redazione@ictsecuritymagazine.com





# Le sfide della Cyber Security e le risposte dell'Unione Europea: il ruolo chiave della ricerca

Pubblicato il 15 dicembre 2017


Quello della cyber security è un settore in fortissima espansione. Il motivo è semplice: aumentano in maniera esponenziale le minacce provenienti dal cyber spazio e, fortunatamente, aumenta anche la consapevolezza da parte dei decision-maker, siano essi del pubblico o del privato, riguardo i rischi derivanti da tali minacce. Il fenomeno, d'altronde, difficilmente potrebbe essere ignorato. Secondo una previsione di Cybersecurity Ventures[1], nel 2021 i costi legati al cyber crime saranno nell'ordine dei 6 **trilioni** di dollari.

Da diverso tempo l'Unione Europea ha intrapreso misure di vario genere per affrontare le minacce provenienti del cyber space, facendo ricorso, tra i vari strumenti, anche a quello del finanziamento alla ricerca. E così, dapprima su iniziativa individuale di alcune specifiche Direzioni Generali (DG) della Commissione Europea (es. DG Home Affairs) e poi in maniera più organica mediante l'inclusione all'interno dei programmi quadro FP6, FP7 ed H2020 (con, nel frattempo, l'adozione della EU Cyber Security Strategy[2]), i policy maker europei hanno messo a disposizione delle organizzazioni pubbliche e private del Vecchio Continente le risorse necessarie per poter sviluppare soluzioni alle principali



ULTIMI ARTICOLI

minacce cibernetiche dell'oggi e del domani. L'obiettivo è quello di creare una capacità di risposta a livello europeo, basata su un ruolo fondamentale esercitato dal settore privato.

Alessandro Zanasi, Presidente di Zanasi & Partners e tra i principali esperti a livello europeo di ricerca in materia di sicurezza e difesa, già membro di ESRAB (European Security Research Advisory Board) ed ESRIF (European Security Research and Innovation Forum) – due comitati di esperti internazionali (indicati dai governi dei vari Paesi membri e nominati dalla Commissione Europea) dedicati a definire le principali minacce alla sicurezza e le risposte da adottare – ci racconta di alcuni dei principali progetti di ricerca in materia di cyber security finanziati dalla Commissione Europea in questi ultimi anni.

## SCADALAB

È sicuramente superfluo ricordare su queste pagine come l'avvento di Internet abbia comportato un'autentica rivoluzione in svariati ambiti. Sorvolando volutamente sulle innumerevoli ripercussioni sugli individui, il crollo dei costi relativi alle comunicazioni ed allo scambio di dati su scala geografica dovuto all'avvento di Internet ha fatto sì che aziende di tutto il mondo si trovassero di fronte alla possibilità di poter operare in maniera remota i propri sistemi di controllo industriale (Industrial Computer Systems – ICS). Tra questi, una delle categorie che ha maggiormente tratto vantaggio dall-avvento della "rete delle reti" è senza dubbio quella dei cosiddetti sistemi SCADA (Supervisory Control And Data Acquisition), responsabili del monitoraggio e del controllo dei sistemi più svariati: dai più semplici macchinari per la produzione industriale, alle più sofisticate ed articolate reti elettriche e sistemi di distribuzione di gas ed acqua.

L'aver aperto questi sistemi di controllo all'accesso via Internet, in alcuni casi in sostituzione di precedenti soluzioni sviluppate ad hoc (e che in quanto tali potevano sfruttare la c.d. "security through obscurity"), ha giocoforza introdotto nuove vulnerabilità, rendendo teoricamente possibile ad attori esterni l'accesso non autorizzato ai sistemi controllati. Stuxnet[3], un malware scoperto nel 2010 che andava ad attaccare il software di controllo (WinCC/Step7) dei PLC responsabili per il funzionamento di specifici tipi di turbine prodotte dalla Siemens ed utilizzate in alcune centrali iraniane (Bushehr e Natanz) per l'arricchimento dell'uranio, rappresenta ancora oggi il più prototipico degli esempi di attacco ad un sistema SCADA. Stuxnet, in grado di infiltrarsi sui sistemi vittima attraverso quattro vulnerabilità 0-day distinte e certificati digitali "rubati", provocava una periodica variazione nella frequenza di funzionamento delle turbine colpite, nascosta all'operatore del software di controllo[4]. Le variazioni in aumento causavano la rapidissima usura delle turbine, rendendone conseguentemente necessaria la continua sostituzione. Quelle in diminuzione provocano invece problemi con il processamento desiderato dell'uranio.[5]

Lungi dall'essersi esaurita nel corso degli anni, la problematica della sicurezza dei sistemi di controllo industriale è ancora estremamente attuale. Nel gennaio del 2017, il Dipartimento dell'Energia statunitense ha pubblicato un report in cui mette in guardia da una minaccia "imminente" alla energy grid USA.[6] Un anno prima, nel 2016, la "Kemuri Water Company", una water utility statunitense (KWC è il nome fittizio utilizzato da Verizon, che ha condotto l'indagine, per mantenerne l'anonimato), è stata vittima di un attacco attraverso il quale ignoti attori hanno preso il controllo di centinaia di PLC che controllano il flusso di elementi chimici tossici utilizzati per il trattamento delle acque.[7] C'erano tutti gli elementi per un disastro, ma fortuna ha voluto che così non fosse.

Tra le varie iniziative proposte a livello europeo per migliorare la protezione dei sistemi di controllo industriale da attacchi di tipo cyber, degno di nota è il finanziamento del progetto di ricerca SCADALAB[8], promosso dalla DG Home attraverso il programma CIPS. [9] Coordinato da INTECO (ora INCIBE, organizzazione facente capo al Ministero dell'Energia spagnolo), il progetto SCADALAB ha permesso la creazione di un "laboratorio" (testbed), accessibile da remoto, dove vengono ricreate fedelmente diverse tipologie di ICS e dove gli utenti possono simulare gli effetti provocati da diverse modalità di cyber attacco al fine di studiare adeguate misure di difesa. L'architettura di riferimento di SCADALAB è visibile in Figura 1, mentre lo schema in Figura 2 riassume le caratteristiche di uno dei vettori di attacco che è possibile testare.

dell'Unione Europea: il ruolo chiave della ricerca


15 dicembre 2017

Intercettazioni del web: la privacy dell'individuo Vs la sicurezza nazionale e comunitaria

14 dicembre 2017

Poteri e obblighi del responsabile del trattamento nel Regolamento generale sulla protezione dei dati

11 dicembre 2017

Il #GDPR: non solo sanzioni amministrative pecuniarie


7 dicembre 2017

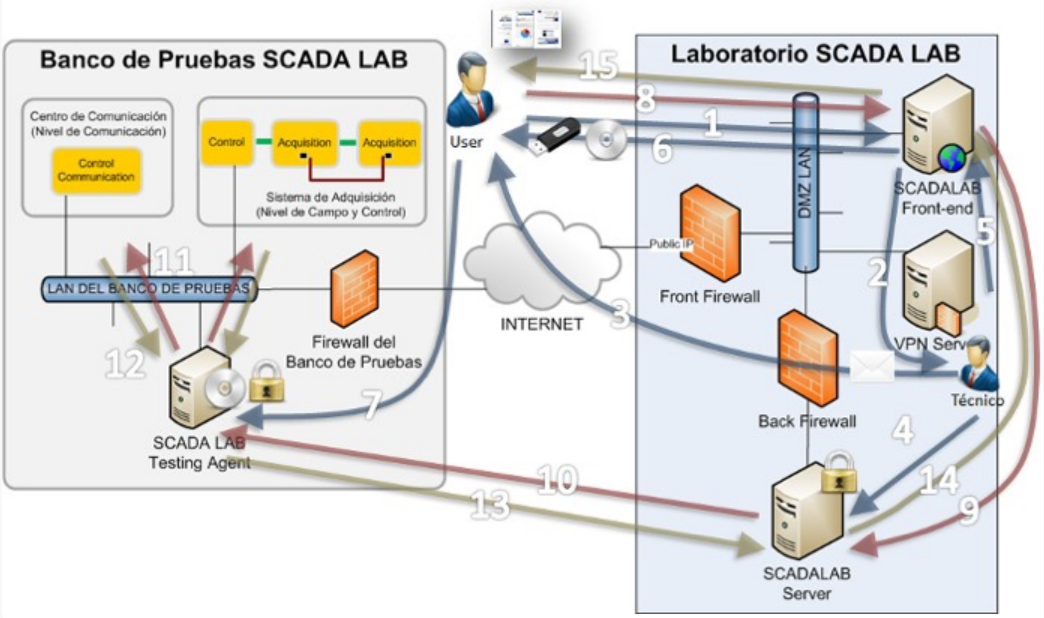


Figura 1. Architettura di SCADALAB.

| TEST | |
|---|---|
| 1.- Test name | 2.- Category/Classification |
| SQL Injection | Program logic flaws |
| 3.- Description | |
| Some malicious SQL code can be executed on the database via legit database access application. | |
| **ASSESSMENT TARGET** | |
| 4.- OSI Layer | 5.- Level of ICS architecture |
| ☒ 7. Application<br>☐ 6. Presentation<br>☐ 5. Session<br>☐ 4. Transport<br>☐ 3. Network<br>☐ 2. Data link<br>☐ 1. Physical | ☒ Control Centre<br>☐ Front End (communications)<br>☒ Field Site |
| 6.- Possible affected components | |
| Database server | |
| **TOOLS** | |
| 7.- Name | 8.- Description |
| Nessus | Remote security scanner performs 6000 security checks against a target system, detecting vulnerable services running on the scanned hosts. |
| Retina | Tool that provides a multitude of vulnerability scanning. |
| SQLmap | Open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. |
| SQLninja | Tool targeted to exploit SQL injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end. |

Figura 2 – SCADALAB: scheda riepilogativa di uno dei test che è possibile effettuare sulla testbed.

## CloudCERT

Per chi si deve occupare di sicurezza, disporre di quante più informazioni possibile è una prerogativa imprescindibile. L'informazione è regina. Il cyber spazio non sfugge a questa regola.

All'interno dell'Unione Europea, deputati a coadiuvare i Paesi Membri nel fronteggiare le minacce cibernetiche sono i CERT (Computer Emergency Response Team) ed i CSIRT (Computer Security

Incident Response Team), presenti nei vari stati (i due termini, CERT e CSIRT, sono spesso utilizzati come sinonimi, per quanto nella comunità della cyber-security non vi sia unanimità di interpretazione[10]). Di natura non necessariamente pubblica, il loro ruolo tipico è quello di monitoraggio rispetto a quanto avviene nel cyber spazio, al fine di poter informare tempestivamente imprese e cittadini riguardo alle principali minacce alla sicurezza. ENISA, l'agenzia europea dedicata alla sicurezza delle informazioni, mantiene un accurato inventario[11] dei CSIRT attivi all'interno dell'Unione Europea, i quali, a giugno 2017, ammontano a 326 unità. Per quanto riguarda il nostro Paese, dal 2014, sotto l'egida del Ministero dello Sviluppo Economico, è operativo il CERT Nazionale Italia[12] (unico, tra i CERT italiani, ad essere parte della CSIRT Network[13] coordinata da ENISA), il quale ha la propria sede presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie.

Uno dei problemi che storicamente affligge i CERT è il fatto che questi tendono spesso a lavorare in isolamento, senza condivisione di informazioni, producendo a livello sistemico una del tutto evitabile moltiplicazione degli effort. Il progetto di ricerca CloudCERT[14], promosso dalla DG Home attraverso il programma CIPS, nasce con l'obiettivo di mitigare questo problema e migliorare l'efficienza dei CERT europei, mettendo a loro disposizione una piattaforma sviluppata al preciso scopo di permettere loro lo scambio sicuro via web di informazioni relative alla cyber security.

Sotto il coordinamento di INCIBE e sulla base di un approfondito studio degli standard più diffusi per la descrizione di cyber minacce e più in generale eventi di cyber security (es. CAIF, EISPP, DAF, OpenIOC, IODEF, VERIS, STIX, ecc.) condotto da Zanasi & Partners[15], il progetto ha portato allo sviluppo di una innovativa piattaforma software per la comunicazione. La piattaforma CloudCERT (uno screenshot è visibile in Figura 3) permette di condividere, tra gli attori autorizzati, cinque diverse categorie di informazioni ("notes", "news", "warnings", "viruses", "vulnerabilities"), andando così a coprire la maggior parte del fabbisogno informativo dei CERT europei.


Figura 3. Screenshot della piattaforma CloudCERT

## SECRET

Le cyber minacce alla sicurezza non passano soltanto attraverso la rete Internet. Un canale di comunicazione particolarmente sensibile è anche quello costituito dall'etere, il quale veicola trasmissioni dati che avvengono attraverso le onde radio e secondo protocolli diversi da quelli che

regolano Internet e le reti di computer. Tali comunicazioni sono di importanza capitale in diversi ambiti, come ad esempio in quello del trasporto ferroviario. L'Unione Europea ha da tempo promosso un programma, chiamato ERTMS (European Rail Traffic Management System)[16], che mira a migliorare l'interoperabilità tra le reti ferroviarie dei diversi Paesi membri, arrivando a creare un unico standard europeo (basato su ETCS, European Train Control System) per quando riguarda i sistemi di segnaletica e di controllo e comando dei treni.

L'ERTMS, nella sua implementazione completa (ETCS livello 3), prevede un vasto numero di componenti, dislocate lungo treni, stazioni ed infrastrutture ferroviarie, che devono poter comunicare tra loro, senza fili, in maniera rapida ed affidabile. Ciò crea una moltitudine di potenziali vulnerabilità che un attaccante potrebbe sfruttare allo scopo di interferire con la circolazione ferroviaria per i fini più disparati.

Il progetto di ricerca SECRET[17], finanziato dalla Commissione Europea nel contesto del Settimo Programma Quadro (FP7), si è focalizzato sullo studio dei possibili effetti provocati da emissioni elettromagnetiche intenzionali (IEMI) indirizzate contro treni ed infrastruttura ferroviaria da parte di attori malevoli, quali potrebbero essere gruppi terroristici e/o organizzazioni criminali. Grazie alla partecipazione di importanti organizzazioni del settore ferroviario e dei trasporti (ALSTOM, SNCF, UIC e la coordinatrice IFSTTAR), coadiuvate da università e centri di ricerca di primo livello, il progetto ha da un lato portato alla luce l'effettiva vulnerabilità di diverse componenti a cyber attacchi operati anche mediante il ricorso a semplici "jammer" commerciali (sia se utilizzati a bordo dei treni, sia lungo i binari), dall'altro ha permesso di elaborare un'ampia serie di raccomandazioni tanto per i produttori di dispositivi ferroviari, quanto per i gestori delle reti ferroviarie ed i policy maker, mirate a migliorare la cyber security posture del sistema ferroviario europeo nel suo complesso.

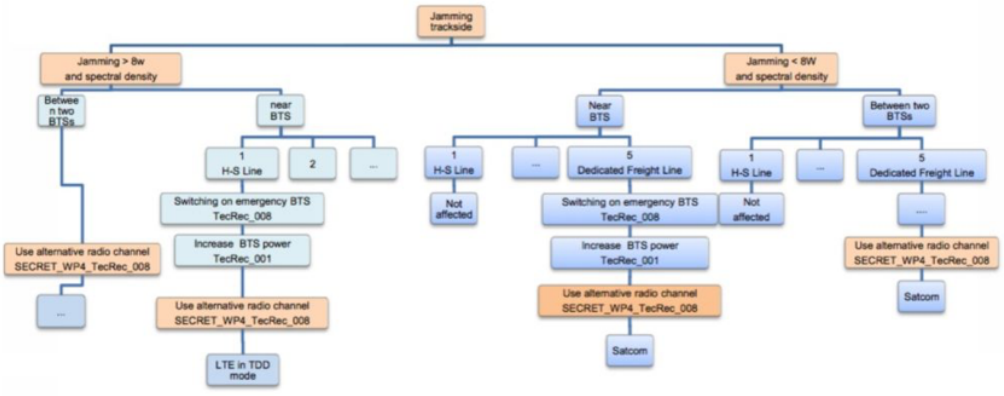


Figura 4. Decision tree relativo alle misure da intraprendere in caso di jamming proveniente dall'esterno del treno.

## iSAR+ e SOTERIA

Strettamente correlato al tema della cyber security è quello della cyber intelligence. La Commissione Europea non è voluta rimanere scoperta sotto questo fronte ed ha finanziato due progetti di ricerca consecutivi, iSAR+ e SOTERIA, entrambi coordinati dalla portoghese TEKEVER, dedicati al tema del monitoraggio dei social media.

Entrambi i progetti muovono dall'assunto secondo il quale, durante situazioni di emergenza (disastri naturali, attacchi terroristici, ecc.), una moltitudine di informazioni potenzialmente utili per i soccorsi viene pubblicata sui social media. Le organizzazioni deputate alla risposta all'emergenza non hanno tipicamente né le risorse sufficienti, né i mezzi necessari per poter attingere a questo patrimonio informativo ed utilizzarlo per rendere più efficace il proprio intervento. Da ciò emerge una duplice necessità: da un lato servono strumenti tecnologici che permettano di analizzare in maniera automatica le informazioni pubblicate sui social media, filtrando quelle irrilevanti e portando l'attenzione dei soccorritori verso quelle potenzialmente utili; dall'altro le organizzazioni che si occupano della risposta all'emergenza necessitano di procedure che permettano di integrare, le informazioni ricevute in maniera "tradizionale" (telefonicamente o mediante appositi canali istituiti con le istituzioni) con quelle attinte da

canali alternativi quali i social media. I progetti iSAR+ e SOTERIA asserviscono esattamente a questi due scopi. In particolare, i due consorzi internazionali coinvolti nella ricerca (costituiti da agenzie di law enforcement, come la Guarda Nacional Republicana portoghese e la North Yorkshire Police britannica, enti specializzati nella gestione delle emergenze, esperti di sicurezza e centri di ricerca) si sono focalizzati sullo sviluppo di innovativi algoritmi di Big Data analytics (data e text mining) per l'analisi automatica dei social media e nell'elaborazione di raccomandazioni per apportare all'interno delle organizzazioni le modifiche procedurali necessarie per poter beneficiare al meglio delle informazioni estratte mediante tali algoritmi.

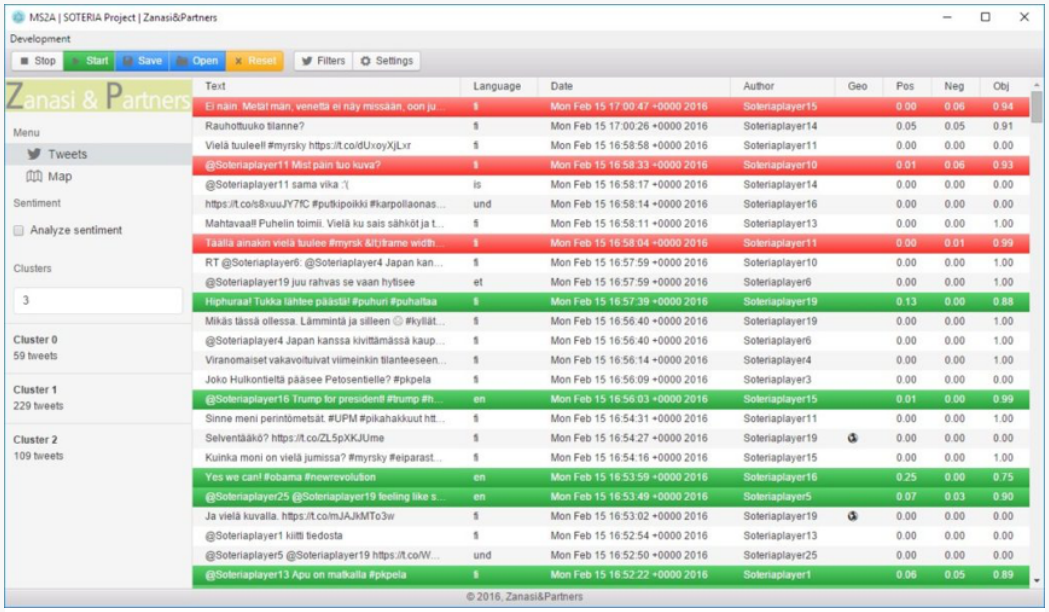


Figura 5. Screenshot di MS2A, un'applicazione sviluppata da Zanasi & Partners durante il progetto SOTERIA, dedicata al clustering ed alla sentiment analysis (multi-lingua) operati su contenuti raccolti da social media.

## Il settore finanziario: la proposta FINSEC

Il settore finanziario, per ragioni immediatamente comprensibili, costituisce da sempre uno dei bersagli preferiti da parte di malintenzionati di qualunque genere.

Prima dell'avvento della finanza, l'unico modo per potersi impadronire di denaro detenuto da un soggetto terzo era quello di sottrarlo fisicamente. Il furto e soprattutto la rapina erano azioni spesso rumorose e vistose, talvolta perfino spettacolari (si pensi alla Great Train Robbery[18] messa in atto da Bruce Reynolds e soci). Con la nascita ed il diffondersi della finanza e soprattutto da quando alla moneta è stata progressivamente tolta la sua "fisicità" fino ad arrivare ad essere una pura e semplice grandezza virtuale, le strategie per impadronirsene in maniera illegale si sono a loro volta evolute. Le eclatanti azioni delinquenziali del passato hanno lasciato il posto a strategie criminali più sofisticate, rapidissime nell'esecuzione (non necessariamente nella pianificazione) e meno vistose, che non richiedono esposizione fisica per essere condotte (essendo il denaro divenuto immateriale), rendendo quindi molto difficile l'identificazione dell'attaccante.

Complice il fatto che banche ed intermediari finanziari, operando in mercati fortemente concorrenziali all'interno dei quali cercano in ogni modo di ritagliarsi un vantaggio competitivo, risultano spesso tra gli "early adopter" delle innovazioni tecnologiche (esponendosi così, spesso, a rischi non debitamente valutati), la situazione è divenuta oramai critica. Un grido d'allarme in tal senso è stato lanciato dal direttore di Europol, Rob Wainwright, il quale di recente ha parlato di un aumento nel livello di sofisticazione dei cyber attacchi tale da "minacciare seriamente parte delle nostre infrastrutture critiche, certamente nei settori finanziario e bancario"[19]. Da un lato gli utenti sono infatti vittime di campagne di phishing sempre più sofisticate e numerose: nel solo 2016, Kaspersky Labs ha individuato 1,06 milioni di attacchi legati al solo settore bancario[20]. Privati e aziende cadono vittime di ransomware sempre più sofisticati (si pensi alle "epidemie" causate da CryptoLocker e WannaCry[21]). Gli ATM

vengono attaccati su base regolare, sia fisicamente sia via software[22]. Le transazioni effettuate on-line risultano spesso vulnerabili a diverse tipologie di attacco[23]. Data breach accadono in continuazione ed in taluni casi i responsabili non si limitano al furto di dati sensibili, ma vanno oltre, utilizzando questi dati per compiere ulteriori illeciti (si veda per esempio quanto successo con il ramo bancario di Tesco, ai cui clienti sono stati complessivamente sottratte circa 2,5 milioni di sterline[24]). I nuovi sistemi di pagamento contactless aprono vere e proprie voragini nel campo della sicurezza[25].

Lo scenario, insomma, è già oggi quantomeno preoccupante[26]. A renderlo ulteriormente complesso si aggiunge poi il tema delle cripto valute, sempre più in auge e con il Bitcoin, prossimo alla sua "naturale" scadenza, pronto ad essere rimpiazzato da valute alternative, anche supportate direttamente dagli Stati nazionali (il Venezuela di Maduro primo tra questi[27]). Una delle maggiori sfide per la sicurezza che attendono l'Europa nei prossimi anni, insomma, è proprio quella di riuscire a rendere il cyber space un luogo sicuro per gli operatori bancari e finanziari, nonché per i clienti, industria e privati, che usufruiscono dei servizi offerti in tale mondo. Una possibile soluzione potrebbe arrivare da un consorzio internazionale che si è riunito attorno alla divisione italiana di GFT, ed ha presentato alla Commissione Europea la proposta per un nuovo progetto di ricerca, chiamato FINSEC. Del consorzio fanno parte industrie di primo piano del mondo dell'IT (es. IBM, HP, Fujitsu, Atos), istituzioni finanziarie (tra le quali Barclays e Liberbank) specialisti della sicurezza e centri di ricerca pubblici e privati. Obiettivo del progetto FINSEC è quello di sviluppare un'architettura di riferimento per la sicurezza, basata su standard innovativi, che permetta agli attori del mondo finanziario la gestione integrata (sia fisica che cyber) della sicurezza. Tale architettura dovrà rendere possibile la tempestiva risposta agli attacchi, contrastando minacce complesse ed i loro effetti a cascata, promuovendo nel contempo la collaborazione tra i diversi stakeholder nel valutare/mitigare il rischio nell'ambito sella supply chain della finanza.

## Cyber war, difesa e futuro: PYTHIA

Quale sarà il futuro della cyber security? Come ricordato anche in questo articolo, quello della cyber security in generale è sicuramente un settore in fortissima ascesa. In uno scenario come quello moderno, caratterizzato da innovazioni che si susseguono ad altissima velocità, risulta tuttavia non immediato riuscire a prevedere quali potranno essere le tendenze tecnologiche del futuro e quindi quale forma potranno assumere le nuove minacce cibernetiche alla sicurezza. Un aspetto sul quale molti esperti concordano è il ruolo preponderante che gli strumenti cyber avranno nel campo della Difesa, sia in ambito strettamente difensivo (per proteggere le informazioni, le comunicazioni ed i mezzi militari), sia quale strumento offensivo (c.d. cyber war).[28]

È specificamente su queste basi che, nel 2017, la European Defence Agency (EDA) ha varato, in collaborazione con la Research Executive Agency (REA, l'organo della Commissione Europea dedicato alla gestione dei finanziamenti alla ricerca), una linea di finanziamenti alla ricerca chiamata Preparatory Action for Defence Research (PADR).[29] Il progetto di ricerca PYTHIA, supportato attraverso tale linea, raccoglie esperti di technology foresight e di big data analytics insieme a diversi Ministeri della Difesa europei (quelli bulgaro, polacco e rumeno partner del consorzio, quelli italiano, greco e belga "supporter" esterni), con il comune obiettivo di sviluppare una metodologia innovativa per poter effettuare previsioni tecnologiche di carattere strategico nel contesto della difesa.

Sarà da iniziative quali PYTHIA che emergeranno gli scenari che caratterizzeranno la futura cyber posture europea in materia di difesa.

## Suggerimenti bibliografici


- INTECO. (2013). *Results of CloudCERT testbed framework to exercise Critical Infrastructure Protection*. Retrieved from http://cloudcert.european-project.eu/docs/results/EC-CLOUDCERT-REP-Dossier_en.pdf
- SECRET project consortium. (2015). *White paper: Security of railways against electromagnetic attacks*. Retrieved from http://www.secret-project.eu/IMG/pdf/white_paper_security_of_railway-against_em_attacks.pdf
- Laudy, C., Ruini, F., Zanasi, A., Przybyszewski, M., & Stachowicz, A. (2017). Using Social Media in Crisis Management. SOTERIA Fusion Center for Managing Information Gaps. In *Proceedings of*

*FUSION 2017, 20th International Conference on Information Fusion* (pp. 1855–1862).

- Zanasi, A. (Ed.). (2007). *Text Mining and its Applications to Intelligence, CRM and Knowledge Management*. Southampton, UK: WIT Press.
- Garcia, A., Velasco, C., Zamalloa, E., Velasco, E., Elejabarrieta, I., Lotero, J., … Schuster, S. (2014). *Mass Surveillance. Part 1 – Risks and opportunities raised by the current generation of network services and applications*. Retrieved from http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA Study Mass Surveillance Part 1.pdf

## Note

[1] https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[2] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[3] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[4] https://www.computerworld.com/article/2514314/security0/new-stuxnet-clues-suggest-sabotage-of-iran-s-uranium-enrichment-program.html

[5] https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[6] https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment

[7] http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report

[8] https://www.certsi.es/blog/scadalab-seguridad-ics

[9] https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks_en

[10] https://cybersponse.com/the-difference-between-certs-and-csirts-what-are-they

[11] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[12] https://www.certnazionale.it

[13] https://www.enisa.europa.eu/topics/csirts-in-europe

[14] http://cloudcert.european-project.eu

[15] http://www.zanasi-alessandro.eu

[16] http://www.ertms.net

[17] http://www.secret-project.eu

[18] https://en.wikipedia.org/wiki/Great_Train_Robbery_(1963)

[19] https://www.reuters.com/article/us-germany-telecoms/german-regulator-urges-broadband-build-out-readies-5g-spectrum-idUSKBN1DY0TV

[20] http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-in-the-banking-industry/#gref

[21] https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

[22] https://www.europol.europa.eu/sites/default/files/documents/public_-

_cashing_in_on_atm_malware.pdf

[23] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

[24] https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m

[25] http://www.dailymail.co.uk/news/article-3849368/Could-fall-prey-contactless-conman-thieves-money-card-walking-street.html

[26] http://www.information-age.com/value-sharing-threat-intelligence-123464586/

[27] https://www.cnbc.com/2017/12/03/venezuela-is-launching-a-cryptocurrency-backed-by-oil-gas-gold-and-diamonds.html

[28] http://www.tandfonline.com/doi/full/10.1080/01402390.2012.730485?scroll=top&needAccess=true

[29] https://www.eda.europa.eu/what-we-do/activities/activities-search/preparatory-action-for-defence-research

A cura di: **Alessandro Zanasi**

Bio

Laureato in Ingegneria Nucleare ed in Economia, Alessandro Zanasi inizia la sua carriera come ufficiale dei Carabinieri addetto al Centro Investigazioni Scientifiche. Decide poi di passare al settore privato, lavorando dapprima come IBM executive in Italia, a San Jose (USA) ed a Parigi e poi ricoprendo il ruolo di responsabile IBM Intelligence in Sud Europa, Medio Oriente ed Africa. Docente di Data/Text Mining e Tecniche di Intelligence alle Università di Bologna e Parigi, nel 2000 è co-fondatore di TEMIS SA (società specializzata in text mining - con sedi a Modena, Parigi, Grenoble, Heidelberg, Washington - ora confluita in Expert System). Dal 2005 membro Italiano dei comitati ESRAB ed ESRIF presso la Commissione Europea. Nel 2007 fonda Zanasi & Partners (Z&P), con la quale partecipa ad oltre 20 progetti di ricerca in sicurezza e difesa finanziati dalle istituzioni europee, inclusi tutti quelli descritti all'interno di questo articolo.

Scarica il PDF

Condividi sui Social Network:

## Ti potrebbe interessare



Intercettazioni del web: la privacy dell'individuo Vs la sicurezza nazionale e comunitaria

Poteri e obblighi del responsabile del trattamento nel Regolamento generale sulla protezione dei dati

Il #GDPR: non solo sanzioni amministrative pecuniarie

La Prima Rivista Dedicata alla Sicurezza Informatica

## ICT Security

La rivista che da oltre 10 anni offre informazione, aggiornamento e riflessioni sui temi della sicurezza informatica.

redazione@ictsecuritymagazine.com

## Rubriche

- Biometria e Firme Elettroniche
- Cloud Security e IoT
- Cyber Risk
- Digital Forensic
- Gestione Sicura di Dati e Documenti
- Normativa e Privacy

## Ultime Notizie

Previsioni e trend 2018 – Le novità in ambito cybersecurity

15 dicembre 2017

Email Security – La tecnologia italiana Libra ESVA tra i migliori sistemi di protezione e analisi dei contenuti della posta elettronica al mondo

20 novembre 2017