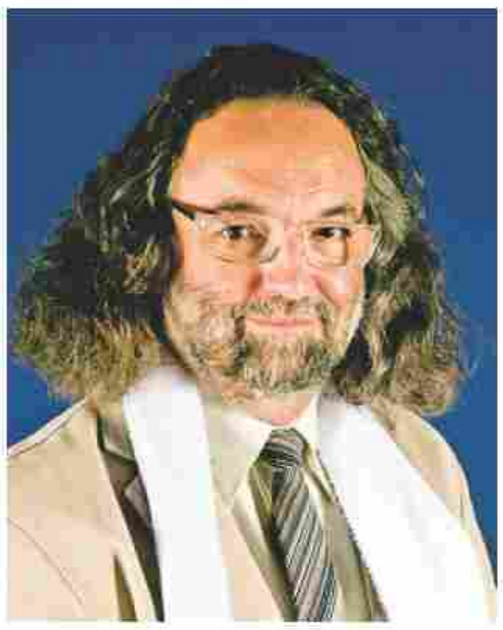
IV. Sumar de apărare cibernetică, de folosit în timpul pandemiei (și după)

43 **O Europă cu echipe de comunicare cibernetică slab coordonate, atât în cadrul UE cât și în diferitele state membre**
Autor: Laurent Chrzanovski

V. Resurse, link-uri utile, recomandări oficiale

55 Rapoarte recente: o selecție
Link-uri utile (România și Republica Moldova)
Recomandări oficiale

Limitările planurilor actuale de apărare cibernetică și nevoia de a regândi lumea digitală



Autor: **Didier Spella**

CHARENTE-MARITIME CYBER SÉCURITÉ — CMCS-CONNECT.FR —

Problematică

Criza actuală ne aruncă într-o situație specială, dar care totuși nu este prima de acest gen și cu siguranță nu va fi ultima.

Într-adevăr, această criză nu este cea dintâi. Cum însă are un impact direct asupra sănătății noastre, a fost pentru prima dată luată în considerare de toți liderii planetei. Dereglările climatice au constituit probabil prima criză de acest tip, însă diferența e că în cazul acesta, toți se simt feriți sau prea puțin îngrijorați... Mai regăsim acest tip de criză la nivelul atacurilor cibernetice.

Chiar dacă crizele sunt inevitabile, obiectivul liderilor trebuie să reprezinte minimizarea impactului pentru ca structura să continue să funcționeze chiar și în sistem de avarie și să-și poată relua după un anumit timp activitatea normală. Este ceea ce numim reziliență (valoare ce caracterizează rezistența la șoc a unui metal).

Astfel, a fost creat conceptul de BCP (Business Continuity Plan). Apoi i-au fost asociate DRP (Disaster Recovery Plan) și, pentru înțelegerea „vulnerabilităților" structurii, BIA (Business Impact Analysis).

BIO

Președinte al Mirat Di Neride, expert în strategie de afaceri și criminalitate informatică, director al CLUSIR Office - New Aquitaine Ouest, Didier Spella este fost ofițer superior al Forțelor Aeriene Franceze, co-fondator al conferinței harente-Maritime Cyber Sécurité. Cunoștințele sale atât din domeniul securității digitale cât și analoage, dar și experiența sa în domeniul analizei de risc și expertiza din cadrul companiilor americane i-au permis să se poziționeze ca un expert în definirea strategiilor de securitate. Confruntările cu atacurile cibernetice din ce în ce mai răspândite și mai intruzive la nivelul stilului de viață l-au determinat să organizeze o conferință care să abordeze riscurile la care populația în general este expusă și cei care au microîntreprinderi sau întreprinderi mici și mijlocii în special.

Definiții

- Business Continuity Plan: Plan de Continuitate a Activităților Comerciale
- Disaster Recovery Plan: Plan de Reluare a Activității după Dezastru
- Business Impact Analysis: Analiza de Impact asupra Activității Comerciale

Standardul 22301

Există un standard pentru evaluarea acestor chestiuni legate de reluarea activității, iar acest standard este ISO 22301. Acesta prevede cerințele pentru planificarea, dezvoltarea, implementarea, exploatarea, supravegherea, revizuirea, menținerea și îmbunătățirea permanentă a unui sistem de gestiune documentat. Implementarea standardului contribuie la reducerea probabilității apariției unui eveniment dezastruos, la pregătirea pentru o asemenea situație, la creșterea capacității de intervenție și de recuperare după incidentele perturbatoare de orice tip.

Cerințele specificate în standardul ISO 22301 sunt generice și sunt concepute pentru a fi aplicate la toate organizațiile (sau la părți din acestea), fără a ține seamă de tipul, mărimea și natura organizației. Aplicabilitatea acestor cerințe depinde de mediul operațional al organizației și de complexitatea acesteia.

Noi provocări

Pentru a înțelege ce se petrece, credem că e necesară modelarea crizelor pentru a le percepe mai bine mizele.

Aceste crize au mai multe caracteristici în comun:

- Absența granițelor geografice;
- Propagarea rapidă
- Propagarea aleatorie
- Impactul global
- Afectează mai multe activități
- Afectează mai multe sectoare
- ...

Aceste caracteristici diferite ne relevă limitările BCP și DRP. Într-adevăr, BIA nu acoperă situații cu astfel de caracteristici. Cerințele prealabile sunt în general următoarele:

- Riscurile acoperite sunt în general localizate în același areal (alunecări de teren, incendii, inundații etc.);
- Furnizorii de servicii nu sunt incluși în situația de criză (nu se află în același loc, nu activează în același domeniu, nu se bazează pe aceleași resurse etc.);
- Personalul sau o parte a personalului se poate deplasa;
- Organizațiile statale funcționează la parametri normali;
- ...

Așadar, rămân în continuare valabile analizele noastre? Planurile făcute vor putea să ne ajute să reluăm activitatea?

Structurile care dețineau deja astfel de analize și planuri au putut să le folosească pentru a trece în modul de izolare. Cele care nu aveau așa ceva, adică majoritatea, au „improvizat" pe loc moduri de organizare și soluții tehnice pentru a-și putea urma activitatea. Fiindcă măsurile de securitate au trecut în plan secund, organizațiile acestea și-au slăbit în mod „deliberat" gradul de protecție al sistemelor informatice proprii.

În ambele cazuri, furnizorii de servicii se regăsesc în aceeași situație; așadar organizațiile n-au putut beneficia de sprijinul acestora, spre deosebire de ceea ce se petrece în contextul unei crize localizate la nivelul unei companii sau, în cel mai rău caz, la nivelul unei regiuni.

Descoperim așadar limitările analizelor și planurilor pe care le-am elaborat până acum.

Deși nu este nici prima și nici ultima, această criză a demonstrat-o încă o dată: este necesar să ne regândim activitățile la nivel mai global.

Analizele noastre trebuie să ia în calcul următoarele noțiuni:

- Companie extinsă;
- Criză extinsă;
- Grade de autonomie.

Este nevoie ca planurile noastre:

- Să aibă o abordare globală din punct de vedere strategic, tactic și operațional;
- Să ia în calcul specificitățile complete ale structurii;
- Să contribuie la dezvoltarea unei conștiințe colective în rândul colaboratorilor.

Primele concluzii despre impactul a atacurilor „cyber-Covid"

Această criză sanitară ne relevă limitările modelelor de securitate pe care le-am conceput și care, constatăm acum, nu aveau decât un scop: liniștirea cetățenilor și a colaboratorilor. Dar limitările acestea au fost dovedite.

Abordările noastre în materie de securitate trebuie regândite într-o manieră mai globală. Ca întotdeauna, trebuie să rămânem în paradigma unei îmbunătățiri continue. De fiecare dată când credem că am acoperit un risc, trebuie să fim capabili să ne gândim la noul risc pe care tocmai l-am generat.

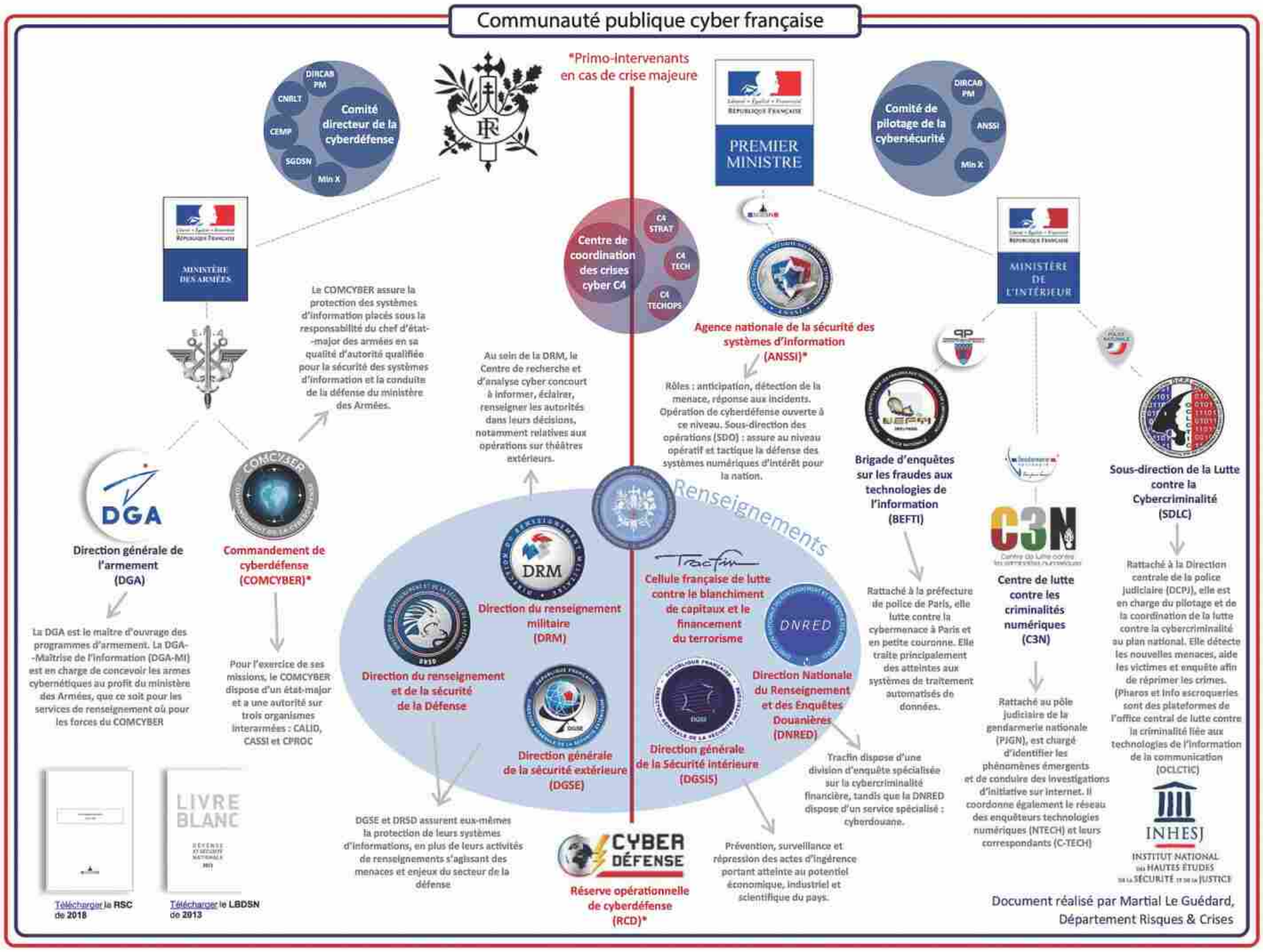
Cu gând la post-Covid: Pentru o maturizare a digitalizării

Digitalizarea pătrunde în toate sectoarele de activitate și cuprinde toate meseriile care rezultă din acestea, ceea ce ne determină să ne punem mai multe întrebări. Redăm aici câteva:

1) Cum vor evolua competențele profesionale?

2) În contextul avântului inteligenței artificiale, ne îndreptăm oare spre sfârșitul gândirii umane în favoarea gândirii mașinilor?

3) Cum poate evolua sistemul de formare?



O privire de ansamblu asupra comunității de securitate cibernetică din Franța.
(https://inhesj.fr/index.php/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure)

Aceste trei întrebări și multe altele referitoare la impactul digitalizării în viețile noastre de zi cu zi, nu reprezintă decât reflectarea unei problematici mai generale legate de acest proces de digitalizare.

Pentru mine, „digitalizarea" nu se poate rezuma doar la un termen care definește vag acțiunea sau acțiunile de transfer sau transformare a unei economii și a comportamentelor de tip analog într-o economie și în comportamente de tip digital.

Cred că, înainte de toate, e necesar să modelăm această digitalizare și să-i atașăm un criteriu de maturitate.

Propun așadar să analizăm împreună întrebările pe care le-am ridicat mai devreme, cu ajutorul modelului pe care-l vom realiza.

Modelul maturității digitalizării

Pentru a înțelege mai bine ce trăim acum, consider că am putea descrie un demers de digitalizare în 4 etape:

Etapa 1: digitalizarea suporturilor

Reprezintă cea dintâi etapă, care constă în transformarea oricărui tip de suport analog în suport digital: documente, muzică, pe scurt, toate categoriile posibile. Omul a atribuit acestor suporturi un uz practic.

Etapa 2: digitalizarea instrumentelor simple

Presupune transformarea, adaptarea instrumentelor de tip analog în instrumente digitale. Mașina de scris devine procesator de text, instrument pentru calcule, registru de calcul etc. Mașinile-unelte sunt digitalizate. Omul devine un utilizator.

Etapa 3: interogarea instrumentelor

Această a treia evoluție constă în integrarea acestor instrumente simple pentru a alcătui instrumente mai complexe, care combină tehnologii diferite: platformă digitală – comunicare – energie. Suporturile digitale sunt și ele combinate.

Suntem martorii apariției unor instrumente complexe, care utilizează mai mult sau mai puțin caracteristicile tehnice ale fiecărei componente tehnologice din care sunt alcătuite. Cei care creează conceptul acestor instrumente cuantifică confortul în parametri, însă nu putem vorbi de un progres real. Omul trebuie să se adapteze la instrumentul digital.

Etapa 4: integrarea digitală

Prin conceptul de „integrare digitală", mă refer la conceperea sistemelor digitale complet integrate, care oferă personalizarea tuturor acestor instrumente și nu doar a unui singur parametru. Omul devine elementul central în această digitalizare; el poate alege instrumentele care îi sunt necesare și utile. Aceste instrumente vor evolua odată cu nevoile omului. Personalizarea este efectivă.

După dezvoltarea acestui model, putem să răspundem la întrebările de mai sus.

Cum vor evolua competențele profesionale?

Dacă reluăm modelul expus anterior, observăm că evoluția competențelor este una reală. În primul rând, oricare ar fi activitatea pe care o desfășurăm, trebuie să fim capabili să folosim funcțiile de bază ale instrumentelor care ne definesc activitatea.

Totuși, acest nivel de competență nu permite accederea decât la primele 3 nivele de maturitate.

Trebuie să planificăm dezvoltarea de noi competențe care să permită atingerea nivelului 4. Acest nivel trece printr-o „redefinire digitală" a activității, lucru care necesită, în plus față de o bună stăpânire a activității propriu-zise, și cunoașterea tuturor posibilităților pe care le oferă lumea digitală, pentru a fi capabili să concepem o integrare digitală a activității noastre.

În contextul avântului inteligenței artificiale, ne îndreptăm oare spre sfârșitul gândirii umane în favoarea gândirii mașinilor?

Lumea digitală ne propune în prezent posibilități imense de calcul care permit conceperea și dezvoltarea unor instrumente capabile să „ia decizii". Cel puțin, asta ne propune lumea inteligenței artificiale.

Totuși, chiar dacă calculele par „infinite", aceste instrumente nu vor reuși niciodată să creeze „de la zero" ceva, așa cum doar mintea umană o poate face. Iar această capacitate ne-a permis să evoluăm și să gândim imposibilul. Într-un mod foarte simplist, aș spune că în acest moment omul e capabil să viseze, lucru pe care o mașinărie digitală nu va ști niciodată să-l facă.

În cazul în care am fi la nivelul 4 de maturitate a sistemelor, ne-am îndrepta deci mai mult spre un ajutor al funcției noastre de decizie. Mașinăria ne-ar propune o gamă de soluții pe care le poate găsi, cu limitările ei: probabil modele de evoluție și reprezentarea lor „mediatică".

Ar rămâne în sarcina noastră alegerea celei mai bune soluții.

Care e locul sistemului de formare în această evoluție?

În contextul acestei reflecții, pare evident că și formarea trebuie să evolueze, ba chiar să se schimbe.

Nu putem să ne mulțumim doar cu perspectiva ca evoluția formării să se reducă doar la digitalizarea suporturilor (ușurarea ghiozdanelor școlarilor) sau utilizarea instrumentelor digitale care să crească interacțiunea dintre elevi și profesori.

În contextul „integrării digitale", trebuie să creăm noi forme de învățare în care subiectul actului învățării să fie în centrul dispozitivului de transmitere de cunoștințe.

Rolul profesorului evoluează spre un rol de element care prescrie învățarea pentru elevii săi. Înlocuim conceptul de „elev" cu cel de „subiect al actului învățării" în centrul dispozitivului de formare. Care este nivelul acestuia, care sunt nevoile sale, care-i sunt competențele, iată primele întrebări pe care ar putea să și le pună profesorul pus față în față cu elevul său. O personalizare completă a actului de învățare ar putea fi implementată astfel încât fiecare elev să dobândească competențele necesare propriei „evoluții".

Concluzie

În concluzie, consider că trebuie să avem în vedere, în context digital, o transformare majoră a societății. Digitalizarea societății nu se poate rezuma doar la a fi utilizatori de instrumente digitale mai mult sau mai puțin dezvoltate și integrate în modul nostru de viață.

Nu trebuie să confundăm progresul cu îmbunătățirea gradului de confort. În prezent, suntem în faza îmbunătățirii gradului de confort. Trebuie să ne adaptăm lumii digitale pentru a profita de ce are aceasta să ne ofere, iar de aici decurg și rupturile digitale la care suntem martori.

Adevăratul progres va fi atins atunci la finalul unui proces de integrare completă a aspectului digital în activitățile noastre. Sfera digitală trebuie să examineze activitățile noastre și nu invers. ■

Manipularea prin gestionarea emoției

Interacțiunile virtuale oferă un anonimat și pot ascunde motivația disimulată a unei comunicări. Utilizatorii creează realități prin declarații cu veridicitate incertă. Caracterul fugitiv și circumstanța schimbului lasă puțin spațiu unei comunicări emotive. Reacțiile se transformă în producții compuse cu grijă. Această regizare a emoțiilor are uneori ca obiectiv manipularea unui sau mai multor interlocutori, fascinându-i sau terorizându-i. Acest lucru poate lăsa cale liberă unor strategii discursive ale unor mișcări teroriste care pun în aplicare, atunci când sunt abordate de potențiali simpatizanți, scenarii care sunt capabile să stârnească o anumită emoție. Prin interacțiunea directă cu interlocutorul său, un manipulator își construiește o relație semantică bazată pe suprapunerea emoțiilor pozitive sau negative pe fondul apartenenței la o comunitate, pe fondul unei legături cu evenimentul sau al unei fascinații cu privire la reprezentările vizuale proprii unei culturi. Articolul Laurei Ascone explorează acest câmp cognitiv abordat arareori în mod științific.

Recursul la emoții în spațiul digital: între strategie discursivă și manipulare

Autor: **Laura Ascone**

Adesea acuzat de dezumanizarea relațiilor interpersonale, spațiul digital reprezintă în realitate laboratorul noilor forme de exprimare a emoțiilor. Reacțiile emoționale, spontane prin natura lor, se transformă aici în producții compuse cu grijă. Această regizare a emoțiilor are uneori ca obiectiv manipularea unui sau mai multor interlocutori, fascinându-i sau terorizându-i.

Emoții și spațiu digital

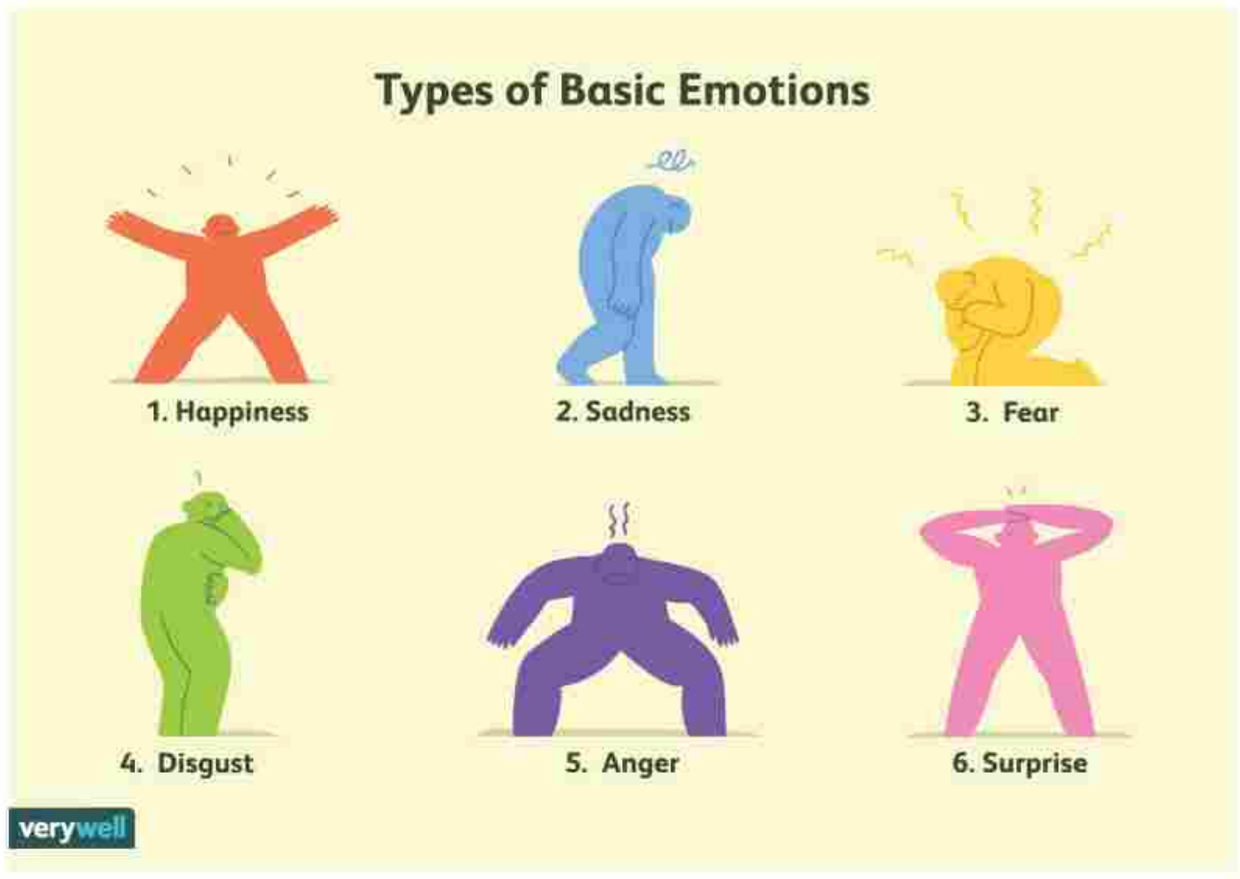
Deschiderea către spațiul digital și numeroasele inovații în comunicare au modificat inevitabil felul în care individul se raportează la lume și la cei care-l înconjoară. Mai precis, noțiunile de timp și de spațiu s-au schimbat dramatic. În spațiul digital, comunicarea prin intermediul rețelelor are propria sa axă a timpului. În ciuda unui aparent caracter instantaneu, interacțiunile virtuale nu sunt atât de fluide temporal ca interacțiunile reale. În timp ce un utilizator trebuie să aștepte ca interlocutorul său să scrie și să trimită mesajul, celălalt trebuie să aștepte ca mesajul să fie citit înainte de a primi un răspuns. Și totuși, niciunul din utilizatori nu pare să perceapă decalajul de temporal. În mod asemănător, interacțiunile virtuale se disting de cele reale în plan spațial. Deși utilizatorul este în fața calculatorului în lumea reală și deși mesajele sunt vizibile pe ecran, interlocutorii nu împart același spațiu (1).

BIO

Doctor în Științele Limbajului, Laura Ascone și-a scris teza despre „Radicalizarea prin exprimarea emoțiilor pe Internet", la Universitatea Paris Seine. În prezent, ea urmează studii post-doctorale la Université de Lorraine în cadrul unui proiect al Agenției Naționale pentru Cercetare despre discursul urii împotriva migranților. Cercetările sale au ca obiect exprimarea emoțiilor pe rețelele sociale, propaganda jihadistă și contra-discursul, precum și mesajele pline de ură împotriva migranților.

MULȚUMIRI: Articolul original al Laurei Ascone a fost publicat în Revue de la Gendarmerie Nationale nr. 266, decembrie 2019, pp. 30-35. Suntem profund recunoscători Generalului Marc Watin-Agouard, director al redacției, și Colonelului Philippe Durand, redactor-șef al revistei, pentru privilegiul de a reproduce acest text și a-l traduce în exclusivitate în română și engleză. Suntem de asemenea recunoscători autoarei, pentru amabilitatea și disponibilitatea sa.

Numerele Revue de la Gendarmerie National sunt disponibile online la adresa: https://www.gendarmerie.interieur.gouv.fr/Notre-communication2/Publications-Documentations/La-revue



Emoțiile de bază © ONG Verywell Mind, www.verywellmind.com

Spontaneitatea emoțiilor pusă la încercare

Decalajul spațio-temporal, care caracterizează interacțiunile virtuale, oferă utilizatorilor posibilitatea de a-și ascunde identitatea și motivul actului comunicării. Altfel spus, utilizatorii pot crea orice tip de realitate și de identitate prin declarații mai mult sau mai puțin veridice. În plus, acest decalaj influențează puternic modul în care interlocutorii interacționează și își exprimă emoțiile. În spațiul digital, atunci când utilizatorul are o reacție emoțională pe care dorește să o comunice interlocutorului său, va ține cont în mod automat de contextul în care se exprimă în acele clipe. Astfel, va avea tendința de a-și adapta exprimarea emoțiilor în funcție de interlocutor, de tipul conversației pe care o poartă și de mijlocul de comunicare folosit.

În plus, adaptarea reacțiilor emoționale influențează indirect reacțiile interlocutorului și, prin urmare, însăși conversația. Cu alte cuvinte, luarea unei decizii cu privire la modul de exprimare a unei emoții reprezintă luarea unei decizii cu privire la modul de acționare asupra interlocutorului, asupra comunicării și asupra mediului. Mai precis, utilizatorul acționează asupra interlocutorului întrucât interpretarea și reacția acestuia din urmă depind în principal de modul în care emoția a fost exprimată. Kramer et at. (2) au demonstrat cum o emoție exprimată pe Facebook influențează emoțiile altor utilizatori.

Exprimarea emoțiilor joacă deci un rol crucial în orice interacțiune, fie ea reală sau virtuală. Atunci când utilizatorul interacționează în spațiul digital, emoțiile pe care le resimte se disipează instantaneu, înainte să aibă timp să le exprime în scris. Această caracteristică provine din faptul că emoțiile nu durează decât câteva milisecunde. Prin urmare, utilizatorul va putea să decidă, mai mult sau mai puțin voluntar, cum să-și verbalizeze reacțiile emoționale. Fără să mai fie vorba despre o reacție spontană, comunicarea virtuală poate fi considerată o comunicare emotivă. Spre deosebire de comunicarea emoțională, în care individul își exprimă emoția în clipa în care o simte, comunicarea emotivă este caracterizată de descrierea emoției odată ce aceasta s-a disipat (3). Cu alte cuvinte, comunicarea emotivă se apropie mai mult de noțiunile de articulare, retorică și persuasiune (4). Emoțiile pot fi așadar regizate cu scopul de a influența reacțiile și comportamentul interlocutorului.

Discursul propagandei teroriste difuzat în spațiul digital constituie un exemplu evident al acestei exploatări, mai mult sau mai puțin subtile, a exprimării emoțiilor.

Legătura dintre discursul de propagandă teroristă și emoții poate fi regăsită în substantivul latin *terror*. Acest termen provine din rădăcina indoeuropeană ter-, care înseamnă „a tremura" și care marchează legătura dintre terorism și frică (5).

Discursul jihadist ilustrează apropierea dintre acțiunea teroristă și frică. La data de 4 iulie 2014, când a fost reinstaurat califatul, Abu Bakr Al-Baghdadi a afirmat că ar trebui să „se revină la Islamul originar pentru a obține iertarea

lui Allah și pentru a regăsi mândria arabă, inspirând teamă infidelilor și musulmanilor necredincioși".

Cu alte cuvinte, conform liderului ISIS, instituirea fricii este mai importantă decât uciderea infidelilor și a musulmanilor necredincioși. În privința discursului propagandist difuzat în spațiul digital, revista jihadistă Dar al-Islam constituie o sursă crucială de analiză, întrucât permite o mai bună înțelegere a strategiilor discursive folosite de ISIS.

Publicată începând cu 23 decembrie 2014, Dar al-Islam are până în prezent 10 numere și se adresează unui public care s-a raliat deja ideologiei jihadiste. Întrucât nu avem de-a face cu o interacțiune, revista nu-și poate adapta discursul în funcție de interlocutor. Editorul trebuie așadar să țină cont de indivizii cu profiluri diferite care pot avea acces la acest conținut. Deși exprimarea emoțiilor joacă un rol central în discursul propagandist, putem constata că emoțiile sunt arareori exprimate în mod direct. Dimpotrivă, emițătorul recurge la scenarii care pot genera o anumită emoție. Discursurile și imaginile contribuie astfel la regizarea emoțiilor pentru a întări apartenența la ideologia jihadistă. Iar dacă exaltarea grupului jihadist are scopul de a crește atașamentul pentru această comunitate, condamnarea inamicului are ca obiectiv alimentarea urii împotriva acestuia.

Emoții și înrolare

Discursul jihadist în spațiul digital nu circulă doar prin intermediul revistelor oficiale. Rețelele sociale constituie și ele vectori de propagandă jihadistă. Spre deosebire de Dar al-Islam, interacțiunile pe rețelele sociale se adresează unui public pe cale de radicalizare. În consecință, exprimarea emoțiilor vizează influențarea interlocutorului, pentru ca acesta să îmbrățișeze ideologia promovată. Videoclipul Ils te disent, produs de guvern pentru a combate radicalizarea jihadistă în spațiul virtual, furnizează un exemplu în acest sens. După ce a vizitat profilurile de Facebook ale mai multor jihadiști, protagonistul din videoclip primește un mesaj:

1. Salut
Cool les trucs que tu like,
ça t'intéresse ce ki se passe
au Cham en ce moment ?

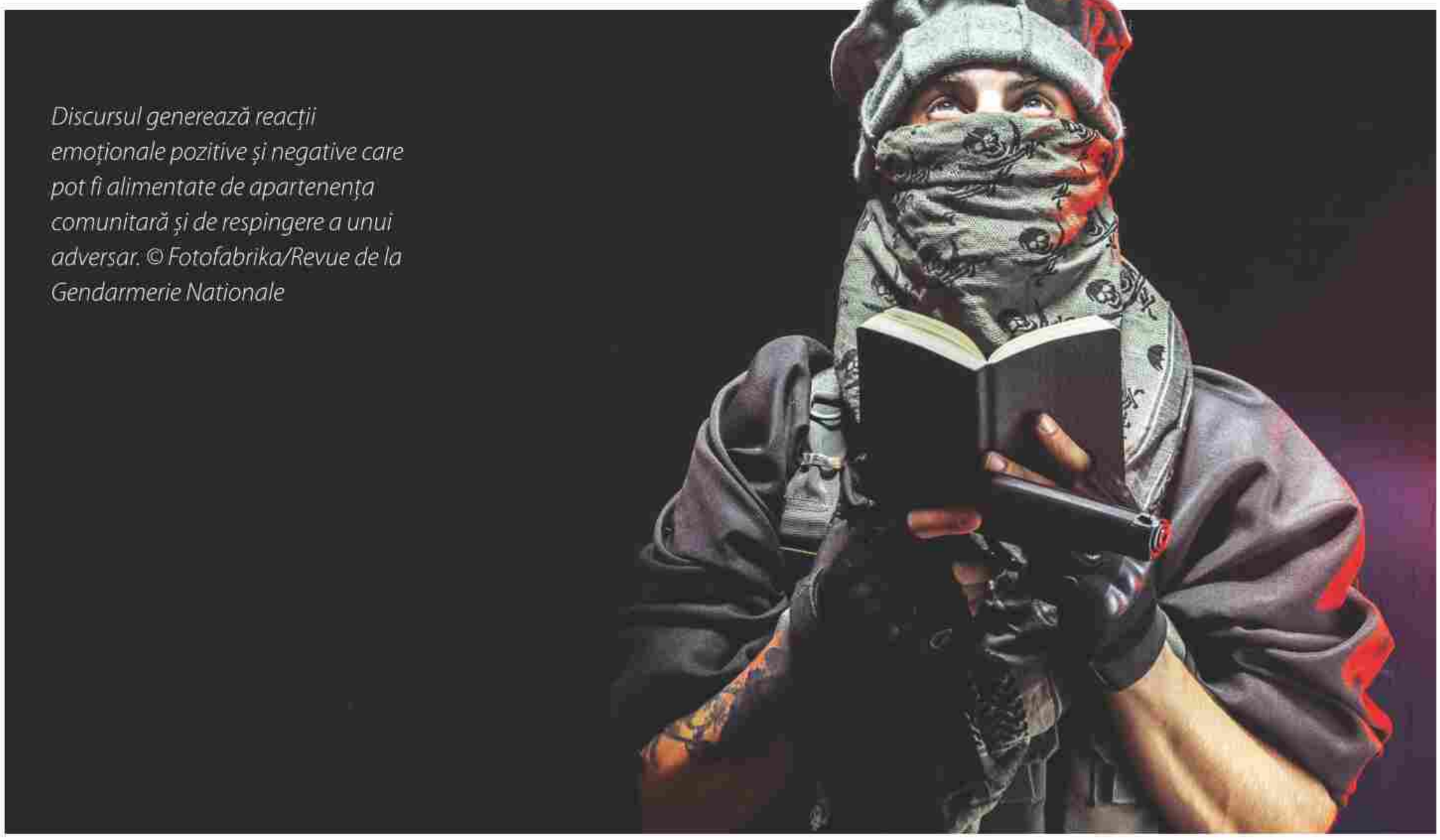
si ta des questions hésite pas,
la vérité elle est la bas,
c'est maintenant qu'il faut partir !

si tu me donnes ton num j'ai des amis
la bas ki se battent jte met en contact.

1. Salut
Mișto chestiile la care ai dat like,
te interesează ce se întâmplă
acum în Siria?

dacă ai întrebări nu ezita,
adevărul e acolo
trebuie să plecăm acum!

dacă-mi dai numărul tău am prieteni
acolo care luptă te pun în contact.



Discursul generează reacții emoționale pozitive și negative care pot fi alimentate de apartenența comunitară și de respingere a unui adversar. © Fotofabrika/Revue de la Gendarmerie Nationale

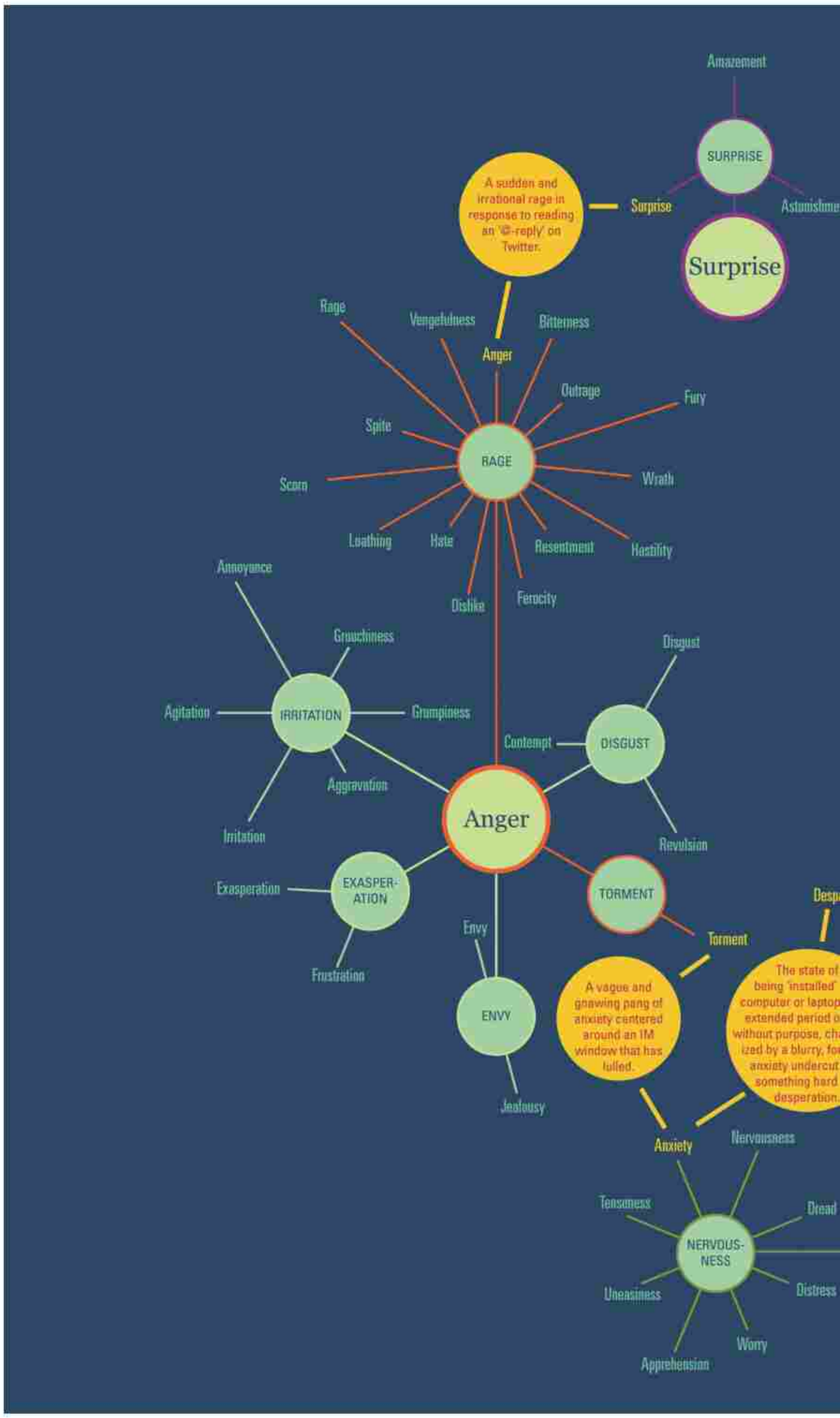
Deşi este o reproducere, acest mesaj demonstrează caracterul anxiogen al mesajelor trimise de cei care se ocupă cu recrutarea. Interacționând în mod direct cu interlocutorul, cel care efectuează racolările își poate adapta cu ușurință discursul. Poate inclusiv să-ți creeze o identitate ad hoc, grație naturii spațiului virtual: percepția pe care o avem vizavi de un individ e construită în principal din informații pe care acesta ni le transmite (6). Alegerea multor jihadiști de a folosi poze cu lei ca poză de profil pe Facebook are scopul de a-i înfățișa ca persoane puternice și curajoase. Utilizatorul, care are tendința de a uita și de a se detașa de lumea reală care-l înconjoară, va sfârși prin a percepe tot ce se petrece în spațiul virtual ca fiind adevărat și real. Ben-Ze'ev (7) definește acest fenomen „detatașare" (detattachment). În ciuda distanței spațio-temporale, utilizatorul este încercat de un sentiment de atracție și stabilește un fel de relație cu interlocutorul său. Obiectivul acestei manipulări a emoțiilor în reprezintă separarea individului de anturajul său real pentru a înceta să manifeste emoții față de cei apropiați. De asemenea, prin expunerea la conținut violent, jihadistul caută să-și obișnuiască ținta cu violența și să îi alunge teama de a muri. Altfel spus, persoana care se ocupă cu racolarea se folosește de emoții pentru ca ținta sa să nu le mai perceapă.

Combinație paradoxală a emoțiilor în discursul jihadist

Deşi legătura dintre terorism și frică este evidentă, discursul terorist jihadist nu e construit doar în jurul fricii și a altor emoții negative. Din dorința de a-i fascina deopotrivă pe simpatizanți, discursul jihadist recurge și la emoții pozitive. În cadrul aceluiași discurs, se împletesc astfel reacții emoționale pozitive și negative. În anumite cazuri, două sentimente opuse (8) se alimentează reciproc. Ura împotriva inamicului necredincios alimentează dragostea pentru comunitate jihadistă. Viceversa, dragostea pentru comunitate alimentează ura împotriva inamicului. Această juxtapunere de emoții pozitive și negative se poate produce și în relație cu un eveniment. Un atac terorist într-un stat occidental va stârni reacții pozitive precum bucuria, mândria și adrenalina în cadrul comunității jihadiste. În plus, același atac ar putea produce reacții pozitive chiar în cadrul comunității vizate. Atentatele săvârșite în Franța, de pildă, au trezit sentimente de solidaritate și de dragoste.

O abordare de analiză a emoțiilor în spațiul virtual

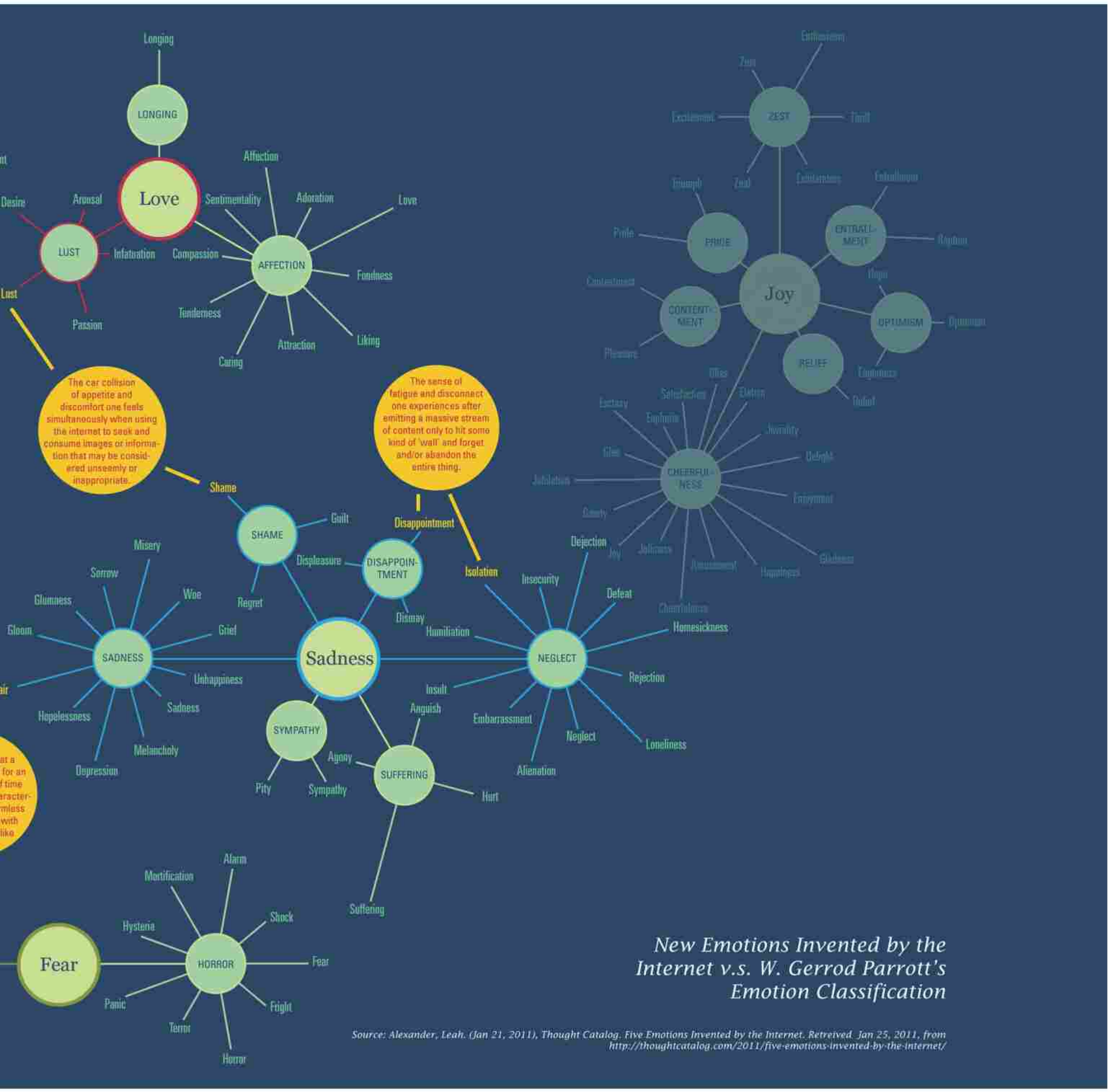
Această panoramă sintetică a exprimării emoțiilor în spațiul virtual a dezvăluit elemente care ar trebui luate în calcul în procesul de examinare a discursului jihadist disponibil pe Internet. Întâi de toate, analizarea unui text în propriul context este foarte importantă. Trebuie luate în considerare mijlocul de comunicare folosit și impactul pe care acesta în poate avea asupra discursului, evenimentele la care interlocutorii pot face referire și punctul de vedere al diverșilor utilizator care participă la conversație. Mai precis, acest din urmă aspect ne ajută să stabilim dacă un mesaj care exprimă o emoție pozitivă integrează un conținut pozitiv sau dacă, din contră, obiectul unei astfel de emoții constituie un pericol potențial pentru comunitate. În plus, trebuie să ținem seama că discursul nostru este încărcat de impresii personale, chiar și atunci când nu ne exprimăm în mod direct emoțiile (9). Prin urmare, pentru



a studia radicalizarea jihadistă prin exprimarea emoțiilor în spațiul virtual, nu ne putem mărgini la analiza exclusivă a emoțiilor negative. Mai mult, așa cum am subliniat-o deja, nu doar exprimarea emoțiilor constituie un subiect important de analiză, ci și felul în care emițătorul, prin discursul său, stârnește reacții emoționale interlocutorului. ■

Note:

(1) Kramsch, C. G. (2009). The Multilingual Subject: what foreign language learners say about their experience and why it matters. Oxford University Press.
(2) Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive- scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 8788-8790.
(3) Plantin, C. (2011). Les bonnes raisons des émotions. Peter Lang Publishing Group.
(4) Arndt, H., & Janney, R. W. (1991). Verbal, prosodic, and kinesic emotive contrasts in speech. Journal of pragmatics, 15(6), 521-549.
(5) Di Cesare, D. (2017). Terrore e modernità. Torino: Giulio Einaudi Editore.
(6) Mantovani, G. (2002). Internet haze: why new artifacts can enhance situation ambiguity. Culture and Psychology 8, 307–326.
(7) Ben-Ze'ev, A. (2005). 'Detattachment': the unique nature of online romantic relationships. In Y. Amichai- Hamburger (ed.), The social net: Human behavior in cyberspace, 115–138. New York: Oxford University Press
(8) Spre deosebire de emoții, care nu durează decât câteva milisecunde, sentimentele au o durată mai mare. Ekman (1992) identifică șase emoții primare: bucurie, frică, furie, surpriză, tristețe și dezgust.
(9) Shaver, P., Schwartz, J., Kirson, D., & O'connor, C. (1987). Emotion knowledge: further exploration of a prototype approach. Journal of personality and social psychology, 52(6), 1061



New Emotions Invented by the Internet v.s. W. Gerrod Parrott's Emotion Classification

Source: Alexander, Leah. (Jan 21, 2011), Thought Catalog. Five Emotions Invented by the Internet. Retreived Jan 25, 2011, from http://thoughtcatalog.com/2011/five-emotions-invented-by-the-internet/

Această ediție specială este plasată sub egida a:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

A fost realizată în partenariat cu:

Gendarmerie Nationale (FR)
www.gendarmerie.interieur.gouv.fr/

Centre de recherche de l'École des Officiers de la Gendarmerie Nationale (FR)
www.gendarmerie.interieur.gouv.fr/crgn/

Police de Genève (CH)
www.ge.ch/organisation/corps-police

Centrul Național CYBERINT, Serviciul Român de Informații (RO)
www.sri.ro

Direcția de Combatere a Criminalității Organizate, Poliția Română (RO)
www.politiaromana.ro

Centrul Național de Răspuns la Incidente de Securitate Cibernetică (RO)
www.cert.ro

Autoritatea Națională pentru Administrare și Reglementare în Comunicații (RO)
www.ancom.ro

Global Cybersecurity Center (IT)
www.gcsec.org/

Association des Utilisateurs des Systèmes d'Informations au Maroc
http://www.ausimaroc.com/

Forum international de la cybersécurité (FR)
www.forum-fic.com

Charente-Maritime Cyber Sécurité (FR)
www.cmcs-connect.fr

Cybersecurity Dialogues (RO-IT-CH)
www.cybersecurity-dialogues.org

SwissCybersecurity (CH)
www.swiss-cybersecurity.ch

Și cu sprijinul a:

www.blockapt.com

www.bursa.ro

www.stanchionpayments.com

Când izolarea asociată cu dezinformarea conduc la internări în spital

Autor: **Octavian Oancea**

Dragă cititorule,

Astăzi voi lăsa deoparte specializarea mea în securitatea informațiilor și îți voi împărtăși o poveste autentică, scoasă din sertarul întâmplărilor personale.

Zilele trecute, s-a petrecut un incident deopotrivă neobișnuit și trist. În timp ce viața și munca mea se scurgeau în relativă liniște venită din actuala izolare auto-impusă, un prieten mi-a telefonat pentru a-mi relata starea unei cunoștințe comune. Se pare că acest terț prieten suferise un sever episod de depresie. De ceva ani, eram cu toții conștienți că el ajunsese un consumator avid de diverse teorii conspiraționiste. Faptele și argumentele științifice prezentate de noi ca și contra-argumente fuseseră mereu în van. Dincolo de inconsistența și veridicitatea îndoielnică a ideilor în sine, nu intuisem însă efectul devastator pe care acești ani de informare eronată îi pot avea asupra minții sale. Derulând evenimentele, iată-ne vizitându-ne prietenul la spital. Da, atât de grav s-a ajuns!

Ca urmare a vizionării în exces a amalgamului de conținut online despre Corvid-19, intensificate de melanjul fără sens din jurul tehnologiei GA și al altor pseudo-incidente, bietul om a ajuns într-o stare de panică exagerată. A ajuns apoi la limita psihică și fizică în care nu a mai putut dormi nopți la rând. În final, organismul a colapsat. Cu ultima licărire de luciditate rămasă, a realizat ce se întâmpla și a cerut ajutor specializat.

În timpul plimbării noastre prin curtea spitalului, ne-a mărturisit că abia acum percepe implicațiile deciziilor lui anterioare, admițând că totuși, în

BIO

Octavian Oancea este, în prezent, CEE Channel Business Manager la Trend Micro. Are o Licență în Științe și un Master în Științe de la Universitatea Politehnică din București. Este pasionat de atingerea excelenței, atât în carieră cât și în viața lui privată. Ca profesionist, se dovedește extrem de abil în evaluarea piețelor și identificarea oportunităților neexploatate prin încheierea de noi parteneriate de afaceri. Pozițiile deținute anterior includ Director General și Fondator McAfee Romania, Avnet Technology Solutions Romania și ZyXEL Communication Romania. Pe partea personală, interesele sale sunt muzica, fotografia, sportul și tehnologia informației, cu accent pe securitatea datelor.

trecut, îi fusese cu neputință să renunțe la acele elucubrații. Într-un mod bizar, îi hrăneau nevoia de senzațional, flatându-i iluzia de privilegiat ce are acces la acest tip de informații.

Această istorisire este un liant pentru subiectul articolului de față: dezinformarea și impactul asupra sănătății. Prinși în agitația cotidiană a vieții, tindem să ignorăm acest risc, în principiu deoarece ne-am educat în a selecta conținutul știrilor pe care le consumăm.

Și asta pentru că noi, lucrând în domeniul securității informațiilor, suntem cei favorizați – profesiunea ne arogă capacitatea de a detecta știrile false și dezinformarea pentru că avem de-a face cu conexele: campanii de phishing, inginerie socială și întreaga pletoră.

Trebuie să recunosc, în multe rânduri, când prietenii îmi cereau ajutorul în a-și securiza datele, le ofeream prompt metode legate, ei bine, de siguranța aparatului în sine și a datelor de pe el - și cum să-și schimbe ei obiceiurile în modul în care îl operează, pentru o mai bună securitate.

Foarte puțin i-am sfătuit în sfera consumului de știri per se, care, în perioada actuală, a căpătat valențe preponderent nocive.

Reflectați câteva clipe: să presupunem că, printr-un context nefast, unul dintre dispozitivele tale este infectat. Șansele sunt ca, având un sistem de securitate anterior instalat, să se soldeze doar cu o ușoară sperietură. Într-o situație mai gravă, ai putea eventual pierde datele acumulate. Și astfel, expus la consecințe, îți reevaluezi alegerile de securitate. Cu toate acestea, în afara frustrării inerente, te adaptezi și corectezi. Inclusiv în cazuri de pierderi financiare semnificative, majoritatea depășesc momentul, odată lecția asimilată.

Acum, să revenim la traiectoria pe care o poate avea frustrarea zilnică provenită din multiple surse - știri, social media, TV - cu precădere pe parcursul perioadei de izolare actuale. Virusul ne conferă niște dileme insolubile, este în afara capacității noastre de a-l controla. În consecință, plutim într-o perpetuă stare de teamă: pentru familiile noastre, sănătate, siguranța financiară. O nesfârșită succesiune de necunoscute, concomitent cu un interval sporit de timp pe care îl acordăm tehnologiei. Rezultă o combinație repetitivă zilnic, cu un masiv potențial distructiv asupra creierului uman. Deloc surprinzător, după carantină, mulți se îndreaptă direct către avocați, iar alții către psihologi.

Însă unde îmi propun să ajung? Conștienți de cele precizate mai sus, este necesar să ne asumăm rolul în societate și să educăm populația în ceea ce privește consumul de informații. Umanitatea a depășit până acum crize severe, însă acum ne confruntăm cu un nivel neobișnuit de manipulare media, pe care majoritatea covârșitoare nu îl poate gestiona. Și, cu precădere în perioada curentă, consecințele sunt neindulgente asupra stării de bine și sănătății mentale ale populației.

la legătura cu prietenii tăi apropiați astăzi. Întreabă-i cum le merge și, dacă poți, îndreaptă discuția încât să îi poți ajuta să își selecteze știrile zilnice. Să începem chiar cu cea de față ☺. ■

Securitatea perimetrală, VPN și Zero Trust în pandemie de Coronavirus

Autor: Cătălin Pătrașcu

Mai multe titluri (1-3) din mass-media atrag atenția că, odată cu pandemia de Coronavirus (SARS-CoV-2), s-au înmulțit simțitor atacurile cibernetice, atacatorii concentrându-se acum pe exploatarea acestei situații, fapt confirmat de altfel și de autorități (4-5).

Acest fapt se datorează pe de o parte faptului că pandemia a acaparat practic toată atenția globală, iar acest interes crescut potențează foarte mult atacurile bazate pe tehnici ce țin de inginerie socială (phishing, spear-phishing, watering hole, spam, scam etc.). Pe de altă parte majoritatea oamenilor lucrează acum de acasă și accesează resursele informatice ale companiei

(email, documente, baze de date, documente etc.) de la distanță, generând vulnerabilități pentru companiile care se bazează încă pe conceptul de securitate perimetrală (din păcate majoritatea).

Nu vorbim totuși de tipuri noi de atac, sau de noi tehnici utilizate de atacatori. Diferența este că pandemia oferă o „platformă" mai bună și un context favorabil. Spre exemplu, atacurile de tip watering hole se bazează pe infectarea cu malware a website-urilor utilizate de grupul țintă, având ca efect infectarea celor care accesează respectivele website-uri. Ori, în acest moment, website-urile care oferă informații și hărți în timp real despre pandemie sunt candidații ideali pentru un astfel de atac, iar atacatorii au sesizat imediat oportunitatea.

BIO

Cătălin este expert în securtate cibernetică, cu peste opt ani de experiență relevantă în domeniu. Și-a început călătoria în domeniul securității cibernetice în cadrul Ministerului Apărării Naționale (2010-2012), a continuat în calitate de coordonator al echipei de răspuns la incidente din cadrul Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO (2012-2018) și activează, în prezent, ca manager de livrare de servicii de securitate cibernetică în cadrul unei companii de profil. A gestionat cu succes proiecte în domeniul securității cibernetice, a planificat și moderat exerciții cibernetice, a gestionat incidente cibernetice la scară națională și a efectuat diverse studii pe teme de securitate cibernetică și criminalitate informatică.

Dar să revenim la conceptul de securitate perimetrală. Tradițional, companiile își securizează infrastructura prin crearea de zone virtuale de rețea, cel mai adesea Internet (zona publică, nesecurizată), DMZ (zonă dedicată de obicei serverelor și aplicațiilor) și LAN (rețeaua internă). Doar că mobilitatea crescută a angajaților și nevoia de accesare a resurselor companiei de oriunde s-ar afla a evidențiat deja limitele acestei strategii. Tehnologia VPN a venit ca o salvare de moment, care înseamnă de fapt că terminalele din afara rețelei sunt conectate printr-o rețea virtuală la rețeaua internă a companiei, având astfel acces la resurse ca și atunci când s-ar afla efectiv în acea rețea.

Doar că pandemia a făcut ca numărul de conexiuni VPN să crească semnificativ și multe companii nu au fost pregătite, în sensul că echipamentele care facilitau acest tip de conexiuni nu au fost dimensionate pentru ca toți angajații să se conecteze de acasă. A trebuit ca într-un timp foarte scurt companiile să facă upgrade de hardware, care pe lângă costuri financiare de obicei înseamnă și o întrerupere temporară a serviciilor.

Ideal ar fi ca securitatea perimetrală și tehnologia VPN să fie înlocuite cu un nou framework numit „Zero Trust" care se bazează pe faptul că un utilizator, terminal, aplicație, sau proces are același nivel de încredere, oriunde s-ar afla, accesul acordându-se granular. Din fericire acest framework este util nu numai în contextul pandemiei de Coronavirus ci mai ales în normalul ultimilor ani, când mobilitatea și munca de la distanță au luat amploare. ■

Software-uri (legale!) pentru piratarea VPN-urilor slab configurate © https://whitehattricks.blogspot.com/2019/09/Hack-VPN-Accounts-Download-All-VPNHunter-free.html

Note:

(1) https://euobserver.com/coronavirus/147869
(2) https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
(3) https://securitytoday.com/articles/2020/03/26/world-health-organization-facing-cyber-attacks-during-coronavirus-response.aspx
(4) https://cert.ro/citeste/alerta-campanii-frauduloase-coronavirus
(5) https://www.us-cert.gov/ncas/alerts/aa20-099a

IV. Sumar de apărare cibernetică, de folosit în timpul pandemiei (și după)

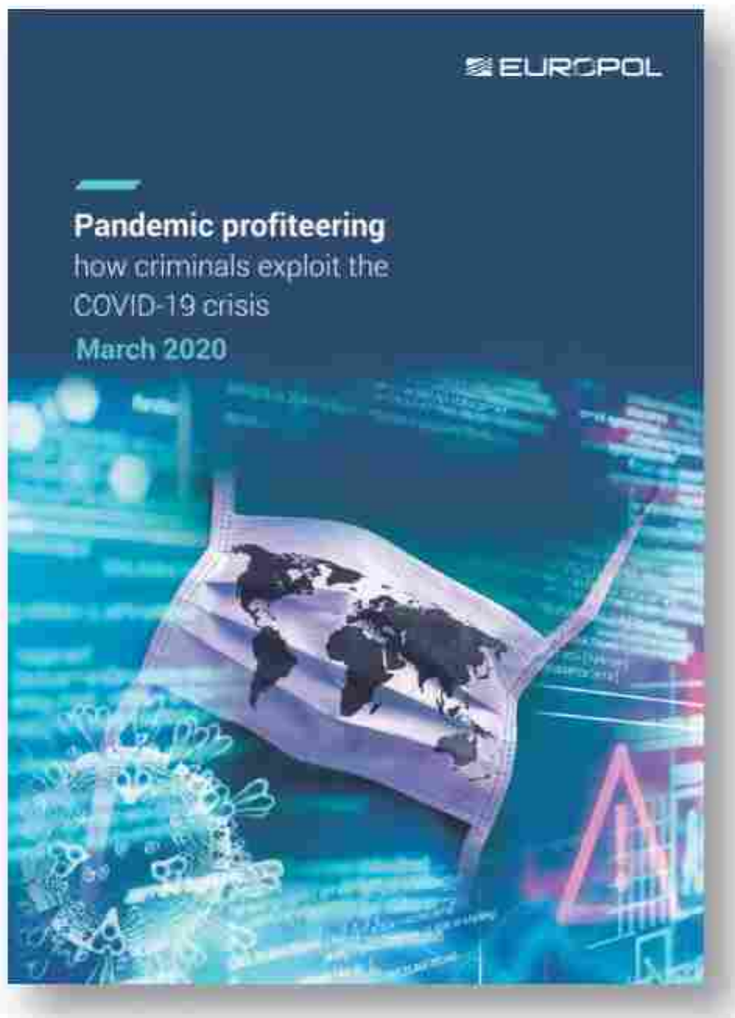
O Europă cu echipe de comunicare cibernetică slab coordonate, atât în cadrul UE cât și în diferitele state membre

Author: **Laurent Chrzanovski**

BIO

Cu un doctorat în Arheologie Romană obținut la Universitatea din Lausanne, o diplomă de cercetare postdoctorală în istorie și sociologie la Academia Română, Filiala Cluj-Napoca și o abilitare UE în a coordona doctorate în istorie și științe conexe, Laurent Chrzanovski este co-director de doctorate la școala doctorală la Universitatea Lyon II Lumière și susține regulat cursuri post-doctorale în cadrul mai multor universități importante din UE; fiind de asemenea, profesor invitat la Universitățile din Fribourg, Geneva și Sibiu.
Laurent Chrzanovski este autor/editor a 18 cărți și a peste o sută de articole științifice. În domeniul securității, este membru al „Roster of Experts" al ITU, membru al think-tank-ului „e-Health and Data Privacy" sub egida Senatului Italian, și manager al congresului anual „Cybersecurity in Romania. A macro-regional public-private dialogue platform".

În ciuda urgenței de a face față tsunamiului de atacuri cibernetice, Europa furnizează, bineînțeles, informații, însă foarte puține agenții centralizate au creat o secțiune specială COVID pe pagina de start. De exemplu, CERT-EU (www.cert-europa.eu) continuă ca și cum nu s-ar fi întâmplat nimic, oferind toate detaliile tehnice ale atacurilor detectate și examinate. La fel și ENISA (www.enisa.europa.eu). Agenția cea mai proactivă rămâne deci celula EC3 a EUROPOL, care nu doar că a creat un grafic de bază educativ, accesibil tuturor, și o secțiune specială pe pagina sa de start (www.europol.europa.eu), dar a publicat și un raport foart *How Criminals Exploit The Covid-19* exemple utile.



Dacă analizăm diferite țări europe
Spania și alte state. La Madrid, s-a de
site-ul web al INCIBE (Instituto Nacionál de Ciberseguridad) (www.incibe.es), afișând un enorm banner pe pagina principală consacrată atacurilor în contextul COVID-19 (17). În afară de rapoarte și de un flux de informații actualizate în timp real, sunt difuzate și diferite mesaje vitale de către toate serviciile de stat – de la poliție la armată, protecție civilă și autorități fiscale – pe site-urile web ale acestora, sub forma a 30 de „pastile" ale căror grafică și claritate a mesajului sunt de admirat.

Câteva din „pastilele" spaniole © INCIBE

La capătul opus, aproape toate celelalte țări de pe continent oferă cetățenilor un veritabil labirint de site-uri care nu trimit unele la celelalte, reducând astfel vizibilitatea sfaturilor și a documentelor cuprinse în acestea, deși foarte utile și redactate cu migală. Dacă luăm exemplul Italiei, **Comisariatul poștal și al comunicațiilor** trece zilnic în revistă faptele cele mai grave (www.commissariatodips.it). Același lucru l-au făcut și site-urile CERT al Administrației publice (18), al Agenției pentru Italia digitală (19) al CertFIN (20) și al Asociației italiene a inginerilor clinici (21), prin pagini consacrate criminalității cibernetice asociate crizei COVID. Alte organisme, urmând modelul CERT-UE, preferă să trateze atacurile așa cum apar, fie că au sau nu legătură cu COVID-19 și cu specificitățile acestui mod de viață și de lucru impus tuturor europenilor.

COVID-19: un front nelimitat în lumea digitală. Atacuri fără precedent în termeni de diversitate și cantitate

Pentru uzul cititorilor noștri, am întocmit o listă a principalelor mijloace folosite de infractorii cibernetici pentru a ataca aproape toate tipurile de persoane și de entități, „urbi et orbi". Conform Bitdefender, atacurile globale din martie 2020 au înregistrat o creștere de 500% în raport cu cele din februarie, care la rândul lor aveau o rată foarte ridicată (unii specialiști vorbesc chiar de o rată de 1500% în plus față de martie 2019).

1. Dezinformare masivă în caz de panică, cu viruși la pachet

Multe state au luat măsuri extraordinare pentru a cenzura fake news. Aproape întotdeauna se lovesc de problema cunoscută de toți specialiștii în domeniu: rețelele sociale și extrateritorialitatea. Lipsa discernământului între un comunicat oficial și o știre falsă, manifestat de mulți cetățeni, continuă să evidențieze *ad eternam* problema – în continuare nerezolvată – unei gestionări eficiente a sensibilizării preventive oferite tuturor pentru a recunoaște fake news.

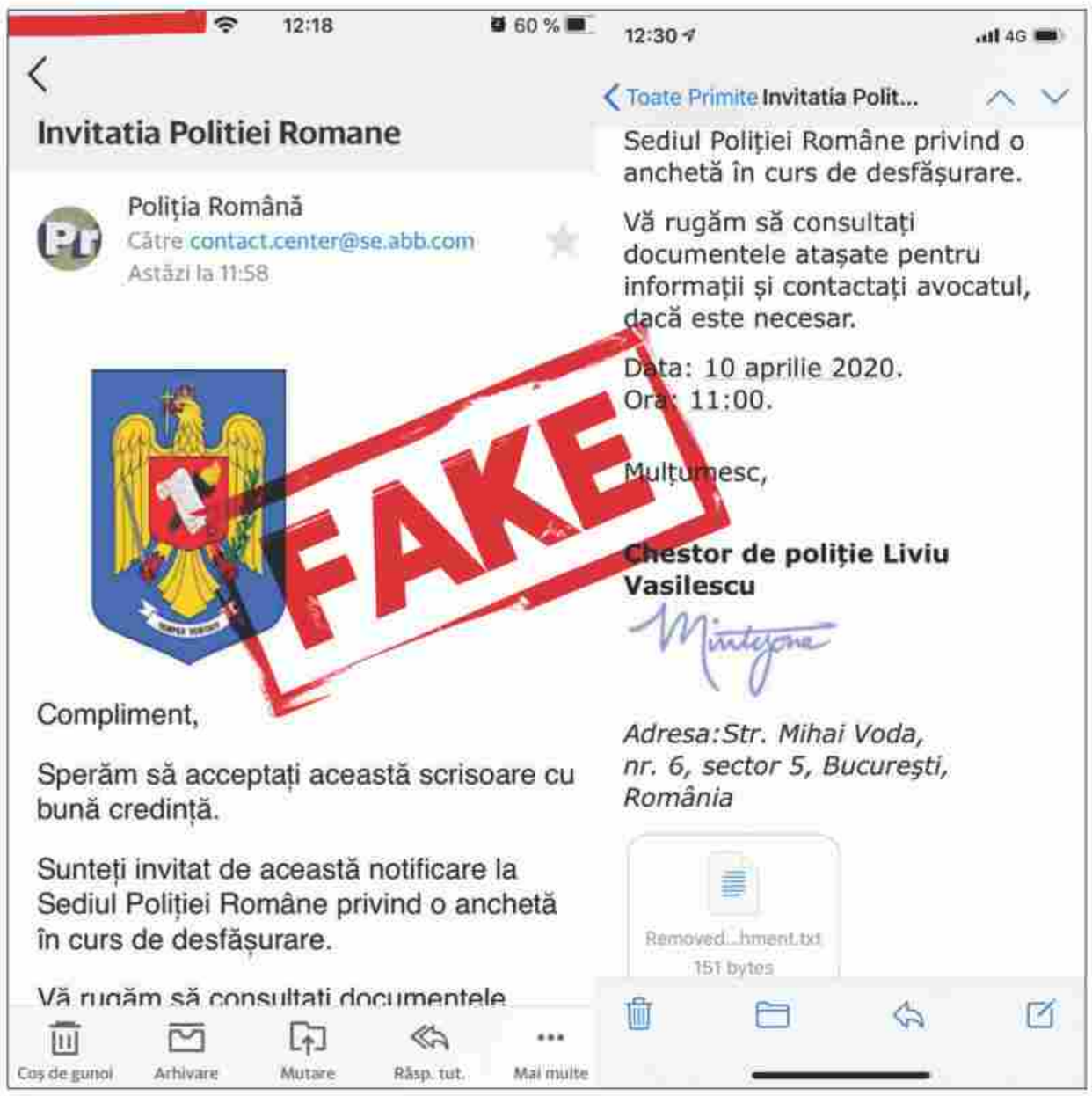
Exemplu oferit de DCCO:

În ultima perioadă a fost înregistrată și o creștere a atacurilor de tip phishing. O campanie recentă, a impersonat o invitație primită din partea Inspectorului General al Poliției Române. Mesajul conținea un atașament malițios, care în urma analizei s-a dovedit că face parte din familia de viruși informatici NanoCore. Acest virus este de tipul *Remote Access Trojan* ce oferă posibilitatea atacatorilor să preia controlul sistemelor infectate.

Mesajul pare a fi o traducere Google aproximativă, de aceea este posibil ca astfel de cazuri să fie întâlnite și în alte state.

În cazul în care primiți astfel de mesaje e-mail este foarte important să nu le deschideți și de asemenea să nu accesați atașamentele sau linkurile conținute. https://www.facebook.com/561241820653723/posts/2763628483748368/

Aproape peste tot se găsesc exemple de false documente oficiale, cum ar fi scrisorile ministeriale precum cea a ministerului educației italian, devenită virală pe rețelele sociale și denunțată de ministrul Lucia Azzolina ca fiind falsificată (22).



▸▸Învățați să vă informați în mod corect!

Odată cu urgența COVID, proiectul proactiv *News Litteracy* a lansat pentru publicul anglofon, una din cele mai bune inițiative posibile: o aplicație pedagogică directă, intitulată aproape ironic *Are you informable?* (lit. Sunteți capabili încă să fiți informați?) (https://newslit.org/coronavirus/.)

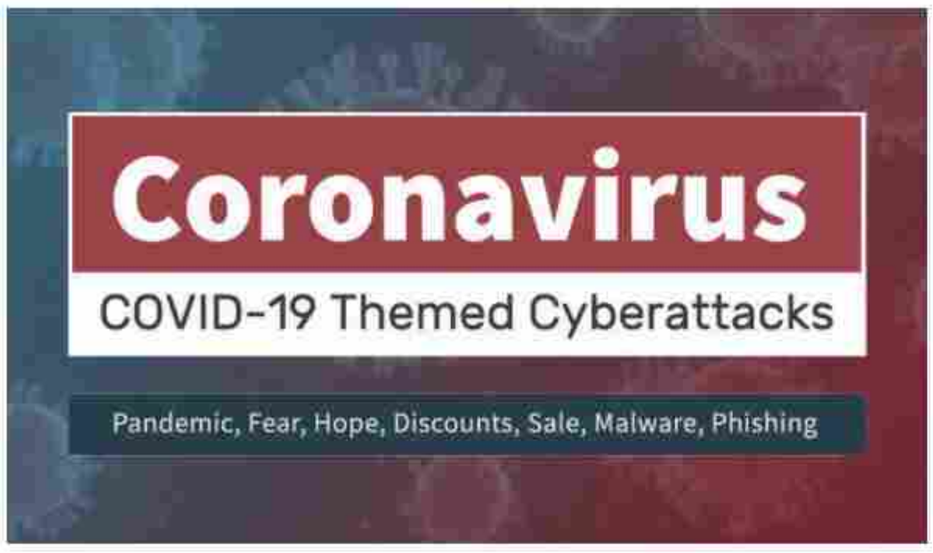
Aplicația care încurajează temperarea stării de panică și revenirea la surse fiabile de informații © News Litteracy Project

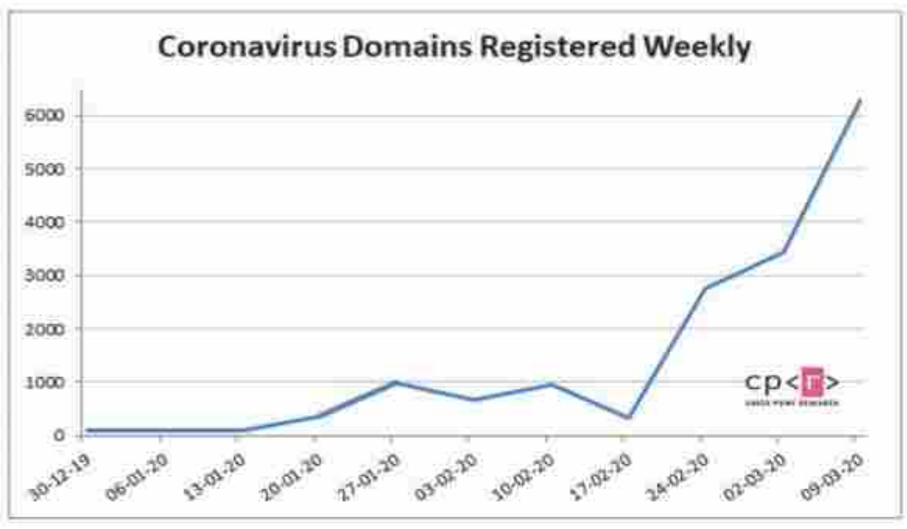
Un element în plin avânt îl reprezintă tocmai folosirea acestor fake news pentru ascunderea de software-uri de tip malware foarte puternice, așa cum a arătat-o un raport al lui Adam Pilkey publicat de societatea F-Secure (a se vedea nota bibliografică 13), ilustrat magistral și reprodus parțial aici. Așa cum putem observa în articol, autorul conferă forță aserțiunilor sale prin exemple, iar malware-uri conexe provenind din nu mai puțin de 12 țări, din Asia, Europa și Statele Unite sunt privite ca exemple. O altă preocupare majoră o reprezintă numărul de domenii care fac referire la numele oficial sau popular al virusului, toate cu potențial de a fi deținute de infractori, așa cum o subliniază raportul lui Lakshmanan (a se vedea nota bibliografică 14).

Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks

2

1. O parte a ilustrației lui Pilkey.
2. Titluri de publicații specializate © Cyberhub și Montalbano, Threatpost (a se vedea nota bibliografică 12)





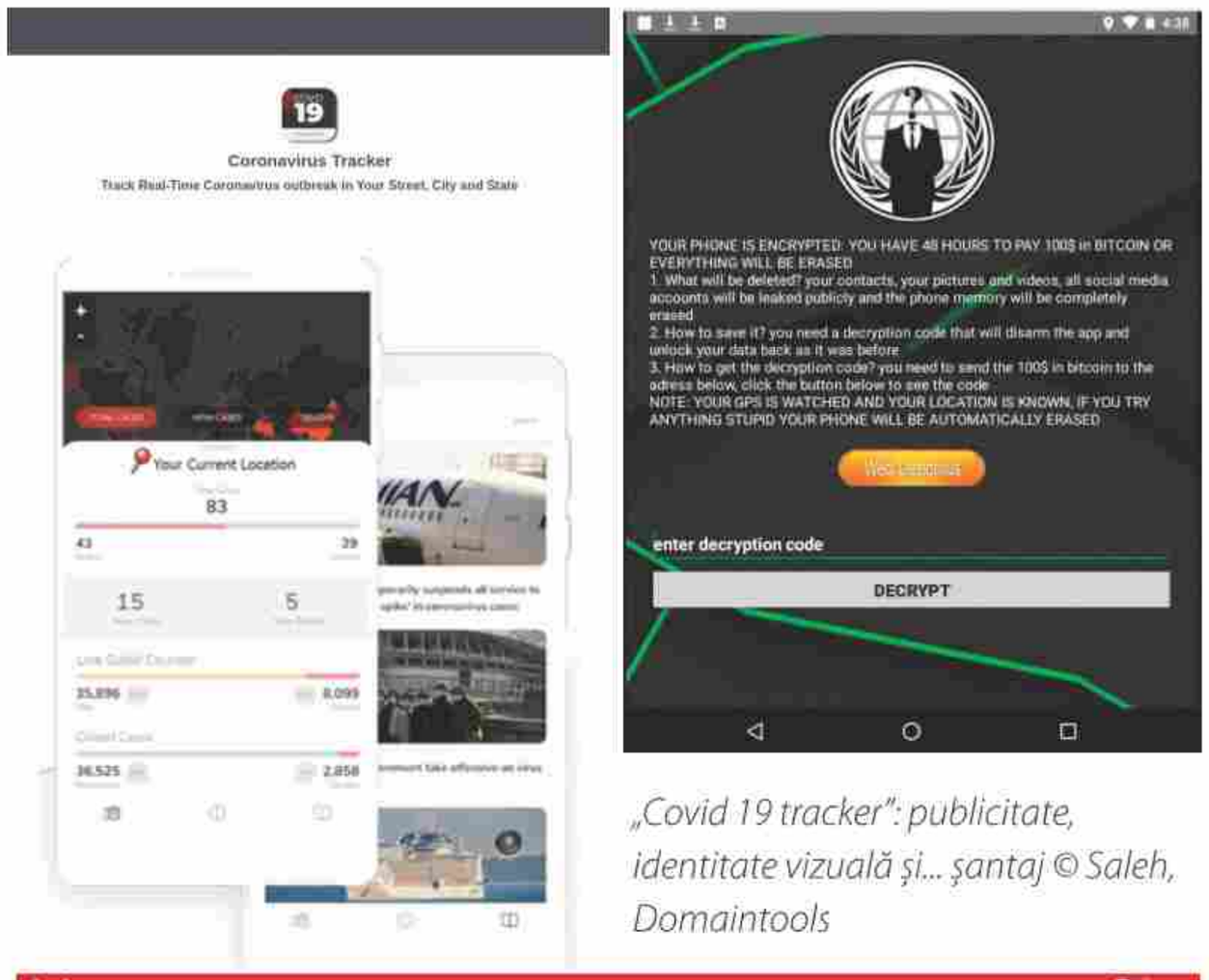
Un număr mare de site-uri legate de numele „Coronavirus" cumpărate de infractori în ultimele săptămâni © Checkpoint, a se vedea Lakshmanan (nota bibliografică 14).

2. Căutare disperată a informațiilor pentru dispozitive mobile: aplicații ilicite consacrate COVID-19

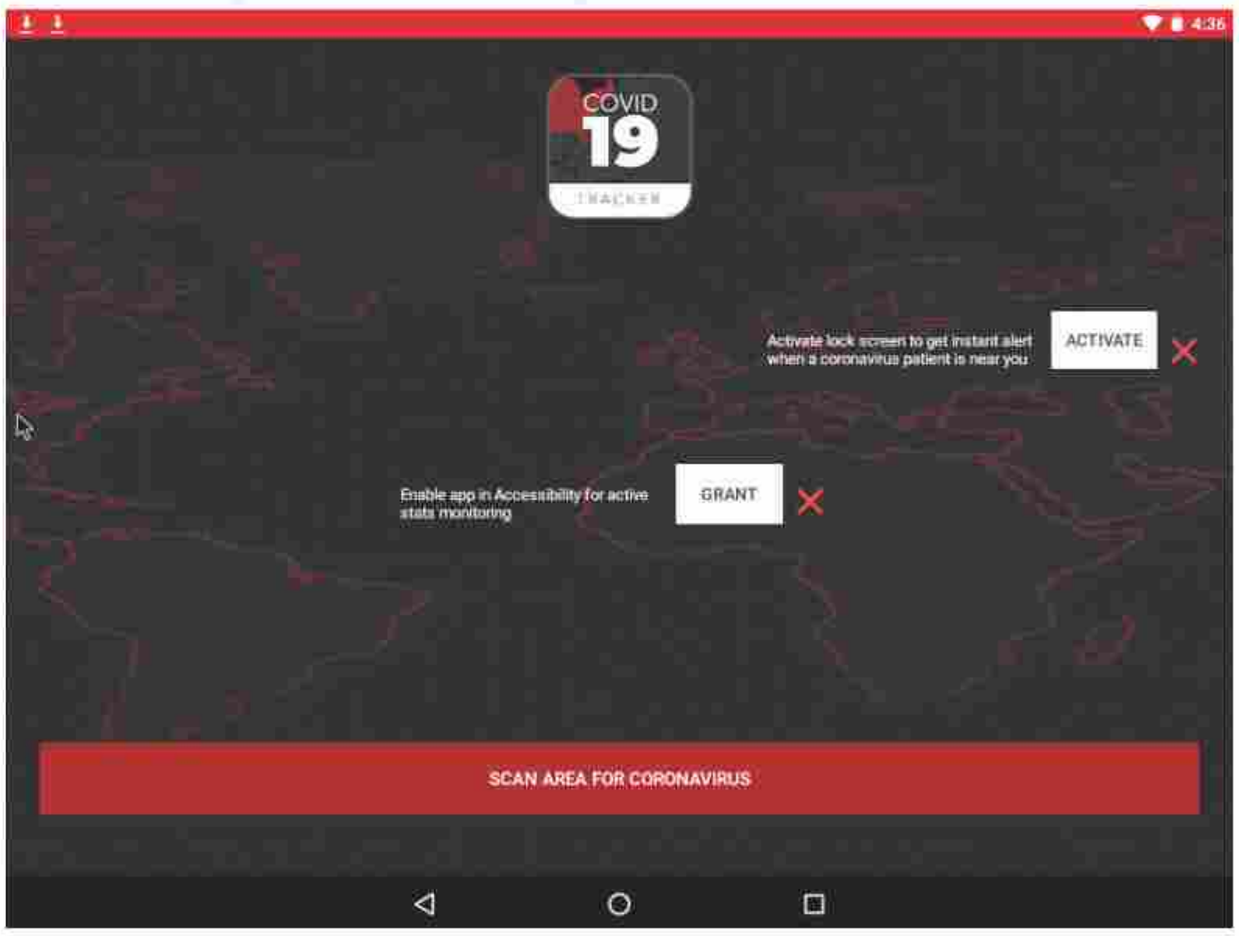
La numărul mare de știri false trimise prin e-mail, escrocherii sau link-uri răuvoitoare postate pe rețele sociale se adaugă zecile de aplicații false create în fiecare săptămână pentru a „informa" utilizatorul asupra situației mondiale, naționale sau pentru furnizarea de „informații utile".

Aproape toate destinate smartphone-urilor cu sistem de operare Android, acestea dau de lucru tuturor specialiștilor în securitate. Chiar dacă sunt refuzate de diferite „store-uri" native ale producătorilor de smartphone-uri, ele sunt descărcate direct de pe Internet de către utilizatori. lar dacă majoritatea acestor app-uri copiază doar părți mai mult sau mai puțin importante din conținutul smartphone-ului victimei, unele dintre ele preiau realmente controlul microfonului și camerei video/foto ale smartphone-ului.

Momentan, cea mai perfidă dintre aplicații este fără îndoială „Covid 19 Tracker", descoperită pe 10 martie, fiindcă este nu doar un spyware foarte puternic, ci și un ransomware. La câteva ore de la activare, blochează smartphone-ul cu un crypto-ransomware și solicită 100 de dolari în bitcoin pentru deblocare, după cum explică Tarik Saleh (23).

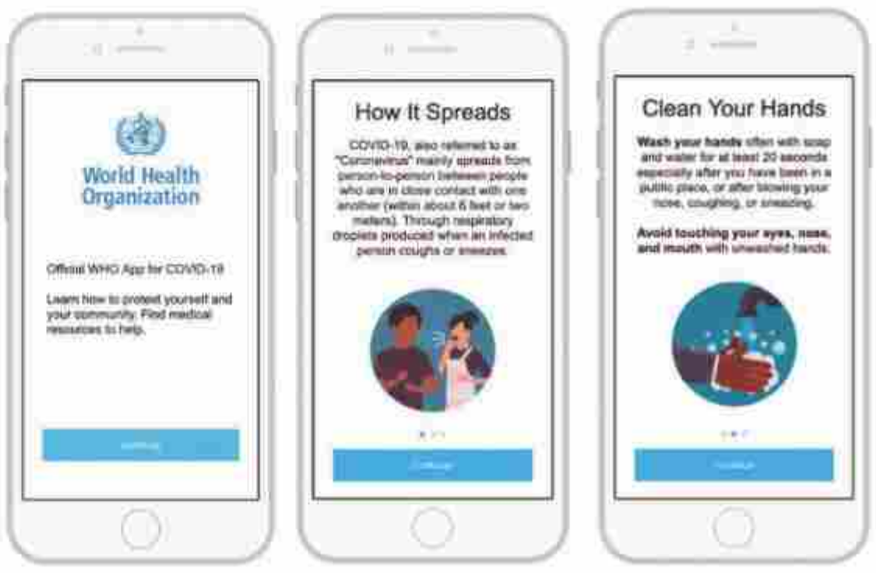


„Covid 19 tracker": publicitate, identitate vizuală și... șantaj © Saleh, Domaintools



▸▸Descărcați aplicațiile autentificate de state, evitați utilizarea aplicațiilor GAFAM

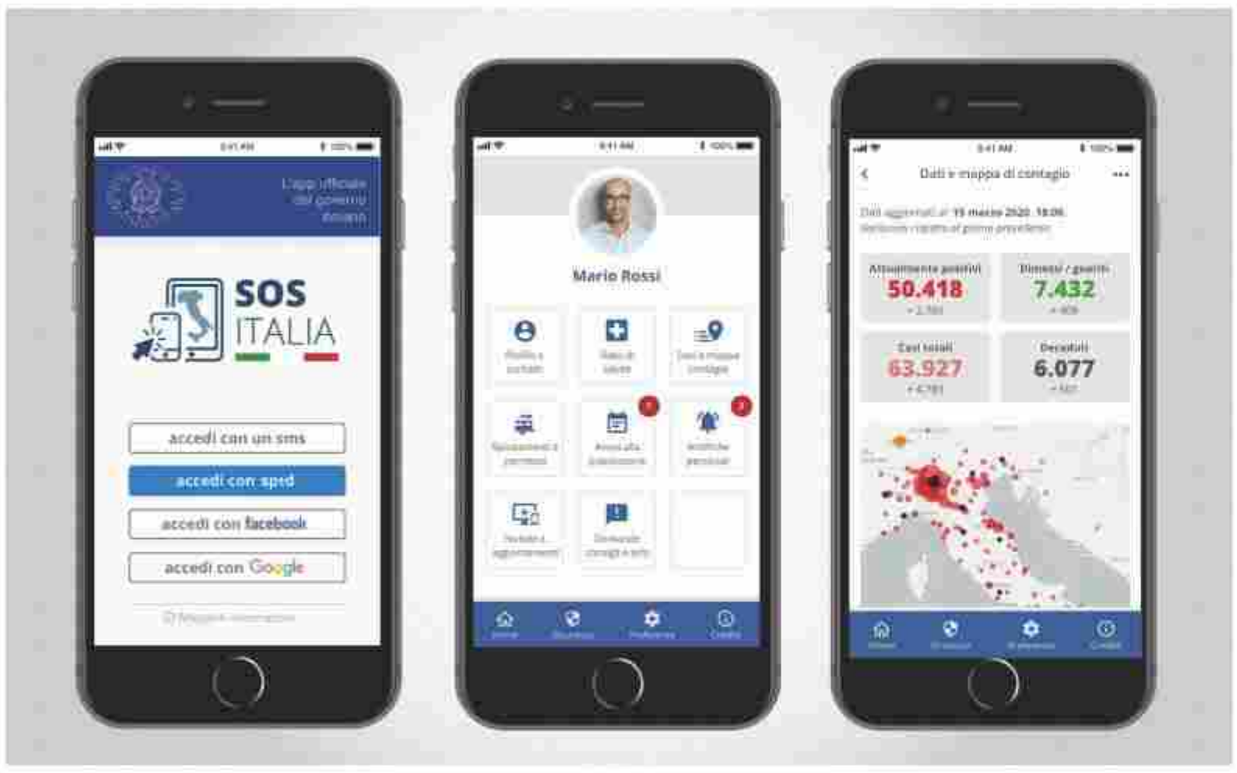
Confruntată cu cantitatea enormă de aplicații dedicate virusului, Organizația Mondială a Sănătății va lansa, la începutul lui aprilie, propria sa aplicație gratuită, disponibilă în toate limbile, intitulată „WHO MyHealth" (24).



Interfața aplicației MyHealth a OMS, conform prototipului transmis presei © New York Post

Între timp, în Italia, două inițiative sunt pregătite. Prima aplicație, pentru diseminarea informațiilor sanitare și științifice, are scopul de a încuraja, de a furniza sfaturi, de a facilita autodiagnosticarea de la primele simptome ale virusului și de a urmări contagiunea. Este rezultatul muncii unui grup științific de elită, iar acum așteaptă validarea finală la ministerul sănătății (25).

Cea de-a doua, care vizează colaborarea cetățenilor în gestiunea crizei și facilitează întocmirea formularelor de deplasare în afara domiciliului, este dezvoltată de Asociația italiană pentru revoluția digitală în parteneriat cu SOS Italia în cadrul unui proiect guvernamental „Innova per l'Italia" (26) și are ca prim obiectiv simplificarea gestionării pandemiilor, grație unui sistem care integrează un instrument de autodiagnosticare, un rezumat al ultimelor știri și comunicări oficiale, o hartă a contagiunii și un sistem de gestiune al auto-certificării bazat pe coduri QR care simplifică munca serviciilor de ordine (27).



Prototipul de interfață pentru aplicația „SOS Italia" © La Stampa

Aplicațiile GAFAM, aceeași extrateritorialitate, aceleași practici: datele voastre devin proprietatea lor, *ad eternam*. Astfel, în acest domeniu, suntem datori să vă încurajăm să fiți prudenți înainte de a lua decizia de a descărca și folosi una din aplicațiile oficiale GAFAM sau ale societăților pe care le dețin.

Valabil și pentru majoritatea aplicațiilor plătite apărute în această piață nouă. Verificați obligatoriu ce fel de parametri și ce informații din smartphone-ul vostru vor fi automat accesibile acestor app-uri „pentru o funcționare optimă" înainte de a le descărca!

Ca în cazul oricărei rețele sociale, acceptați printr-un click un contract foarte lung care explică cum toate datele voastre **pot/vor fi înregistrate (fără limită de timp) „pentru îmbunătățirea produselor noastre",** cum putem citi, de exemplu, în *politica de confidențialitate* a aplicației „COVID-19 Screening Tool" a Apple (https://www.apple.com/legal/privacy/en-ww/).

3. O inimă de aur? Nu lăsați infractorii să profite de generozitatea voastră!

Pe paginile web și pe conturile de rețele sociale ale tuturor unităților de poliție din Europa, nu trece o zi fără postarea vreunui anunț urgent privind false campanii de strângeri de fonduri; în cazul Italiei, anunțurile se găsesc pe pagina Poliției comunicațiilor (28).

Exemplu oferit de DCCO:

În urma instituirii situației de urgență la nivel național, precum și în conformitate cu prevederile ordonanțelor militare emise de către Ministerul Afacerilor Interne, cetățenii români au obligația de a completa o declarație pe proprie răspundere atunci când se află în spațiul public.

Imediat după intrarea în vigoare a acestei prevederi, în spațiul on-line au apărut diferite site-uri web ce ofereau posibilitatea utilizatorilor de a-și genera o declarație, prin introducerea datelor personale în câmpuri prestabilite. Multe dintre aceste soluții web colectau datele personale ale utilizatorilor nefiind în concordanță cu prevederile legislative privind protecția datelor cu caracter personal.

De aceea, Poliția Română, împreună cu alte instituții naționale partenere, au făcut demersuri pentru verificarea acestor site-uri și de asemenea, a informat populația cu privire la pericolele folosirii unor astfel de soluții. De asemenea, a încurajat cetățenii să folosească doar surse oficiale.

https://cert.ro/citeste/comunicat-declaratie-pe-proprie-raspundere-surse-oficiale

Cea mai gravă dintre aceste campanii a vizat chiar agenția mondială responsabilă cu gestionarea crizei, Organizația Mondială a Sănătății (OMS). Milioane de e-mailuri de phishing au fost trimise, în aproape toate limbile din lume, solicitând donații și copiind logo-uri și părți din descrierile „Fondului de răspuns

Răspândirea COVID-19 și atacurile cibernetice: o dublă amenințare pentru societate

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

Autor: Arthur Mattli, Ambasador al Confederației Elvețiene în România

Răspândirea Covid-19 și răspândirea actuală a atacurilor cibernetice au multe lucruri în comun: ambele se împrăștie în mod invizibil și cu viteză foarte mare, perturbă viețile a milioane de oameni într-un mod înspăimântător, au un impact economic global îngrijorător și acționează într-o simbioză cumplită. Majoritatea măsurilor de izolare impuse de guverne au antrenat o perturbare însemnată a comportamentului uman. În timp ce pare că lanțurile de aprovizionare cu produse alimentare și companiile de transport o duc bine, asistăm la o mutație profundă a industriilor de servicii spre locuri de muncă la distanță, școli care-și mută temporar lecțiile online și servicii online confruntate cu o explozie a cererii.

Din fericire, lumea digitală în care trăim ne oferă, în această perioadă dificilă fără precedent, nenumărate posibilități pentru a ne continua relațiile comerciale, pentru a ne menține contactele sociale și chiar pentru a îmbunătăți calitatea vieții. Însă efectele neprevăzute din minunata lume nouă digitală asupra securității indivizilor și statelor din toată lumea sunt foarte reale: în mod ironic, constrângerile impuse pentru protejarea milioanelor de persoane împotriva Covid-19 expun în același timp un număr record de utilizatori la atacuri cibernetice. Deși oamenii au învățat, prin toate mijloacele de informare, importanța spălării mâinilor și a feței și a dezinfectării clanțelor de la uși, au fost puse la dispoziția lor foarte puține instrumente de educație și prevenție pentru a-i ajuta să-și protejeze calculatoarele și rețelele împotriva atacurilor cibernetice. Aceste atacuri sunt însoțite cu precădere de fake news. În 28 martie, Secretarul General al ONU a lansat un avertisment grav în ceea ce privește infectarea spațiului virtual cu fake news despre virus.

În contextul Covid-19, criminalitatea cibernetică organizată s-a înmulțit cu o viteză și o amploare fără precedent. Sunt în derulare campanii de fraudă la scară mare, în special publicitate falsă pentru produse medicale de care este nevoie urgent. Infractorii cibernetici exploatează fără încetare și fără milă faptul că milioane de utilizatori își fac publice informațiile și comportamentele digitale, în această perioadă zbuciumată. Ca niște prădători, aceștia atrag persoane necunoscătoare, novici, exploatează breșe și întind capcane.

Ediția de față a Cybersecurity Trends își propune să suplinească lipsa de informații în circumstanțele actuale legate de securitatea cibernetică și să contribuie la o mai bună înțelegere a riscurilor actuale și a amenințărilor imediate din lumea digitală, în contextul Covid-19 și nu numai.

Le mulțumesc lui Laurent Chrzanovski, echipei sale de redacție, tuturor autorilor textelor din publicația de față, pentru clarviziunea în alegerea tematicii și pentru contribuția pe care au avut-o în întreținerea unei discuții și a unei coordonări internaționale indispensabile. ■

Disclaimer: Întreaga responsabilitate pentru opiniile și observațiile exprimate mai sus aparține autorului lor și nu reprezintă neapărat poziția oficială a Confederației Elvețiene.

de solidaritate COVID-19", cu numere false de conturi bancare, adesea dublate de solicitări de date personale, uneori acompaniate chiar – cireașa de pe tort – și de fișiere atașate care conțineau malware. Reacția oficială a organismului Națiunilor Unite explică bine gravitatea acestui incident (29):

World Health Organization

Feriți-vă de infractorii care pretind că réprezintă OMS

Infractorii pretind că reprezintă OMS pentru a fura bani sau informații sensibile. Dacă sunteți contactat de o persoană sau o organizație care pare a fi de la OMS, verificați autenticitatea acesteia înainte de a răspunde.

Organizația Mondială a Sănătății:

- nu vă va solicita niciodată numele de utilizator sau parola pentru a obține informații legate de securitate
- nu va trimite niciodată fișiere atașate nesolicitate
- nu vă va solicita să accesați un link extern www.who.int
- nu vă va solicita bani pentru aplicarea pentru un post, înscrierea la o conferință sau rezervarea unui hotel
- nu va organiza niciodată loterii și nu va oferi premii, subvenții, certificate sau finanțări prin e-mail

Singura campanie de strângere de fonduri lansată de OMS constă în Fondul de răspuns de solidaritate COVID-19, iar link-ul îl găsiți mai jos. Orice alt apel de fonduri sau donații care pare lansat de OMS este o escrocherie.

▸▸Folosiți doar informații furnizate de site-uri web oficiale

Singurul sfat, valabil în această perioadă mai mult ca niciodată, este de a nu da curs propunerilor de cadouri primite prin poșta electronică. După ce ați ales organizația sau ONG-ul pentru care doriți să contribuiți în numerar, trebuie să verificați pe site-ul web oficial al organizației alese care sunt modalitățile de plată, condițiile exacte și datele bancare corecte ale beneficiarului.

4. Vă este teamă? Atenție la medicamente, măști și alte produse sanitare disponibile online

Toate site-urile de „anunțuri" sunt inundate de publicitate care îndeamnă la cumpărarea de „antivirale" miraculoase, măști de protecție și o panoplie de metode pentru „prevenirea infectării".

O mare parte din escrocherii – dintre care unele însoțite de viruși puternici (30) – primite prin poșta electronică profită de teama oamenilor și de dorința lor de a se proteja: ele țintesc veriga cea mai slabă a rațiunii pe care cu toții avem tendința să o pierdem atunci când este în joc viața noastră sau a celor apropiați.

ESTE IMPORTANT DE SUBLINIAT CĂ, ÎN ACEST MOMENT, NU EXISTĂ NICI VACCIN ȘI NICI REMEDIU RECUNOSCUT UNIVERSAL PENTRU LUPTA ÎMPOTRIVA COVID-19

Tratamentele – **administrate exclusiv la spital** – care au contribuit la vindecarea multor pacienți care nu sufereau de antecedente medicale grave sunt diferite de la o țară la alta și adesea de la un spital la altul. Este important de știut că anumite produse ridicate în slăvi de către presă, precum *clorochina*, nu sunt altceva decât compuși parțiali ale unor „cocktailuri farmaceutice" dezvoltate de spitale. Ca atare, nu trebuie folosite în automedicație, achiziționarea lor este ilegală iar utilizarea lor fără supraveghere medicale a cauzat deja numeroase decese în Statele Unite.

Achiziționarea acestora online, de pe site-ul care-și ascund localizarea geografică reală, este foarte periculoasă. Cel mai mic rău care se poate întâmpla, ca în cazul falselor polițe de asigurare care propuneau acoperire pentru COVID-19 (31), este că nu veți primi niciodată nimic după efectuarea plății.

În cel mai rău caz, comanda achitată va fi livrată, iar în ea veți regăsi cutii și mai ales medicamente contrafăcute, care pot fi doar pastă cu făină, sau un amestec de substanțe care vă pot trimite direct în spital, așa cum o ilustrează mai jos o pagină de benzi desenate a *Grupului elvețian pentru prevenirea criminalității* (32).

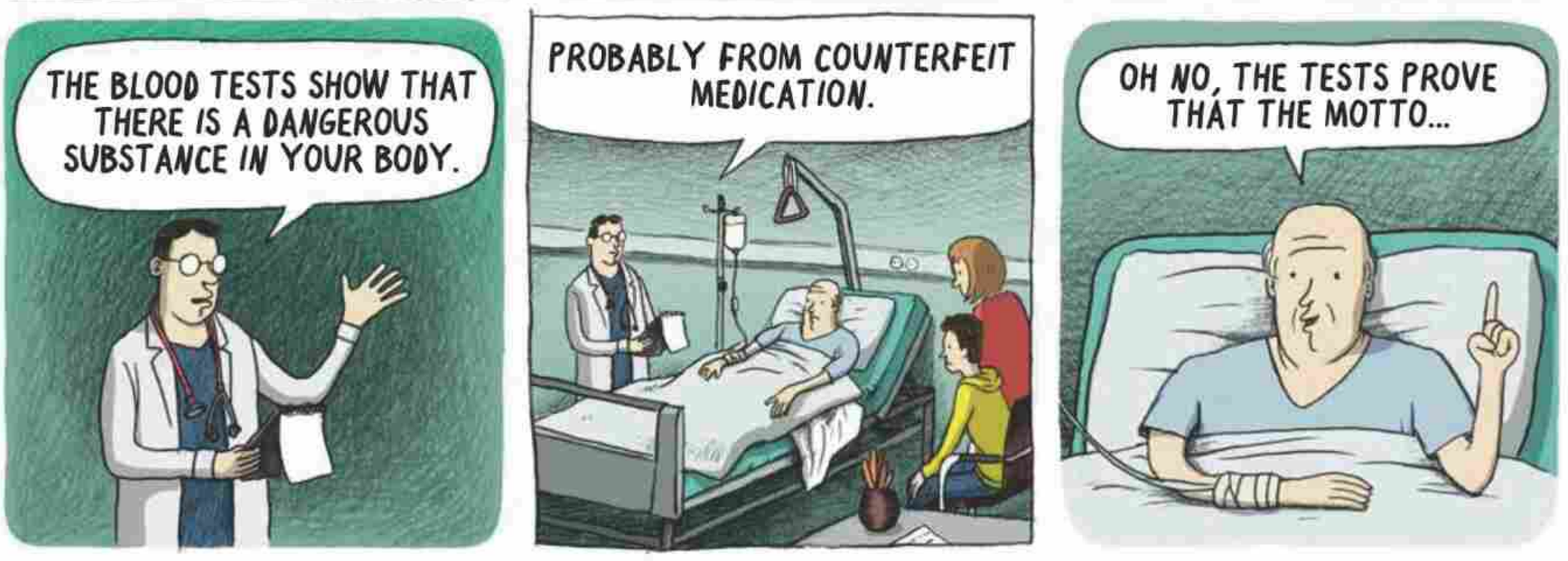
▸▸Folosiți doar site-urile web oficiale ale farmaciilor sau magazinelor online pe care le cunoașteți deja.

Pentru a respecta dispozițiile emise de autoritățile naționale, nu cumpărați medicamente produse în alte țări, nici chiar din Uniunea Europeană. Cerințele de prescripție pentru fiecare medicament în parte sunt foarte diferite de la un stat la altul, la fel și dozele.

Același lucru se aplică și achiziționării de măști de protecție, de dezinfectanți medicali sau de alte produse sanitare. Cea mai bună soluție este să vă prezentați la farmacia locală și să comandați de acolo tot ce aveți nevoie.

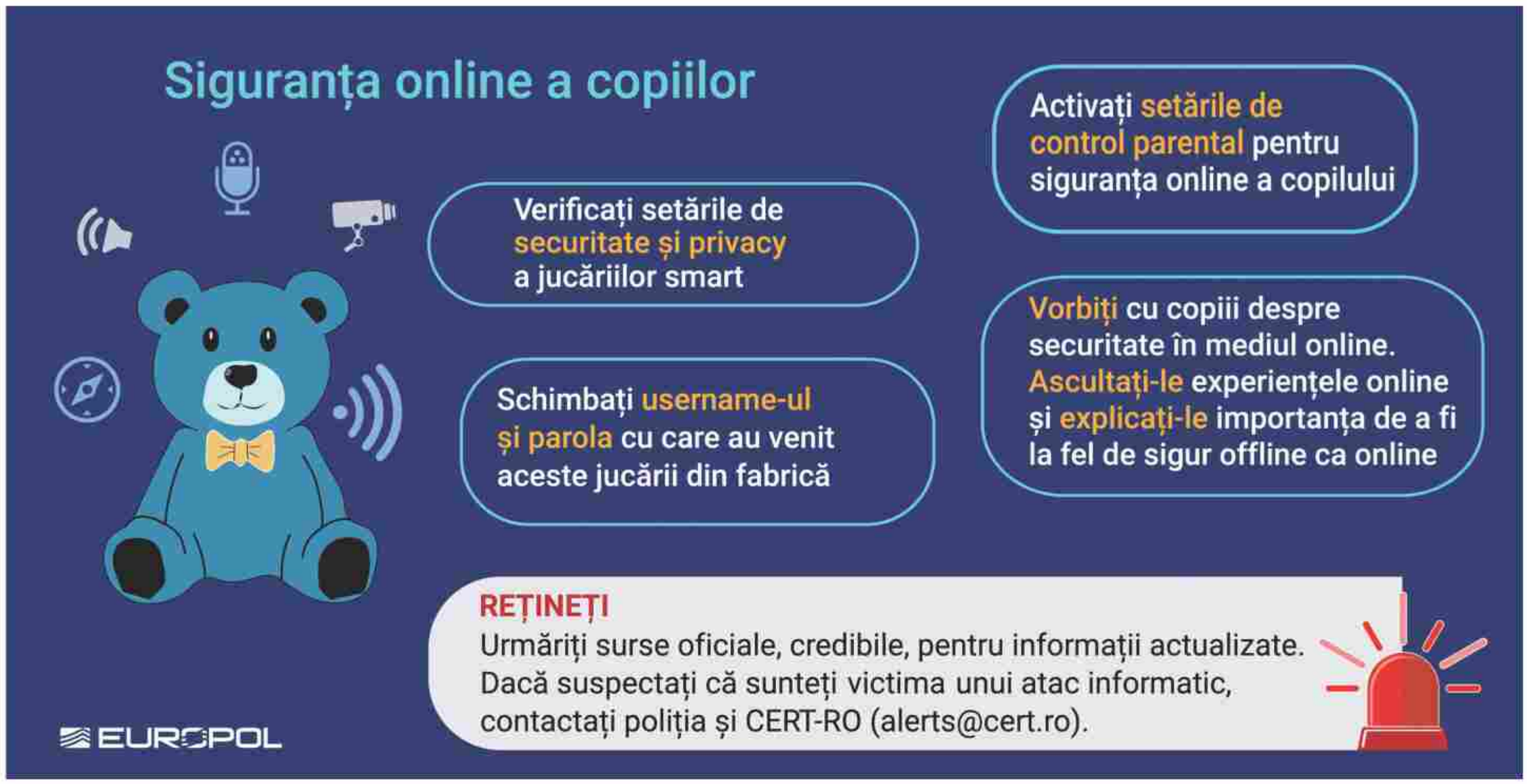
Atenție maximă la mesaje de tip „antivirus care" care se referă la site-ul antivirus-Covid (domenii diferite): odată deschisă pagina web, se declanșează pe calculatorul vostru un malware foarte puternic numit BlackNet (33). Dacă calculatorul e infectat, contactați imediat poliția.

NO RISK NO FUN



TIP:

NOBODY KNOWS EXACTLY WHAT IS IN MEDICINES SOLD ON THE INTERNET. THE PRICE AND EASY ACCESSIBILITY GET IN THE WAY OF COMMON SENSE. THERE IS LITTLE THOUGHT OF THE (POSSIBLY FATAL) WORST CASE SCENARIO WHEN CLICKING THE "BUY NOW" BUTTON. SO KEEP YOUR HANDS AND MOUTH AWAY FROM ANY MEDICINES FROM UNLICENSED SOURCES! AND THIS GOES FOR EVERYONE - NOT JUST GRANDPA.



5. Izolați la domiciliu? Aveți grijă de copii!

Minorilor trebuie să li se acorde o atenție specială. Școlile fiind închise, infractorii cibernetici creează jocuri noi care foarte adesea ascund malware; de asemenea, asistăm la un val de cereri de prietenii pe rețelele sociale (cu scopul de a stabili relații de încredere, pedofilie etc.), semnalate de majoritatea unităților de poliție (34).

Cumpărați exclusiv jocuri originale oferite de diferite „app store-uri" ale producătorilor de smartphone-uri și de magazine autorizate să vândă licențe de jocuri PC/Xbox online.

O gamă largă de măsuri de urmat, ținând cont de vârsta minorilor, a fost întocmită de parteneriatul public-privat englez Getsafeonline, prin tutoriale realizate sub forma unor scurte clipuri video ușor de înțeles și adaptate situației actuale:„Asigurarea securității online a copiilor în timpul epidemiei de coronavirus" (35)

6. Izolați la domiciliu? Aveți grijă la sursele de distracție și la shopping!

Asistăm la un atac generalizat împotriva platformelor de streaming video și de jocuri gratuite – un „zero-day" foarte puternic a întrerupt chiar și serviciul GooglePlay timp de o oră – și asistăm de asemenea la o întețire a escrocheriilor care redirecționează utilizatorii către site-uri ilicite care oferă luni întregi de filme și de jocuri gratuite, însă... solicită datele cardului bancar pentru înregistrare.

Cele mai periculoase arme împotriva celor mai vulnerabili dintre noi sunt tonele de e-mailuri de phishing cu oferte comerciale false de toate tipurile, al căror număr crește în mod exponențial zi de zi. Deși sunt mai ușor de recunoscut pentru că sunt în general pline de greșeli – în cazul limbilor care nu sunt de circulație internațională – sau de fraze generice, unele sunt totuși destul de bine realizate. Precauția utilizatorului este uneori pusă la grea încercare, ca de exemplu în cazul petrecut în România și raportat de CERT-RO (36). Chiar dacă conținutul e plin de greșeli, ergonomia e-mailului, poziționarea logourilor aparținând unui mare lanț de supermarketuri germane și, mai ales, numele site-ului-capcană au fost foarte bine studiate: adresa este cea a multinaționalei (Kaufland.com), la care se adaugă totuși „-bon" (voucher) și, mai ales, elementul care indică falsul: domeniul final al site-ului (.club).

Website capcană © CERT-RO

Sfaturi pentru cumpărături online sigure

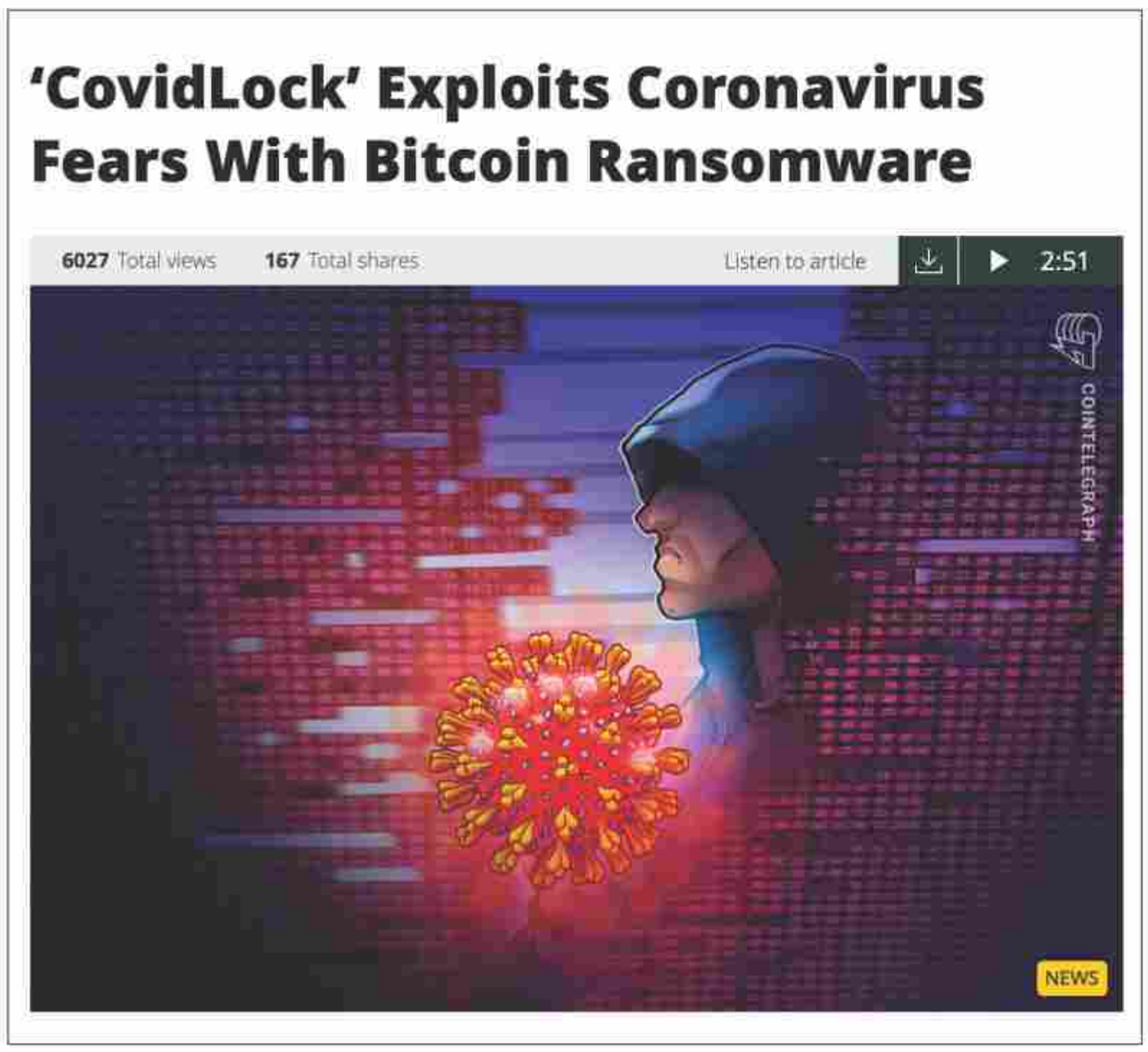
- Cumpără exclusiv de la magazine cunoscute și citește recenziile
- Este mai sigur să folosești cartea de credit pentru cumpărături online
- Nu te grăbi să accepți orice ofertă! Dacă promoția sună prea bine pentru a fi reală, probabil este o încercare de fraudă
- Verifică frecvent tranzacțiile din cont pentru orice activitate suspicioasă

▸▸Nu cumpărați nimic din ce vi se oferă pe e-mail, prin accesarea unui link integrat

Cunoașteți fără îndoială site-urile magazinelor de la care ați cumpărat sau la care v-ați creat un cont. Ca măsură de precauție, nu accesați ofertele acestor magazine online, chiar dacă sunt veridice. Le puteți accesa în momentul în care intrați pe site-ul oficial al acestora.

7. Izolați la domiciliu? Feriți-vă de orice ofertă bancară sau financiară!

În aproape toate statele europene, există o rată imensă de phishing/ înșelătorii în domeniul financiar. Apar oferte incredibile precum credite mari cu dobândă zero, amânări de plată a ipotecilor, rambursarea unor sume mari din cheltuielile efectuate, cu condiția utilizării „acestui nou instrument" etc., iar poliția comunicațiilor italiană a rezumat acest fenomen foarte bine (37).



Graficul din articolul lui Haig © Cointelegraph

▸▸Nu acceptați nimic din ce vi se oferă pe e-mail, prin accesarea unui link integrat

Supravegheați-vă totodată și ***conturile bancare***. Verificați frecvent soldul contului, folosind online banking-ul. Pentru proprietarii de **Bitcoin**, nu efectuați decât tranzacții absolut necesare: un ransomware foarte puternic și complex, conceput special pentru tranzacțiile în Bitcoin, face ravagii în momentul de față.

8. Lucrați de acasă? Aveți grijă la obiectele conectate!

Multe companii nu erau pregătite ca majoritatea angajaților să lucreze de acasă. Protocoalele de videoconferință, accesul la date, dar și reziliența sistemelor de interacțiune între telefonul mobil, laptopul angajatului și infrastructura informatică centrală a companiei (și a cloud-ului acesteia) sunt asediate. Este de ajuns să amintim rezultatul obținut de piratii informatici care au descoperit o breșă în VPN-urile solide ale iPhone-urilor, pe care în prezent Apple a reușit să o soluționeze.

În plus, în „vechea Europă", rețelele fixe – cu excepția zonelor cu fibră optică – sunt pe cale să se prăbușească din cauza supra-solicitării, în multe dintre regiuni, în timp ce viteza reală disponibilă a rețelelor mobile variază de la o poziție la alta, chiar în aceeași arie geografică.

Acest fenomen reprezintă paradisul pe care infractorii cibernetici îl așteptau de mult timp, nu doar pentru a satura și mai mult rețelele, dar și pentru prilejul de a introduce malware și „zero days" de toate soiurile, și chiar escrocherii sau false apeluri telefonice de la persoane care pretind că sunt membri în conducerea companiei pentru care lucrează un anumit angajat sau reprezentanți ai altor companii/clienți/furnizori.

▸▸ Asigurați-vă că beneficiați de cea mai bună protecție

a) Instalați și actualizați antivirusurile/metodele de protecție și actualizați în mod regulat sistemele de exploatare ale echipamentelor pe care le dețineți.

b) Acoperiți camera sau camerele video și microfoanele laptopurilor și ale telefoanelor mobile după ce ați ieșit din teleconferința profesională: multe sisteme și protocoale de teleconferință au fost piratate, companiile au reacționat prin publicarea de patch-uri (care adesea nu au fost instalate de către IMM-uri), iar patch-urile au fost la rândul lor piratate.

c) Sfaturi pentru smartphone-uri, tablete și PC-uri: în acest moment, cele mai pertinente sfaturi pentru punerea în siguranță a „biroului de acasă" pot fi găsite, în italiană, pe site-ul CertFin (a se vedea nota bibliografică 20) iar, pentru telefoane mobile și tablete, pe pagina serviciilor de informații germane (39). Sfat: descărcați documentele și introduceți textele pe www.deepl.com, cel mai bun instrument de traduceri online existent în prezent, pentru limbile de circulație internațională.

Liniile directoare (în pdf) ale Centrului canadian pentru securitate cibernetică (40) și cele ale ICAEW (Institutul de contabili autorizați din Anglia și Țara Galilor) (41) sunt foarte folositoare pentru păstrarea unei igiene digitale complete, cu precădere pentru profesiile liberale, dar și pentru simplii angajați.

Pentru verificarea eficienței sistemului VPN în cazul companiilor, e bine de consultat raportul excelent al Department of Homeland Security, care detaliază deopotrivă amenințările și soluțiile (42), precum și toate recomandările Staysafeonline, la categoria „Companii" (a se vedea nota bibliografică 10).

9. Medic, specialist medical, director de spital? Sunteți ținta cea mai vizată!

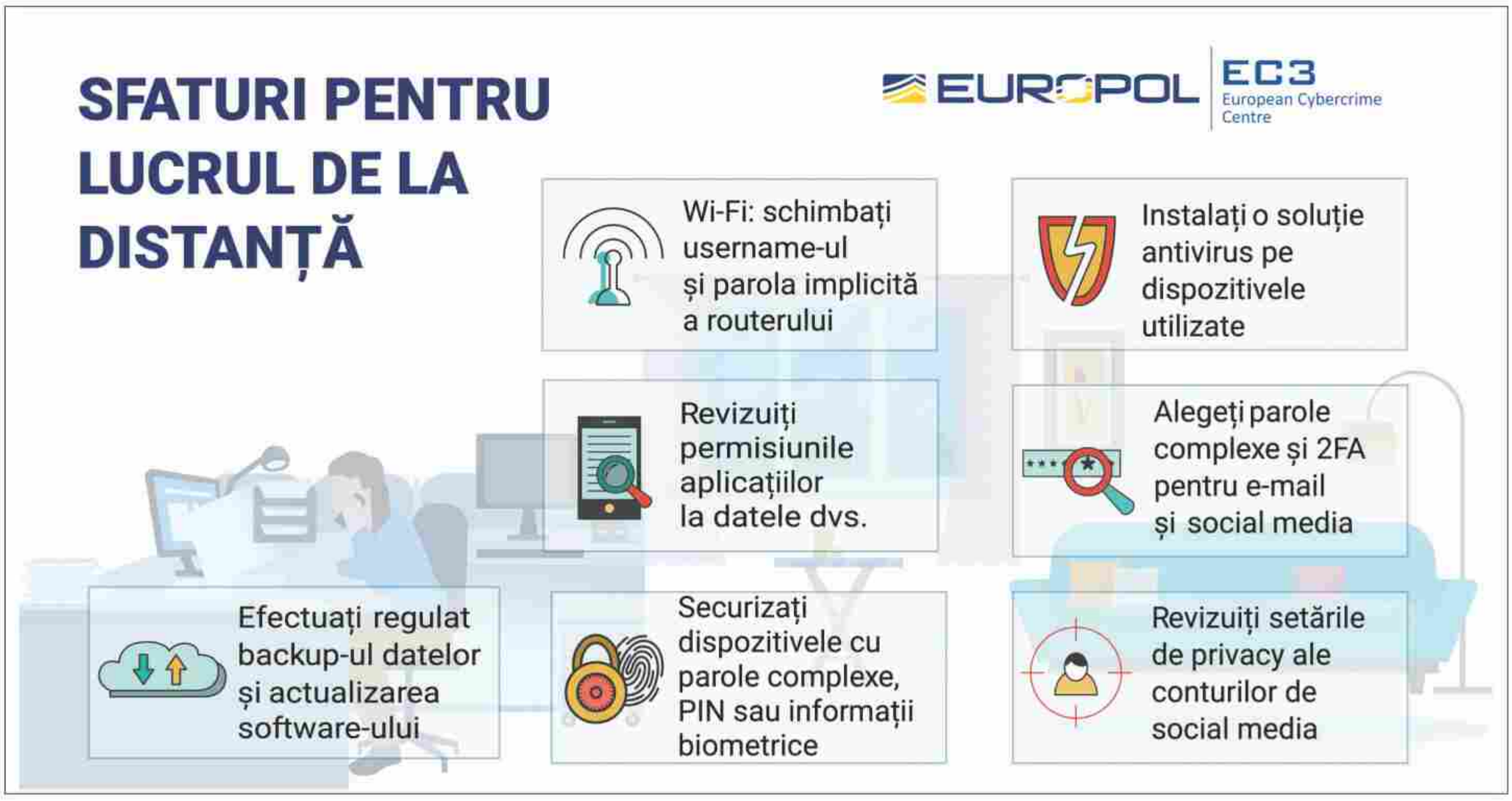
Nici nu are rost să intrăm în detaliile nenumăratelor atacuri care au vizat unitățile sanitare și medicii, în special instrumentele de telemedicină. Așa cum am explicat în mai multe rânduri, fișa medicală a unui pacient valorează pe piața neagră de o sută de ori mai mult decât datele unui card bancar.

Atenție, nu avem de a face doar cu atacuri extrem de sofisticate: de la medici la infirmiere, toți angajații, orice persoană care lucrează în ecosistemul unui spital poate fi ținta unui număr foarte mare de escrocherii, phishing și alte tentative de stabilire de false relații de încredere sau prietenie, număr semnificativ mai mare decât în cazul altor sectoare profesionale (43).

▸▸ Informați-vă din cele mai bune surse

Întrucât sistemul medical din Canada și din Statele Unite ale Americii este unul preponderent privat, directivele, alertele și sfaturile sunt urmărite pe site-urile guvernamentale și private în aceste două state (în Canada, toate documentele sunt disponibile și în franceză).

Recomandăm așadar tuturor celor care lucrează în sectorul medical – și mai ales celor responsabili de infrastructura digitală – să acceseze zilnic surse precum (exemple selectate): https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations; https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19?utm_source=hp_slideshowtm_medium=webtm_campaign=dhsgov



Spre ce ne îndreptăm?

Pentru a încheia într-o notă optimistă, sperăm ca cetățenii și guvernele să învețe câte ceva din situația actuală. Așa cum a spus-o Yuval Noah Harari (nota 5), „Omenirea trebuie să facă o alegere. Vom urma oare calea dezbinării sau vom lua calea solidarității mondiale? Dacă alegem dezbinarea, nu vom face decât să prelungim criza, fapt ce va duce probabil în viitor la catastrofe și mai grave. Dacă alegem solidaritatea mondială, va fi o victorie nu doar împotriva coronavirusului, ci și împotriva tuturor epidemiilor și crizelor viitoare care ar putea lovi omenirea în secolul 21."

ALERTS **Cyber threats to Canadian health organizations**

E rândul fiecăruia dintre noi să facem alegerile corecte și să dăm un exemplu. ■

Note:

(1) Giorgio Agamben, Reflections on the plague, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste)

(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/ ; ed: we propose here an excerpt in Italian from the CNN interview during which Harari took up most of the topics of his article https://it.gariwo.net/educazione/yuval-noah-harari-sull-emergenza-covid19-21870.html).

(3) Translation (author) of two final paragraphs by Michel Onfray, Berezina, in Les Observateurs, 17.03.2020)

(4) Translation (author) of a paragraph by SlavojŽižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plait ! in Le Nouvel Observateur, 18.03.2020 (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)

(5) Yuval Noah Harari, The World, after the Coronavirus, in Optimists and Rational, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/)

(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

(7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

(8) https://www.csa.gov.sg/singcert

(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html

(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/

(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049

(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

(14) Ravie Lakshmanan: Hackers Created Thousandsof Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html

(15) Salvatore Lombardo: The alarm: Coronavirus, increasing cyber attacks, phishing and malspam: advice to defend oneself, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/

(16) Europol REPORT: PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS (pdf) https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

(17) Subdomenio COVID of INCIBE (Instituto nacional de Ciberseguridad) https://www.incibe.es/cibercovid19

(18) Cert Public Administration, COVID page: https://www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/

(19) Agency for Digital Italy, COVID page: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/27/ coronavirus-difendersi-malware-truffe-online

(20) CertFin, COVID page: https://www.certfin.it/newsroom/rendi-la-tua-casa-una-cyber-fortezza/

(21) Italian Association of Clinical Engineers, COVID page: http://www.aiic.it/covid19/

(22) Communications Police: Coronavirus: Minister Lucia Azzolina reports false document of the Ministry of Education, 21.03.2020 https://www.commissariatodips.it/notizie/articolo/coronavirus-il-ministro-lucia-azzolina-denuncia-falso-documento-del-ministero-dellistruzione/index.html

(23) Tarik Saleh, CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware, in Domaintools, 13.03.2020 - with additional link containing full technical description of the malware https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#

(24) Kyle Bradshaw, World Health Organization to launch COVID-19 tips app for Android, iOS, in 9to5Google, 26.03.2020 https://ww.9to5google.com/2020/03/26/world-health-organization-covid-19-app/#

(25) Elena Tebano, Coronavirus, ready the Italian app to trace the contagions: „So we can stop the epidemic", in Corrieredella Sera, 20.03.2019 https://www.corriere.it/tecnologia/20_marzo_18/coronavirus-pronta-app-italiana-tracciare-contagi-cosi-possiamo-fermare-l-epidemia-c6c31218-6919-11ea-913c-55c2df06d574.shtml?refresh_ce-cp

(26) https://innovaperlitalia.agid.gov.it/home/

(27) Andrea Nepori, SOS Italy, here is how the app for the monitoring of the epidemic could be, in La Stampa, 26.03.2020 https://www.lastampa.it/tecnologia/news/2020/03/25/news/sos-italia-ecco-come-potrebbe-essere-l-app-per-il-monitoraggio-dell-epidemia-1.38636482

(28) Communication Police : Coronavirus: Beware of false fundraisingcampaigns ! https://www.commissariatodips.it/notizie/articolo/coronavirus-attenzione-alle-false-campagne-di-raccolta-fondi/index.html

(29) https://www.who.int/about/communications/cyber-security

(30) Communications Police : Coronavirus: BlackNET: RAT distributed via fake „Corona Antivirus". https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(31) Communications Police : Coronavirus : false insuranceproposals for coverage by COVID-19 https://www.commissariatodips.it/notizie/articolo/coronavirus-false-proposte-assicurative-per-la-copertura-da-covid-19/index.html

(32) Internet Stories. Federal Office of Communications OFCOMFederal Office of Consumer AffairsOFCOMFederal Data Protection and TransparencyCommissionerFDPIC Coordination Unit for Combating Internet Crime CYCOReporting and Analysis Centre for Information Assurance MELANIAvailable and downloadable online at: https://www.websters.swiss/it/

(33) Communications Police : BlackNET: RAT distributed via fake „Corona Antivirus". https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html

(34) Communications Police : Coronavirus : risk of solicitation of minors online https://www.commissariatodips.it/notizie/articolo/coronavirus-rischio-adescamento-minori-online/index.html

(35) Keepingchildrensafe online during the Coronavirus outbreak https://www.getsafeonline.org/news/keeping-children-safe-online-during-the-coronavirus-outbreak/

(36) Continuă valul de campanii de tip scam. Atacatorii se folosescacum de imagineaMega Image https://cert.ro/citeste/alerta-scam-kaufland-ikea

(37) Communications Police : Coronavirus : smishingwith false messages fromcredit institutions https://www.commissariatodips.it/notizie/articolo/coronavirus-smishing-con-falsi-messaggi-di-istituti-di-credito/index.html

(38) Samuel Haig, 'CovidLock' Exploits Coronavirus FearsWith Bitcoin Ransomware, in Cointelegraph, 14.03.2020 https://cointelegraph.com/news/covidlock-exploits-coronavirus-fears-with-bitcoin-ransomware

(39) EffectivelyprotectBSI-BUND, smartphone and tablet https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

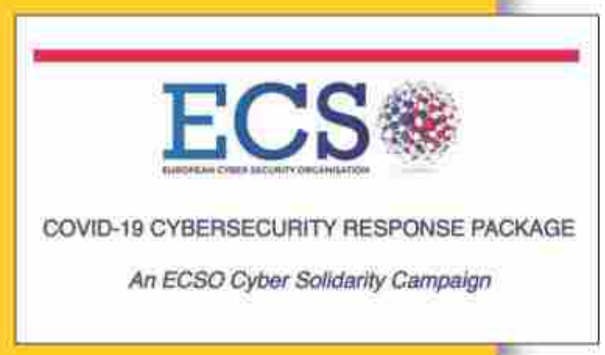
(40) Canadian Centre for Cyber Security, Cyber Hygiene for COVID-19 https://cyber.gc.ca/sites/default/files/publications/Publication-COVID-19-e.pdf

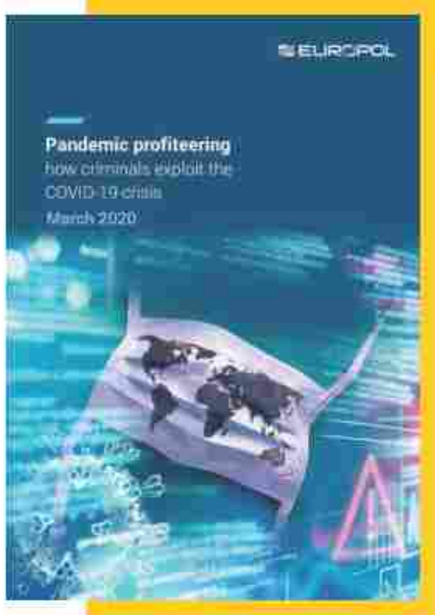
(41) IVCAEW (Institute of CharteredAccountants in England and Wales), Coronavirus guide: cyber hygiene and data https://www.icaew.com/-/media/corporate/files/technical/information-technology/tech-faculty/coronavirus-guide-cyber-hygiene-and-data.ashx

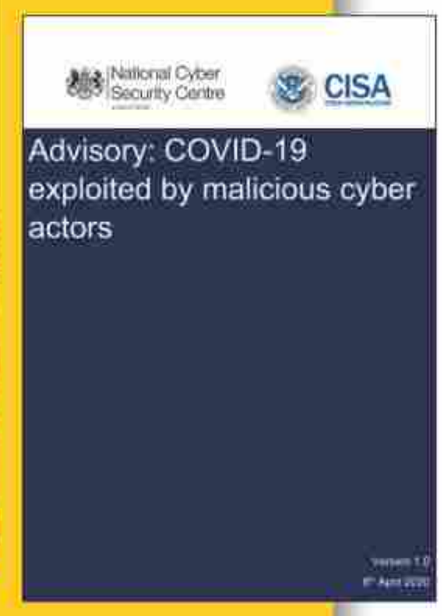
(42) CISA (U.S. Department of Homeland Security) : Alert (AA20-073A) Enterprise VPN Security https://www.us-cert.gov/ncas/alerts/aa20-073a

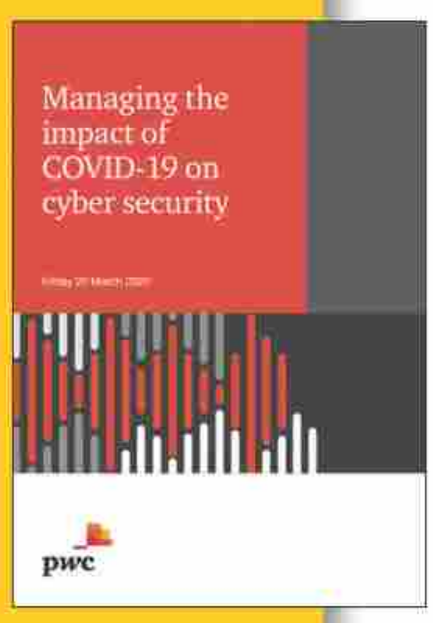
(43) Gareth Corfield, Health workers are top of phishers' target lists thanks to data value, in The Register, 16.03.2020 https://www.theregister.co.uk/2020/03/16/proofpoint_interview/

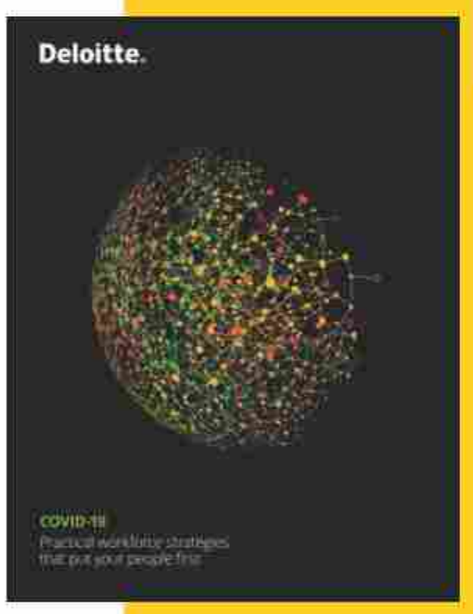
V. Resurse, link-uri utile, recomandări oficiale

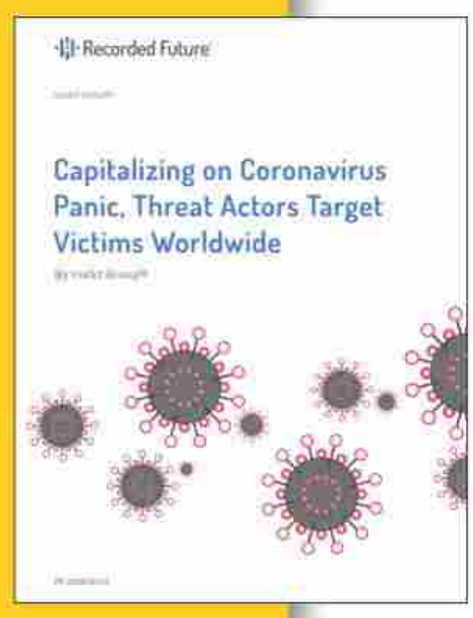


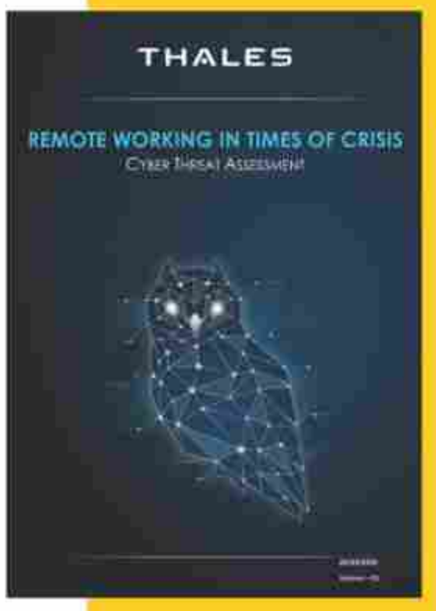


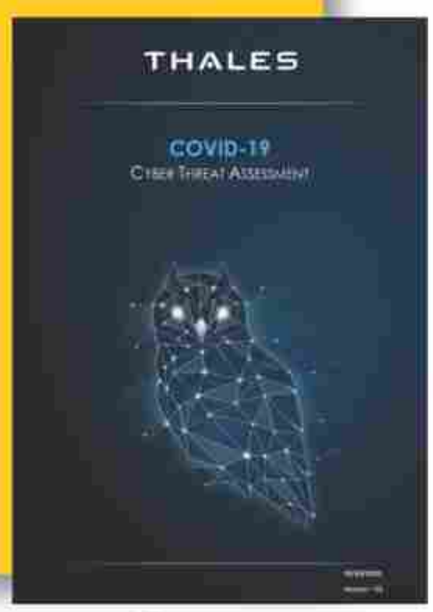












Rapoarte recente: o selecție

Europol (EC3): *Pandemic Profiteering: how Criminals exploit the COVID-19 Crisis* (27.03.2020)
Url: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).
Advisory: COVID-19 exploited by Malicious Cyber Actors (April 2020)
Url: https://www.ncsc.gov.uk/files/Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20V1.pdf

European Cyber Security Organization, *COVID-19 CYBERSECURITY RESPONSE PACKAGE. An ECSO Cyber Solidarity* Campaign (April 2020)
(gathering an impressive list of links and useful resources by companies and State Agencies Europe-wide)
Url: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

McKinsey &Co, *The cybersecurity posture of financial-services companies: IIF/McKinsey Cyber Resilience Survey* (April 2020)
Url: https://www.mckinsey.com/business-functions/risk/our-insights/the-cybersecurity-posture-of-financial-services-companies-iif-mckinsey-cyber-resilience-survey?cid=eml-app

PWC, *Managing the Impact of COVID-19 on Cyber Security* (20.03.2020)
Url: https://www.pwc.co.uk/cyber-security/pdf/impact-of-covid-19-on-cyber-security.pdf

Deloitte, *COVID-19 Practical workforce strategies that put your people first* (April 2020)
Url: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-workforce-strategies-that-put-your-people-first.pdf

Insikt Group, *Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide* (13.03.2020)
Url: https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf

Thales Group, *Remote Working in Times of Crisis - Cyber Threat Assessment* (03.04.2020)
Thales Group, *COVID-19 - Cyber Threat Assessment* (24.03.2020)
Url: https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/covid-19-new-weapon-cyber

România

Raportează spam:
http://www.botfree.ro/spam-reporting.html
Raportează orice are legătură cu online-ul: pagini false, mail-uri false, escrocherii, viruși, hackeri care sparg conturi, informații despre atacuri plănuite etc.:
https://hackout.ro/raporteaza/
Raportează fraude online:
https://ec.europa.eu/anti-fraud/olaf-and-you/report-fraud_ro
Raportează vulnerabilități:
https://cert.ro/pagini/CVD

Numărul unic 1911, prin care persoanele fizice, juridice şi instituţiile publice din România poate raporta incidentele de securitate cibernetică pe care le-au constatat
Raportează încălcări ale drepturilor ce vă sunt recunoscute de RGPD:
https://www.dataprotection.ro/?page=Plangeri_pagina_principala
Notifică o breșă RGPD :
https://www.dataprotection.ro/?page=pagina_formular_679
Poliția Română: adresa de email la care puteți anunța poliția despre activitățile suspecte petrecute în mediul informatic: ***clonare de site-uri, comenzi online în numele dvs dar neautorizate de dvs, spargerea contului de email sau de facebook, postarea de fotografii sau filme pornografice cu minori, primirea de amenințări sau distribuirea de poze intime ce vă aparțin sau fotografii din interiorul casei dvs fără acceptul dvs.***
cybercrime@politiaromana.ro

SRI - GHID DE BUNE PRACTICI PENTRU SECURITATE CIBERNETICĂ (30 p.)
https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf
CERT-RO (Centrul Național de Răspuns la Incidente de Securitate Cibernetică), cu ghiduri, news, tools
www.cert.ro
HACKOUT (partenariat public-privat) cu ghiduri, news, tools
https://hackout.ro/
ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal)
www.dataprotection.ro
ANCOM (Autoritatea Națională pentru Administrare şi Reglementare în Comunicații): news și tools precum platforma informatică Netograf care cuprinde o serie de aplicații menite să ofere utilizatorilor posibilitatea de a măsura și evalua parametrii de calitate tehnici pentru serviciul de acces la internet.
www.ancom.ro

Republica Moldova

Raportează un incident:
https://stisc-cert.gov.md/index.php/report-an-incident/
Serviciul Tehnologia Informației și Securitate Cibernetică
https://stisc.gov.md/ro/
CERT-GOV-MD (Centrul de Răspuns la Incidente Cibernetice) cu ghiduri, news, tools
https://stisc-cert.gov.md

Număr unic pentru raportarea incidentelor de securitate cibernetică

1911

Numărul unic 1911, prin care persoanele fizice, juridice şi instituțiile publice din România vor putea raporta incidentele de securitate cibernetică pe care le-au constatat, a fost lansat oficial în data de 2 mai 2019.

Call Center-ul este disponibil tuturor cetățenilor şi organizațiilor publice şi private din România pentru a raporta incidente de securitate cibernetică, în mod gratuit şi fără întrerupere (24/7).

Este o platformă de colaborare între operatorii de servicii esențiale şi furnizorii de servicii digitale şi are scopul de a contribui la educația celor implicați în incidente de securitate cibernetică.

Primul nivel al Call Center-ului este cel de suport, asistență şi triaj.

Practic, la acest prim nivel al Call Center-ului victima unui atac va avea asigurat suportul tehnic pentru a depăşi momentul, asistența pentru a diminua sau a înlătura incidentul cibernetic, şi triajul, adică faptul că mesajul este receptat şi se face un ticket cu informații specifice.

Apoi, la nivelul 2, aceste informații sunt analizate, iar, pe baza informațiilor analizate, sunt întoarse către victima indicații privind coordonarea incidentului de securitate cibernetică şi, foarte important, se transformă într-o alertă de securitate cibernetică foarte utilă celor care pot fi victime ale aceluiaşi incident.

Prin înființarea acestui Call Center, CERT-RO va îndeplini cerințele impuse CERT-urilor naționale prin Directiva NIS:

- **crearea mai multor mijloace de contact și contactare în orice moment pentru persoane, instituții private și publice din câmpul de responsabilitate a CERT-RO și alte entități cu care CERT-RO cooperează, inclusiv autorități.**
- **nivel ridicat de disponibilitate a serviciilor de comunicații.**
- **personal suficient pentru a asigura disponibilitatea în orice moment.**
- **monitorizarea incidentelor la nivel național.**

I. Cuvinte introductive ale partenerilor

FRAUDA "MESAJ DE LA ȘEF"

Frauda "Mesaj de la șef" vizează angajaţii autorizaţi să efectueze plăţi, care, prin inducere în eroare, sunt determinaţi să plătească o factură falsă ori să efectueze un transfer.

CUM FUNCȚIONEAZĂ?

Un autor sună sau trimite un e-mail, pretinzând că este unul din managerii de top din companie.

De obicei este bine informat cu privire la organizaţie.

Solicită efectuarea urgentă a unei plăţi.

Folosește un limbaj persuasiv, de tipul: "avem încredere în tine, rămâne între noi, eu sunt ocupat acum".

Se referă la o situaţie sensibilă (ex. control autorităţi, achiziţii etc.).

Angajatului i se cere să nu respecte procedura obișnuită de autorizare a plăţilor.

Instrucţiuni complete pot fi trimise mai târziu, de către o persoană sau prin e-mail.

Deseori, solicită ca plata să se facă într-un cont din afara ţării și chiar a Europei.

Angajatul transferă banii într-un cont al autorului.

CARE SUNT SEMNELE?

- E-mail sau apel telefonic nesolicitat.
- Contact cu un oficial cu care nu ești în legătură directă, în mod normal.
- Solicitare de confidenţialitate.
- Presiune sub semnul presupusei urgenţe.
- Solicitare neobișnuită, ieșită din tiparele procedurilor interne.
- Ameninţări sau promisiuni neobișnuite, flatare.

CE POȚI FACE?

CA ORGANIZAŢIE

Conștientizaţi riscul și asiguraţi-vă că **angajaţii sunt informaţi permanent**.

Instruiţi-vă staff-ul să manifeste **atenţie maximă la efectuarea plăţilor**.

Implementaţi proceduri interne stricte referitoare la plăţi.

Implementaţi proceduri de verificare a legitimităţii plăţilor solicitate prin e-mail.

Stabiliţi reguli de raportare a tentativelor de fraudă.

Verificaţi datele publicate pe site-ul companiei, **restricţionaţi accesul la datele importante** și fiţi atenţi la reţelele sociale.

Actualizaţi soluţiile tehnice de securitate.

Sesizaţi poliţia la orice încercare de fraudă, chiar dacă nu aţi devenit victima acesteia.

CA ANGAJAT

Respectaţi cu strictețe procedurile de securitate în cazul plăţilor și achiziţiilor. **Nu săriţi nici un pas procedural și rezistaţi presiunilor.**

Verificaţi cu atenţie adresele de e-mail când primiţi solicitări de informaţii sensibile/transferuri de bani.

Dacă aveţi dubii în cazul unui transfer de bani, **consultaţi un coleg.**

Niciodată nu deschideţi link-uri sau atașamente dubioase primite prin e-mail. Fiţi foarte atenţi când verificaţi mail-ul personal pe calculatorul de serviciu.

Manifestaţi precauţie și restricţionaţi informaţiile de pe reţelele sociale.

Evitaţi publicarea de date despre conducerea, securitatea sau procedurile firmei.

Dacă primiţi un e-mail suspect, informaţi imediat departamentul IT.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

FRAUDE CU INVESTIȚII

Fraudele obișnuite cu investiții pot include ”oportunități” de investiții în acțiuni, obligațiuni, criptomonedă, metale prețioase, imobiliare în străinătate sau energii alternative.

CARE SUNT SEMNELE?

- Ești asigurat că afacerea e sigură și îți recuperezi foarte repede investiția.
- Oferta este limitată în timp.
- Primești un apel nesolicitat, în mod repetat.
- Oferta este doar pentru tine și nu trebuie să o divulgi altcuiva.

CE POȚI FACE?

- **Întotdeauna cere sfaturi financiare de la o peroană imparțială,** înainte de orice investiție ori plată.
- **Refuză orice apel necunoscut** legat de așa zise oportunități de investiții.
- **Fii precaut** la ofertele care promit investiții ”sigure”, recuperare garantată ori câștiguri mari.
- **Atenție la tentativele viitoare**. Dacă ai fost victima unei fraude, foarte probabil autorii te vor ținti din nou sau îți vor vinde datele altor infractori.
- **Contactează poliția** dacă ai suspiciuni.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

FRAUDE CU FACTURI

CUM FUNCȚIONEAZĂ?

- O firmă este contactată de cineva care pretinde că este reprezentantul unui furnizor.
- Poate fi o abordare încrucișată - prin telefon, scrisoare, e-mail etc.
- Autorul solicită modificarea datelor bancare (numărul de cont, banca la care e deschis etc) pentru plăţile viitoare. Noul cont este deţinut/controlat de acesta.

CE PUTEȚI FACE?

CA ORGANIZAŢIE

Asiguraţi-vă că **angajaţii sunt informaţi și cunosc acest tip de fraudă** și cum să îl evite.

Instruiţi-vă personalul ca **întotdeauna să verifice orice neregulă** posibilă la plăţile facturilor.

Implementaţi **proceduri clare de verificare** a legitimităţii plăţilor.

Reanalizaţi informaţiile postate pe site-ul companiei, în special referitor la contracte și furnizori. Limitaţi datele despre companie pe care angajaţii le pot posta pe reţele sociale.

CA ANGAJAT

Verificaţi orice solicitare pretinsă a fi din partea creditorilor, în special dacă cer modificarea detaliilor bancare pentru viitoare plăţi.

Pentru plăţi peste o anumită sumă, **instituiţi o procedură suplimentară de verificare** cu beneficiarul.

Folosiți **datele de contact din corespondenţa anterioară** pentru a verifica și nu pe cele din mesajul prin care se solicită modificările.

Când efectuaţi o plată, **trimiteţi un e-mail de confirmare destinatarului**. Pentru siguranţă, includeţi denumirea băncii și ultimele 4 cifre ale numărului de cont.

Stabiliţi puncte de contact unice cu companiile partenere către care efectuaţi plăţi regulate.

Fiţi precaut cu datele despre locul de muncă pe care le postaţi pe reţelele sociale.

Sesizaţi poliţia la orice încercare de fraudă, chiar dacă nu aţi devenit victima acesteia.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

FRAUDE LA CUMPĂRĂTURI ONLINE

Cumpărăturile online pot fi benefice, dar atenție la fraude.

CE POȚI FACE?

- **Folosește site-uri românești**, pe cât posibil - pot fi mai ușor de detectat eventuale probleme.
- **Verifică înainte să cumperi** - recenziile site-ului/produsului.
- **Folosește cardul de credit** - ai mai multe șanse de a-ţi recupera banii.
- **Plătește folosind servicii de plăţi sigure** - ţi se solicită plata prin transfer bancar? Mai gândește-te!

- Plătește doar când ai o **conexiune sigură la internet** - evită folosirea hot-spot-urilor publice de wi-fi.
- Folosește un **dispozitiv sigur când plătești** - fă-ţi la timp actualizările de sistem și securitate.
- Atenţie la reclame, "oferte miraculoase", "afaceri-bombă" - **dacă e prea frumos ca să fie adevărat, probabil nu e!**
- O fereastră pop-up îţi spune că ai câștigat un premiu fabulos? **Mai gândește-te!**
- Dacă produsul comandat nu sosește la timp, contactează imediat vânzătorul. Dacă nu răspunde, **contactează banca**.

Sesizaţi poliţia la orice încercare de fraudă, chiar dacă nu aţi devenit victima acesteia.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

E-MAIL-URI TIP PHISHING

Phishing se referă la mesaje false care induc în eroare destinatarii, pentru a-și divulga date personale, financiare ori de securitate.

CUM FUNCȚIONEAZĂ?

Aceste e-mail-uri:

pot arăta identic cu acelea pe care le primiţi de la bancă.

imită logo-ul și designul mesajelor reale.

îţi solicită să descarci un atașament sau să deschizi un link.

utilizează un limbaj care sugerează urgenţa.

CE POȚI FACE?

- **Actualizează permanent programele** calculatorului, inclusiv sistemul de operare.
- Fii **extrem de atent** dacă primești mesaje "din partea băncii" prin care ţi se solicită date sensibile (date despre cont, parole etc.).
- **Citește cu atenţie mesajele** - compară adresa expeditorului cu cea din corespondenţele anterioare. Verifică eventuale greșeli de exprimare.
- **Nu răspunde la mesaje dubioase**. Eventual, le poţi retransmite băncii tale, scriind adresa.
- **Nu deschide link-urile și nu descărca** atașamentele din astfel de mesaje.
- Dacă ai dubii cu privire la o tranzacţie, **efectuează verificări suplimentare**.

Infractorii informatici se bazează pe faptul că oamenii sunt ocupaţi; la prima vedere, aceste e-mail-uri par legitime.

Atenţie la folosirea dispozitivelor mobile. Poate fi mai dificil de depistat o încercare de phishing pe telefonul mobil sau pe tabletă.

#CyberScams

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

IUBIRE PREFĂCUTĂ

Autorii vizează victimele pe site-uri de întâlniri, dar pot utiliza și reţele de socializare sau e-mail-ul pentru contact.

CARE SUNT SEMNELE?

O persoana recent cunoscută online, îţi declară sentimente de iubire și îţi cere să vorbiţi în privat.

Mesajele lor sunt vagi și/sau conţin greșeli de exprimare.

Profilul online nu corespunde cu ceea ce spun.

Îţi pot solicita filme sau fotografii intime.

€€€

Încearcă să îţi câștige încrederea repede, apoi îţi cer bani, cadouri ori date bancare.

Dacă nu trimiţi bani de bună voie, vor recurge la șantaj. Cu cât trimiţi mai mult, vor cere mai mult.

AI DEVENIT VICTIMĂ?

Nu te simţi rușinat/ă!
Oprește imediat contactul cu autorul!
Dacă este posibil, salvează/păstrează convorbirile purtate.
Fă o plângere la poliţie.
Raportează autorul la site-ul pe care te-a contactat inițial.
Dacă ai transmis detalii bancare, contactează imediat banca.

CE PUTEŢI FACE?

- **Fiți foarte atent** cu datele personale pe care le postaţi pe reţele de socializare ori site-uri de întâlniri.
- **Evaluaţi permanent riscurile.** Escrocii sunt prezenţi pe cele mai populare site-uri.
- **Nu vă grăbiţi** și întrebaţi.
- **Verificaţi** profilele și fotografiile persoanelor. Pot fi copiate și folosite nelegitim.
- **Fiţi atenţi** la greșelile gramaticale, neconcordanţele în informaţii și scuzele de tipul "camera mea foto nu funcţionează".
- **Nu transmiteţi** materiale compromiţătoare, care ar putea fi folosite la șantaj.
- Dacă vreţi să vă întâlniţi personal, **spuneţi familiei/prietenilor** locul și perioada.
- **Atenţie la solicitările de bani!** Nu trimiteţi niciodată bani, datele card-ului ori alte detalii financiare sau copii ale actelor personale.
- **Evitaţi** plăţile în avans.
- **Nu intermediaţi transferuri de bani!** Spălarea de bani este infracţiune.

EUROPOL EC3 European Cybercrime Centre

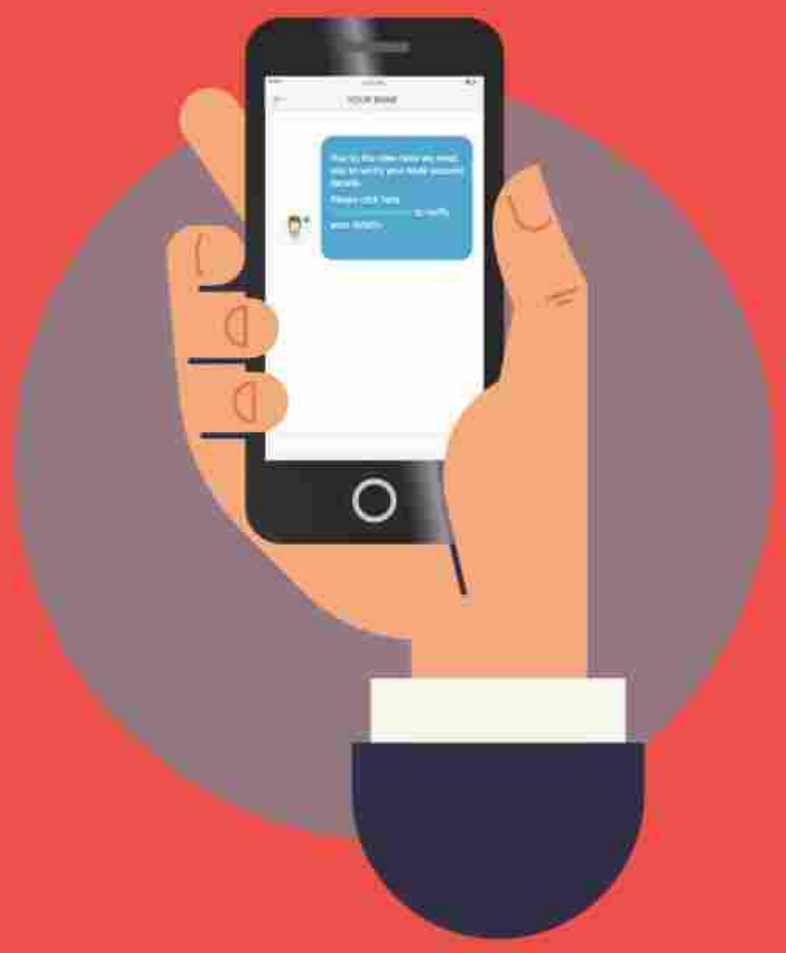
EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

PHISHING PRIN SMS

Smishing (combinaţie de cuvinte dintre SMS și Phishing) este încercarea de inducere în eroare prin mesaje text, pentru obţinerea de date personale, bancare ori de securitate.



CUM FUNCȚIONEAZĂ?

Prin mesajul text (SMS), autorii, de obicei, îţi solicită să apelezi un număr de telefon sau să accesezi un link prin care "îţi verifici, actualizezi, reactivezi" contul. Dar...în realitate ești direcţionat către un site fals sau un operator-complice, pretins reprezentant al băncii.

CE POȚI FACE?

- **Nu accesa link-uri, atașamente sau imagini nesolicitate**, primite prin SMS de la persoane necunoscute.
- **Nu acţiona în grabă**. Ia-ţi timp și verifică informaţiile înainte de a trimite un eventual răspuns.
- **Niciodată nu răspunde unui SMS** prin care ţi se solicită codul PIN, parole de acces la contul de online banking ori alte credenţiale de siguranţă.
- **Contactează imediat banca**, dacă știi că ai răspuns unui astfel de mesaj și ai furnizat detalii bancare în aceste condiţii.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

SITE-URI BANCARE FALSE

E-mail-urile tip phishing includ de obicei link-uri care te direcţionează către site-uri bancare contrafăcute, unde ţi se solicită să îţi divulgi date personale și financiare.

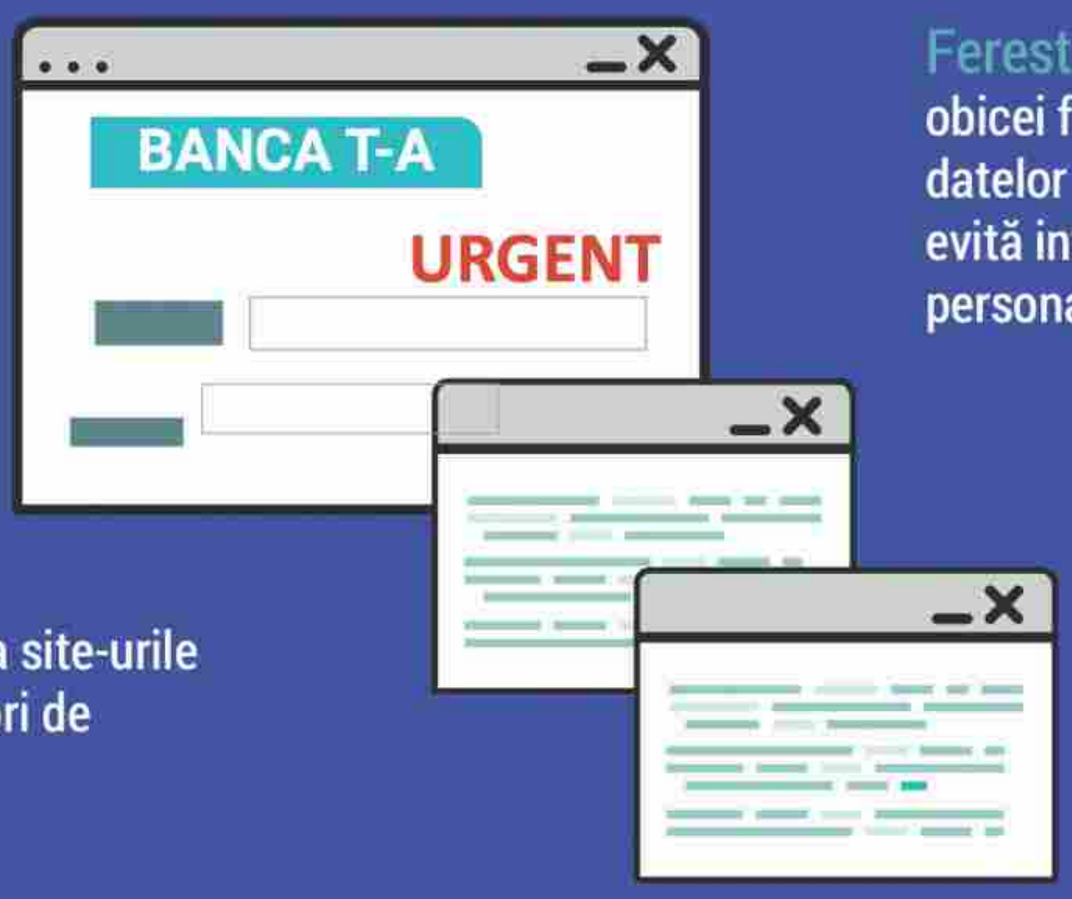
CARE SUNT SEMNELE?

Site-urile false arată aproape identic cu cele legitime. Cel mai des, acestea te conduc către o fereastră pop-up, unde ţi se cer credenţialele bancare. Site-urile reale nu folosesc astfel de ferestre.

În astfel de mesaje de obicei apar:

Urgenţa: nu veți găsi asta pe site-urile legitime.

Design defectuos: fiţi atenţi la site-urile care conţin greșeli gramaticale ori de exprimare.



Ferestre tip pop-up: sunt de obicei folosite pentru culegerea datelor tale. Nu le accesa și evită introducerea datelor personale în astfel de ferestre.

CE POȚI FACE?

Niciodată nu accesa site-ul băncii tale prin link-uri trimise pe e-mail.

Tastează manual adresa băncii când vrei să accesezi site-ul acesteia.

Folosește browsere care permit **blocarea ferestrelor pop-up**.

Dacă banca are ceva important să îţi comunice, vei fi notificat **după ce îţi vei accesa contul online**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

APELURI TELEFONICE TIP PHISHING

Vishing (combinaţie de cuvinte între "Phishing" și "voce") este o fraudă în care autorii, apelând telefonic victima și folosind diverse pretexte, o conving să divulge date personale și/sau financiare ori să le transfere bani.

CE POȚI FACE?

- **Fii prudent** cu privire la apelurile telefonice primite de la necunoscuţi.
- **Cere numărul apelantului** și spune-i că revii tu cu un apel.
- Pentru verificarea identităţii acestuia, **apelează organizaţia în numele căreia pretind că sună**.
- **Chiar dacă îţi transmit un număr la care îi poţi contacta,** nu considera asta ca formă de verificare a realităţii expuse.
- Autorii pot găsi informaţii despre tine în mediul online, în special pe reţele sociale. **Nu lua de bun orice telefon,** doar pentru că apelantul știe câte ceva despre tine.
- **Nu transmite prin telefon codul PIN ori parola** de la contul de Internet Banking. Niciodată banca nu ţi le va solicita în acest mod.
- **Nu transfera bani** către necunoscuţi care îţi solicită asta.
- Dacă ai bănuieli, **contactează banca**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

Reguli de igienă cibernetică pe timp de COVID-19!

Ce puteți face ca organizație?

- Asigurați accesul angajaților la documente de lucru doar prin canale de comunicare criptate (SSL VPN, IPSec VPN).
- Oferiți angajaților acces la un software sigur dedicat apelurilor video.
- Conștientizați riscurile de securitate posibile și asigurați-vă că angajații sunt constant informați.
- Asigurați-vă că există o persoană de contact, disponibilă să ofere suport de la distanță angajaților, în cazul în care apar erori tehnice sau de securitate.
- Verificați regulat datele publicate pe pagina oficială a instituției și restricționați accesul la date importante.
- Asigurați-vă că angajații respectă prevederile cadrului legal privind cerințele minime de securitate.
- Asigurați-vă că angajații respectă legislația referitoare la protecția datelor cu caracter personal.

Ce puteți face ca angajat?

- Folosiți preferabil dispozitive și conexiuni furnizate de organizație (laptop și telefon de serviciu, conexiune privată protejată prin parolă, etc.)
- Nu partajați adresele URL a conferințelor video online pe diverse canale de social media pentru a evita accesul unor părți terțe neautorizate.
- Folosiți parole puternice și unice pentru fiecare cont (minim 8 caractere) de litere mari și minuscule, numere și caractere speciale.
- Faceţi cu regularitate copii ale fișierelor şi salvaţi-le pe suporturi sigure.
- Asigurați confidențialitatea strictă a datelor cu caracter personal(ale colegilor sau clienților).
- Nu lăsați dispozitivele spre a fi utilizate de către copii sau alți membri ai familiei.
- Nu lăsați laptopul deschis (unlocked) la părăsirea spațiului de lucru. Puteți bloca ecranul dispozitivului prin apăsarea combinației de taste (Windows+L).

SEMNE DE ALARMĂ!

În perioada pandemiei de COVID-19, fiți precauți și respectați regulile de igienă cibernetică pentru a evita escrocherii și fraude în mediul online!

- Mesaje suspecte, care creează o imagine de urgență sau prin care se solicită lucruri neobișnuite, uneori aparent transmise de la persoane cunoscute.
- Atașamente din email, care au extensii neobișnuite (ex. ".pif", ".exe", ".liliac", ".vbs"). Nu le deschideți niciodată.
- e-mail-urile nesolicitate, cu ataşamente sau link-uri către pagini ce conțin prea multe greșeli gramaticale și neconcordante de informații.

REȚINEȚI!
Infractorii cibernetici profită de anxietatea și panica oamenilor în mod special pe perioada pandemiei. Fiți atenți și urmăriți doar surse oficiale și credibile pentru informații actualizate.

I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"

022 820 911
www.stisc.gov.md
stisc@stisc.gov.md
info@cert.gov.md

Despre importanța de a repoziționa elementul uman ca actor al securității cibernetice si de a reda o semnificație pozitivă acestui comportament

Centre de recherche de l'EOGN

FIC — FORUM-FIC.COM —

Autor: **General Marc Watin-Augouard**

Criza generată de Covid-19 va grăbi fără îndoială transformarea digitală, cu consecințe dintre cele mai bune, dar și dintre cele mai proaste. Prădătorii au înțeles că această criză le oferă oportunitatea de a se muta într-un spațiu digital care nu cunoaște limite. Și vor rămâne acolo! Utilizatorii cinstiți de pe internet n-au folosit niciodată atât de mult aplicații, al căror număr a crescut enorm, mai ales în contextul adoptării masive a muncii la distanță și al nevoii de a păstra contactul uman în ciuda „distanțării sociale". În viitorul apropiat, vom vedea cu siguranță o reorganizare a teritoriului, cu o revenire a traiului „la țară", satele fiind mai reziliente decât orașele, cu condiția să aibă internet de mare viteză. În curând, contribuția tehnologiei 5G, Big data, inteligenței artificiale vor genera moduri noi de folosință, mai ales în beneficiul telemedicinii, predicției unor epidemii și a modului lor de răspândire. În curând, roboți controlați de la distanță vor face posibilă munca la distanță celor care acum sunt „în prima linie", livrarea de produse, protejarea persoanelor vulnerabile.

Însă nimic nu se va putea înfăptui fără identificarea unui sens! „Repoziționarea elementului uman în centrul securității cibernetice" nu mai constituie o opțiune între atâtea altele, ci a devenit o exigență. Mai mult ca niciodată, securitatea cibernetică va trebui să fie în serviciul libertății. Suntem conștienți de cât de mult o prețuim și înțelegem că trebuie apărată de cei care au alte viziuni despre Om.

Securitatea cibernetică a fost construită din straturi succesive. După controlul „gestiunii" datelor (1978) a venit protejarea „sistemelor" de gestionare automatizată a datelor (1988), apoi cea a „datelor", repoziționate în centrul ecosistemului digital (2018). Datele cu caracter personal s-au bucurat întotdeauna de o vigilență specială, însă caracterul lor sensibil n-a fost niciodată accentuat atât de tare, iar acest lucru se datorează creșterii exponențiale a platformelor, aplicațiilor, sistemelor conectate care „reformatează" societatea cu o viteză adesea imperceptibilă prin propriile simțuri. Mai mult ca oricând, aceste date ne caracterizează, ne dezvăluie intimitatea, intră în sfera secretului vieții noastre private fără de care nu ar exista libertate. Supus unei profilări realizate de algoritmi mai scrutătoare ca niciodată, omul nu mai este în totalitate stăpân, ci tinde să devină subiect, cu riscul chiar de a sfârși sclav. Și totuși, nu e timpul pierdut, fiindcă înțelegerea deplină a transformării digitale necesită o

Atenție sporită la Phishing prin email, telefon și SMS-uri

Phishing - mesaje false care induc în eroare destinatarii, pentru a-și divulga date personale, financiare ori de securitate.

- Nu vă grăbiți să faceți un clic. Dacă aveți dubii cu referire la email, cel mai sigur este să îl ștergeți înainte de a-l deschide.
- Nu deschideți și nu descărcați atașamente, mai ales dacă sunt dubioase. Comparați adresa expeditorului cu cea din corespondența anterioară, sau eventual verificați posibile greșeli de exprimare.
- Nu răspundeți la e-mail-urile care solicită numere de cont, datele cardului de credit, transferuri bancare, etc. Nu există niciun motiv să partajați aceste informații prin mesaj sau pe un site nesigur.

Vishing - atacatorii apelând telefonic victima, o conving să divulge date personale și/sau financiare ori chiar să le transfere bani.

- Fiți prudenți la apelurile telefonice primite de la necunoscuți.
- Pentru siguranță, cereți numărul apelantului și confirmați că reveniți ulterior cu un apel.
- Nu transmiteți codul PIN ori parola de la contul de Internet Banking prin telefon. Banca niciodată nu solicită informația în acest mod.
- Pentru orice îndoieli, nu ezitați să contactați banca.

Smishing - atacatorii prin intermediul mesajelor text (SMS) obțin de la victime date personale, bancare și de securitate.

- Nu accesați link-uri, atașamente sau imagini nesolicitate, primite prin SMS de la persoane necunoscute.
- Nu acționați în grabă. Neapărat verificați informațiile înainte de a transmite un răspuns.
- Nu răspundeți la un SMS care vă solicită codul PIN, parole de acces la contul de online banking sau alte informații confidențiale.
- În cazul în care ați oferit răspuns unui mesaj dubios și respectiv ați furnizat informații bancare, contactați imediat banca.

REȚINEȚI!

Pe perioada pandemiei, fiți îndeosebi atenți la orice e-mail/SMS/apel telefonic, care face referire la virusul COVID-19, deoarece acestea pot fi încercări de înșelătorie sau escrocherii.

I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"

022 820 911
www.stisc.gov.md
stisc@stisc.gov.md
info@cert.gov.md

Atenție la pagini web false!

- Atenție la bara de adrese. Dacă un site web folosește http: // (fără S), atunci fiți atenți și nu introduceți informații personale.
- Verificați numele de domeniu și greșelile de ortografie. De multe ori, escrocii emit adresele web a unor companii mari cu renume, cum ar fi Yah00.com sau Amaz0n.net.
- Țineți cont că atacatorii imită perfect logoul și designul mesajelor expediate, iar de foarte multe ori, utilizează un limbaj care sugerează urgență.
- Folosiți doar opțiuni de plată sigure, cercetând în prealabil pagina web (analiza recenziilor).
- Folosiți instrumente de securitate. Instalați program antivirus și utilizați plugin-uri pentru browsere, care vă pot avertiza dacă încercați să accesați site-uri web potențial periculoase.

- Cumpărați exclusiv de la magazine cunoscute și citiți atent recenziile.
- Folosiți cartea de credit pentru cumpărături online.
- Nu vă grăbiți să acceptați orice ofertă! Dacă promoția este una prea bună pentru a fi reală, atunci cel mai probabil este o încercare falsă.
- Păstrează întotdeauna documentele referitoare la plățile pe care le-ai efectuat online.
- Nu trimite niciodată numărul de card, PIN-ul sau alte date ale cardului prin email
- Verificați periodic tranzacțiile din cont, pentru a identifica din timp orice activitate suspicioasă.
- Dacă produsul comandat nu sosește la timp, contactați imediat vânzătorul. Dacă nu răspunde, contactați banca.

Sfaturi pentru cumpărături sigure în regim online!

REȚINEȚI!

Pentru a evita escrocheriile online mai ales atunci când doriți să procurați diverse produse, fiți vigilenți și precauți. Nu uitați, infractorii cibernetici profită de panica și disperarea populației.

I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"

022 820 911
www.stisc.gov.md
stisc@stisc.gov.md
info@cert.gov.md

Stimată Doamnă, Stimate Domn,

Piața profesioniștilor în domeniul securității IT este limitată, iar în prezent există un deficit de competențe în acest sector. Acesta este unul dintre motivele pentru care multe țări europene au lansat competiții naționale de securitate cibernetică, pentru a găsi tinere talente în rândul studenților, liceenilor sau chiar a școlarilor și pentru a-i încuraja să urmeze o carieră în domeniul securității cibernetice.

Toate aceste inițiative singulare de descoperire a celor mai experimentați tineri în domeniu s-au transformat sub umbrela *ENISA (Agenția Europeană pentru Securitate Cibernetică)* în *Campionatul European de Securitate Cibernetică*, care a debutat în anul 2015 si care se deruleaza în conformitate cu *Planul de Actiune pentru Implementarea Strategiei de Securitate Cibernetica a UE*. Fiecare țară participantă la competiție trimite în finală o echipă formată din *10 tineri talentați*, selectați în urma concursurilor naționale.

În ultimii 4 ani, *Serviciul Român de Informații, CERT-RO și Asociația Națională pentru Securitatea Sistemelor Informatice*, alături de *ceilalți partenerii implicați*, Orange, Certsign, Bit Sentinel și CISCO, au susținut procesul de selecție, training și participare a *echipei naționale a României* la Campionatul European. Ediția din 2015 ne-a oferit oportunitatea de a debuta la această competiție la nivel european, ocazie cu care concurenții s-au familiarizat cu formatul și au înțeles exigențele concursului. Grație experienței acumulate, a pregătirii susținute și a dedicării instructorilor, la următoarele două ediții echipa noastră a cucerit titlul de viecampioană europeană.

După editia din 2018 de la Londra, *ECSC 2019 a fost organizat la București, în cadrul unui eveniment de amploare, la finalul căruia România a cucerit titlul de Campioană a Europei în domeniul securității cibernetice.*

În 2020, ne vom apăra titlul de campioană la Viena. Faza finală este programată la începutul luni noiembrie, însă până atunci, România trebuie să-și formeze lotul cu care va aborda competiția. Înscrierile se pot face pe site-ul cybersecuritychallenge.ro, iar prima etapă constituie o preselecție a candidaților la nivel național și va avea loc online, în perioada 9-10 mai. La concurs pot participa tineri cu vârste de până la 25 de ani, pasionați de securitate cibernetică.

Competiția națională se desfășoară în două stadii. După procesul inițial de preselecție online vor urma două etape suplimentare, în care tinerii vor fi testați și antrenați pe parcursul a două sesiuni de training (bootcamp) prin exerciții din domeniul securității aplicațiilor web, atacului și apărării cibernetice, criptografiei, analizei traficului de rețea, reverse engineering și abilități de prezentare. La faza finală a competiției, fiecare țară participantă va fi reprezentată de o echipă formată din 10 concurenți: 5 din categoria de vârstă 16-20 de ani și 5 din categoria de vârstă 21-25 de ani.

Campionatul European de Securitate Cibernetică reprezintă o oportunitate pentru participanți, care nu sunt *profesioniști în domeniul IT, să își testeze competențele digitale*. În plus, tinerii beneficiază de recunoaștere națională și promovare, mentorat cu specialiști în domeniu, stagii specializate de pregătire tehnică și soft skills, premii oferite de parteneri sau oportunități de angajare în domeniu. Detalii despre materialele educationale recomandate pentru pregătire se regăsesc pe site.

Tinerii interesați de dezvoltarea abilităților tehnice de profil se pot pregăti pentru Campionatul European de Securitate Cibernetică pe platforma online cyberedu.ro, un spațiu digital în care se regăsesc majoritatea exercițiilor propuse în faza națională și faza internațională de la ECSC 2019 dar și alte exerciții construite pentru competiții de securitate cibernetică internaționale.

O particularitate a Campionatul European de Securitate Cibernetică este faptul că abilitățile și competențele tehnice superioare ale unei echipe nu-i garantează victoria. Echipa câștigătoare va trebui să demonstreze că deține și competențe social-culturale (așa numitele soft skills), precum capacitatea de a lucra în echipă, strategia de abordare și de alocare a fiecărei sarcini, stilul de prezentare sau abilități de comunicare.

În acest context, vă adresăm rugămintea să ne sprijiniți în identificarea a cât mai multor tineri talentati în acest domeniu precum și în promovarea campaniei de înscriere. Mai multe informații, precum și calendarul evenimentelor se regasesc pe site-ul competitiei naționale, unde se poate face și inscrierea candidaților: www.cybersecuritychallenge.ro ■

SRI - GHID DE BUNE PRACTICI PENTRU SECURITATE CIBERNETICĂ (30 p.)

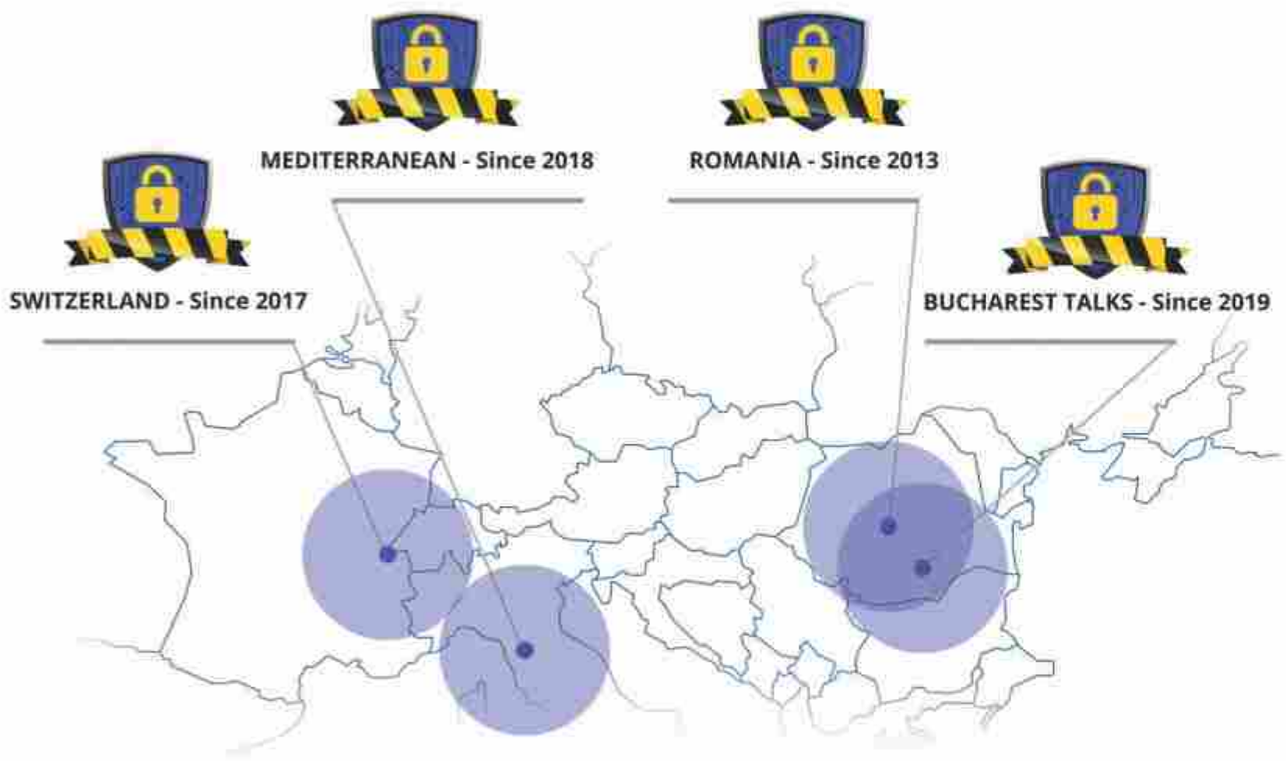
URL: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

CYBERSECURITY DIALOGUES

www.cybersecurity-dialogues.org

BROUGHT TO YOU BY:

web for your business
swiss webacademy



www.cybersecurity-dialogues.org

The only platform with it's own quaterly magazine

https://issuu.com/cybersecuritytrends

O publicație

web for business
swiss webacademy

Redactori:

Laurent Chrzanovski,
Romulus Maier †

Traduceri și corecturi:

Lucia Sevestrean
Gabriela Marinescu

ISSN 2393 – 4778
ISSN-L 2393 – 4778

Adresa:

Școala de Înot nr. 18,
550005 Sibiu, România
www.swissacademy.eu
www.cybersecurity-dialogues.org

Pentru a descărca acest volum special
editat în română, engleză şi franceză
accesați pagina:
https://swissacademy.eu/cybercovid/

Partner Congresses

CHARENTE-MARITIME CYBER SÉCURITÉ
— CMCS-CONNECT.FR —

CYBERSECURITY PUBLIC - PRIVATE DIALOGUES
— CYBERSECURITY-DIALOGUES.ORG —

FIC
— FORUM-FIC.COM —

Charente Maritime Cyber Sécurité
CMCS2020 - 13, 14 & 15 octobre 2020

OBJECTIFS : L'évolution grandissante des attaques numériques et informatiques nécessitent prévention et sécurisation. Ces cybers attaques sont massives, multiples et incessantes. La gravité de leurs impacts ne fait que s'accroître au fil du temps. C'est une criminalité organisée à l'échelle mondiale tournée vers l'extorsion de fonds. CMCS 2020 traitera des risques économiques et sociaux, notamment sur les populations les plus fragiles. Le tourisme sera l'axe économique qui permettra de pragmatiser le discours. C'est une véritable approche sociétale du cyber monde que nous voulons explorer.

Quels Risques ? : Aujourd'hui, il est facile d'identifier les risques qui nous menacent :

- L'Hyper numérisation des outils, qu'ils soient du quotidien ou professionnels
- L'Hyper connexion des différents éléments de notre vie quotidienne
- L'Hyper information que nous créons dans tous les domaines
- L'Hyper utilisation de l'énergie électrique

INFORMER

SENSIBILISER

FAIRE AGIR

Quelles Parades ?
Les parades sont nombreuses et devront s'appliquer aux 4 types de risques que nous avons identifiés. Mais en aucun cas ces parades ne sauraient nous protéger de façon globale. Nous sommes donc contraints d'adopter un comportement qui visera à renforcer la résilience des systèmes plutôt que leur résistance.

Stanchion Payment Solutions

Global Payment Specialists

Our experience in complex payments environments and our international perspective of client engagements enable us to offer a range of solutions, services and products to integrate, improve, optimise and secure your payments systems.

Please contact us at *engage@stanchionpayments.com* for further details on our security and payment health-check services.

Visit our website: *stanchionpayments.com/insights/brochures/* to download free brochures on security and securing your payments systems.

STANCHION

Engage | Innovate | Solve | Secure

www.stanchionpayments.com

Prefețe - Cybersecurity Trends

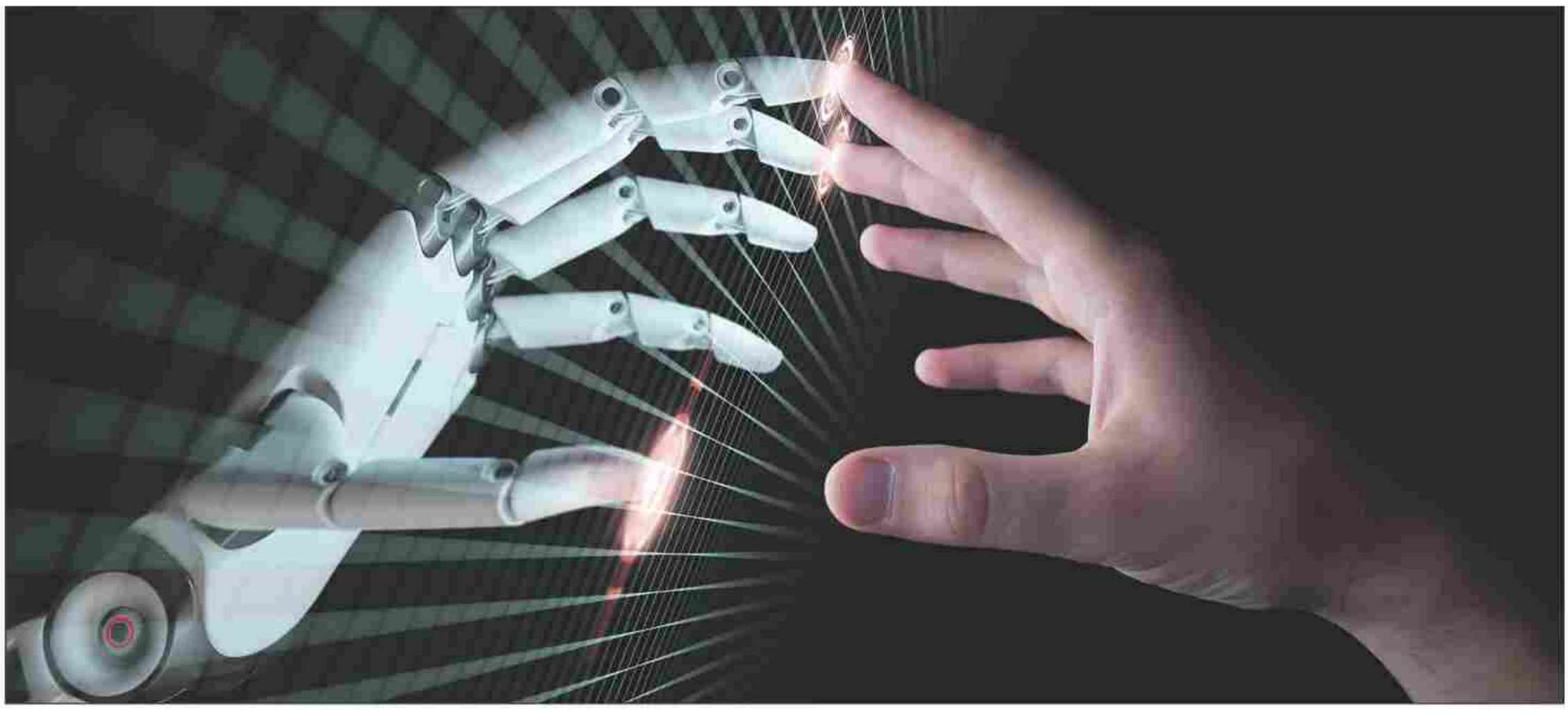
BIO

- Fondator și Codirector, Forumul internațional de securitate cibernetică (Forum international de la cybersecurité – FIC)
- Director, Centrul de Cercetări al Școlii de Ofițeri a Jandarmeriei Naționale (Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale - CREOGN)
- Fost inspector general al armatei-jandarmerie
- General de armată (2008)
- General al corpului de armată (2007)
- General de divizie (2006)
- Comandant, Jandarmeria pentru zona de apărare Nord (2005 – 2008)
- Comandant, Jandarmeria regiunii Nord-Pas-de-Calais
- Consilier al jandarmeriei, Cabinetul lui Dominique de Villepin (2004 – 2005)
- General de brigadă (2003)
- Consilier de securitate, Cabinetul lui Nicolas Sarkozy (2002 – 2004)
- Comandant al legiunii de jandarmerie departamentală din Champagne-Ardenne (2000 - 2002)
- Învățământ: Profesor Asociat în drept la Universitățile Panthéon-Assas (Paris II), René Descartes (Paris V) și Aix-Marseille III-Méditerranée.

mobilizare a competențelor, o aculturație împărțită cu provocările acestei noi lumi. Adesea abandonată în sarcina specialiștilor și experților, securitatea cibernetică trebuie în realitate să fie produsul unei atitudini individuale și colective, rezultată dintr-o formare în masă de la cele mai fragede vârste. Adesea identificată ca fiind un domeniu rezervat bărbaților, securitatea cibernetică trebuie susținută și de către femei, care în prezent ocupă doar 10% din posturile din domeniu, deși reprezintă mai mult de jumătate din populație. Fără îndoială, trebuie să recurgem la tehnologii precum inteligența artificială pentru a ne securiza rețelele, schimburile, datele. Însă este obligatorie de asemenea repoziționarea elementul uman ca actor al securității cibernetice și de a reda o semnificație pozitivă acestui comportament, deoarece momentan acesta e văzut doar ca victimă sau autor, voluntar sau involuntar, al incidentelor și faptelor răuvoitoare din domeniul digital.

În procesul nostru de urmărire a consolidării securității cibernetice, suntem adeseori tentați să primim răspunsul la întrebarea „cum?", lăsând răspunsul în sarcina tehnologiilor, astfel că am omis să ne punem întrebarea „de ce?", solicitând finalități conforme cu concepția noastră despre elementul uman. *„Știința fără conștiință este ruina sufletului"*, scria Rabelais în Pantagruel. Această invitație de a împleti științele „dure" cu științele umaniste este mai actuală ca niciodată. Securitatea cibernetică are nevoie de juriști, sociologi, filozofi, istorici etc. pentru a putea garanta securitatea tuturor în serviciul libertății fiecăruia.

A venit vremea repoziționării elementului uman în centrul discursului și al acțiunii. Cunoaștem faptul că, fără o viziune împărtășită la nivel european, va trebui în curând să alegem între o „libertate supravegheată" și o „securitate supravegheată", în funcție de care vom și „colonizați" dinspre vest sau dinspre est. Este momentul ca Europa să vină cu un proiect politic veritabil care să aibă ca obiectiv asigurarea unei „libertăți securizate", garantă a valorilor împărtășite de cele 27 de state membre. Este un prilej bun pentru a da un imbold transformării digitale mult prea materialiste. Ar fi baza minimală pentru a oferi lumii o alternativă la imperiul în continuă expansiune al celor doi giganți ai lumii digitale. Am pierdut bătăliile din domeniul hardware, software și al platformelor. Putem s-o câștigăm pe cea din domeniul umanului. Nenumărați utilizatori, din Europa, „de la Atlantic până la Urali" și din Africa, așteaptă exact asta. ■



Intensificarea atacurilor cibernetice în contextul pandemiei de COVID-19

Autor: **General Anton Rog**

În contextul generat de răspândirea virusului SARS-CoV-2, în decursul lunii martie a.c., a fost observată intensificarea activităților cibernetice nelegitime îndreptate, inclusiv, împotriva unor instituții ale statului român.

Astfel, actorii cibernetici sunt interesați de lansarea de numeroase campanii de atacuri cibernetice în scopul afectării și/sau indisponibilizării capacității de funcționare a sistemelor acestor instituții, prin exploatarea pandemiei. Cele mai întâlnite tipuri de campanii, în această perioadă, sunt atacurile cu ransomware și cele de tip web defacement.

În cadrul acestor campanii, sunt vizate, cu preponderență, infrastructurile IT&C utilizate și administrate de ministere/instituții guvernamentale, de entități responsabile cu adoptarea de măsuri pentru diminuarea efectelor generate de COVID-19, precum și de companii din sectorul privat din domenii precum: sănătate, educație și cercetare.

Pentru a asigura o rată crescută de succes al acestor activități, atacatorii cibernetici și-au actualizat modul de operare la contextul internațional/național, diversificându-ți tacticile și tehnicile de atac. Aceștia urmăresc distribuirea de malware prin intermediul campaniilor de phishing și/sau spear-phishing, prin care exploatează nevoia generală de informare cu privire la stadiul răspândirii COVID-19, respectiv lipsa de resurse medicale.

De asemenea, pentru a câștiga încrederea victimelor, atacatorii integrează în email-urile/mesajele transmise în cadrul campaniilor de phishing și spear-phishing elemente de impersonare (adrese de email, titluri, conținut de text) specifice unor instituții internaționale și naționale abilitate cu gestionarea situației pandemice.

Amenințarea cibernetică este potențată și de circularea unui număr ridicat de fișiere pe canale neoficiale.

Este de așteptat să crească numărul campaniilor de atacuri cibernetice, pe fondul pandemiei de COVID-19, context în care recomandăm adoptarea unei conduite preventive în mediul online care să includă, neaccesarea email-urilor și documentelor atașate provenite din surse care nu prezintă încredere, utilizarea strict a aplicațiilor legitime și informarea doar din surse oficiale. ■

BIO

General de brigadă Anton Rog, Director Centrului Național Cyberint din cadrul Serviciului Român de Informații (SRI). Cyberint este responsabil pentru desfășurarea 24/7 a activităților de a descoperi, caracteriza și combate proactiv amenințările cibernetice împotriva sistemelor și rețelelor critice pentru securitatea națională a României. Anton Rog a deținut numeroase poziții de dezvoltare tehnică, inclusiv proiectarea de software și sisteme. De asemenea, a fost director adjunct al departamentului central SRI IT & C. Este activ cu comunitatea academică ca profesor asociat la DRESMARA Brașov. Anton Rog a absolvit Universitatea din București în 1998 cu o diplomă de licență B.S. în domeniul tehnologiei informației, iar în 2011 a obținut o diplomă postuniversitară în managementul programelor și al proiectelor de la DRESMARA. A fost desemnat Cavaler al Ordinului Omul și Credința în 2014 și Cavalerul Ordinului Virtuții Militare în 2005 de doi președinți ai României.