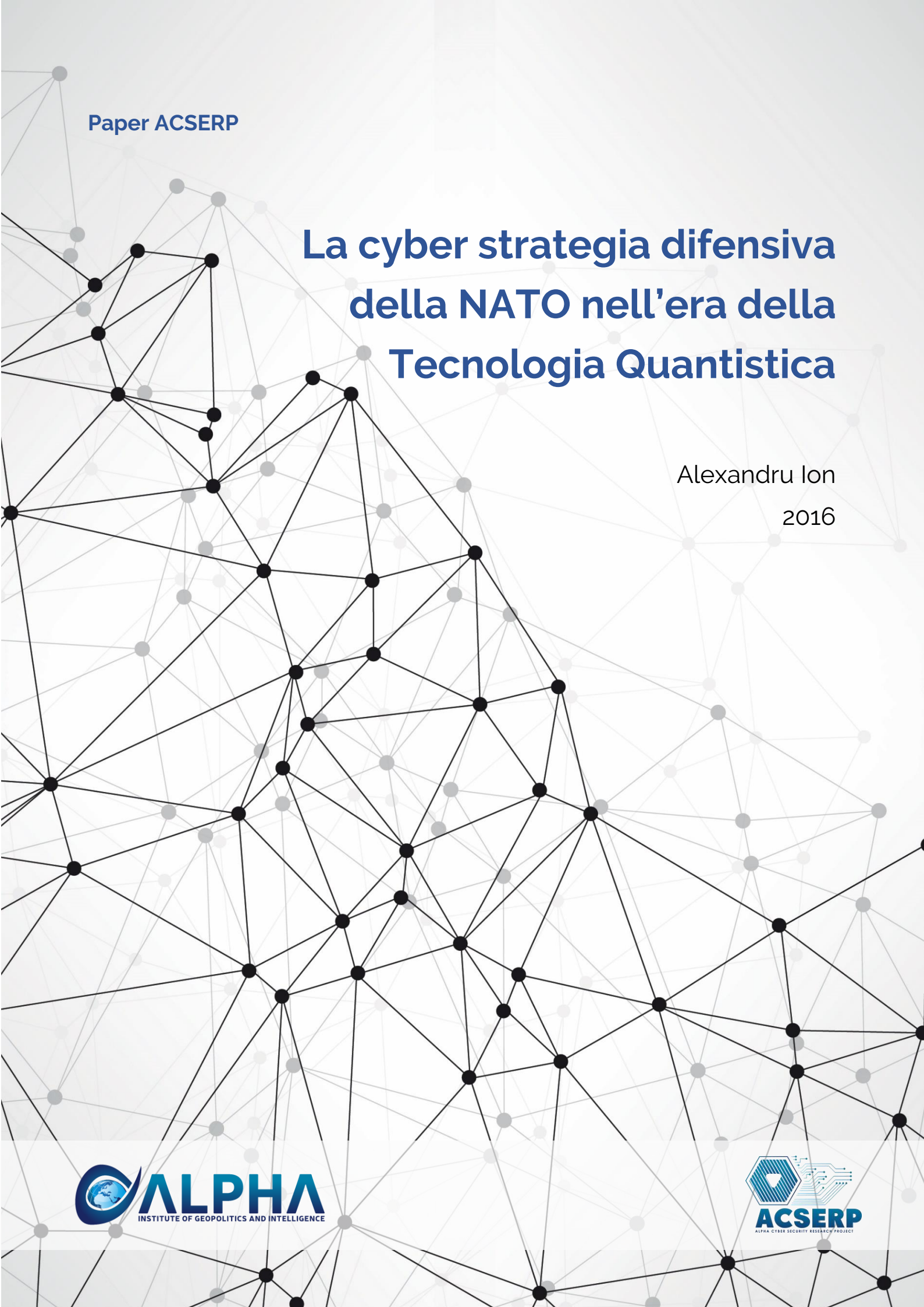
Paper ACSERP

La cyber strategia difensiva della NATO nell'era della Tecnologia Quantistica

Alexandru Ion

2016



ALPHA INSTITUTE OF GEOPOLITICS AND INTELLIGENCE

ACSERP
ALPHA CYBER SECURITY RESEARCH PROJECT

The Alpha Institute of Geopolitics and Intelligence
Paper ACSERP - Alpha Cyber Security Research Project

Roma, Giugno 2016

The Alpha Institute of Geopolitics and Intelligence

ACSERP
Alpha Cyber Security Research Project

La cyber strategia difensiva della NATO nell'era della Tecnologia Quantistica

Alexandru Ion

2016

(Traduzione di Antonino Santoro)

Contenuti

Abstract

La mia ricerca abbraccia un'area multi disciplinare delle relazioni internazionali e degli studi sulla sicurezza riguardo la strategia difensiva della NATO in relazione all'imminente minaccia dei nuovi processori quantistici. Il lavoro si concentra su importanti questioni che cambieranno il cyber spazio facendoci ripensare la progettazione della nostra cyber sicurezza. Lo sviluppare nuovi tipi di criptaggio avrà un grande ruolo nella protezione delle nostre informazioni nell'utilizzo di tutti i mezzi di comunicazione.

Keywords: computer quantistici, cyber sicurezza, NATO, crittografia

Introduzione

Dal momento che la tecnologia odierna sta progredendo sempre più velocemente, ci troviamo ad affrontare ogni giorno sfide sempre più grandi provenienti da internet. In tutto il mondo abbiamo attualmente una popolazione totale di 3.366.261.156 utenti che usano internet quotidianamente su piattaforme multiple (Internet World Stats 2016). Sotto queste circostanze, la protezione della nostra privacy è l'obbiettivo principale del nostro governo e di organizzazioni internazionali quali la NATO. Attraverso la collaborazione internazionale degli ultimi anni, centinaia di gruppi di hacker e di siti internet maligni sono stati chiusi facendo, tuttavia, ben poca differenza se paragonati con l'attività sommersa di internet. Con l'evoluzione dei computer, fermare i cyber attacchi sta diventando ogni giorno sempre più difficile.

L'innovativa teoria quantistica ha il potenziale per elaborare informazioni 100 milioni di volte più velocemente rispetto ai vecchi super computer e questo cambierà la nostra attuale visione sul mondo rendendo le nostre vite molto più semplici (D-wave 2015). Ma insieme alla rivoluzionaria tecnologia nel cyberspazio arriva anche un nuovo pericolo dato che, come suggeriscono molti esperti di cyber security, le informazioni criptate diventano molto più vulnerabili alla nuova potenza di decriptaggio del processore quantistico (Naughton 2015). Anche se questa nuova tecnologia è ancora in via di sviluppo e solo poche compagnie vi hanno accesso, principalmente a causa del suo costo, in pochi anni essa si diffonderà largamente a livello mondiale proprio come gli odierni personal computer (Akama 2015, pp. 1-2). Al momento non è disponibile alcun software per poter testare le reali performance della tecnologia quantistica, ma la NATO dovrebbe fare di ciò una priorità sviluppando un software di sicurezza che possa resistere ai cyber attacchi di questo nuovo tipo di processori.

Come abbiamo visto negli scorsi anni gli obsoleti software di sicurezza hanno reso i computer vulnerabili agli attacchi: Rocra, Mini Duke, Turla sono solo alcuni dei casi in cui negli ultimi anni data server nazionali hanno affrontato delle azioni malware

note come cyber-spying (Monografia SRI 2015, p. 328). Perdere questo genere di informazioni a favore di paesi stranieri significherebbe perdere anni di lavoro sulla ricerca e sviluppo di dati militari e governativi.

Analisi sulle cyber minacce odierne

Per comprendere meglio il pericolo che affronteremo una volta che i computer quantistici saranno disponibili in tutto il mondo, dobbiamo capire gli attuali problemi relativi alle strategie di cyber difesa. Se analizziamo le statistiche sui cyber attacchi dello scorso mese, Gennaio 2016, scopriamo che il 60% aveva un movente cyber-criminale, il 27% sono stati casi di hacktivismo mentre per il restante 13% si è trattato di casi di cyber spionaggio e cyber war. Gli obbiettivi di tali attacchi sono: al primo posto troviamo le industrie col 22%, al secondo posto i governi col 17% mentre per il 10% dei casi sono singoli individui (Hackmaghedon 2016). E questi sono solo i casi che sono stati documentati. Ci sono molte più vittime di cyber attacchi che restano ignare degli attacchi fino a diversi mesi dopo.

Fornire una soluzione economica alle cyber violazioni dei dati porterebbe sempre più persone ad utilizzarle dato che molti dei computer governativi, a causa di limiti di bilancio, usano software obsoleti (Cidon 2016). La Symantec Corporation ha rilasciato nell'aprile 2015 un report sull'e-crime comparando il tasso del crimine online del 2013 con quello del 2014. Questa panoramica generale ci mostra che l'aumento annuale delle minacce su internet sta diventando una seria preoccupazione per la sicurezza sia del settore pubblico che di quello privato. Più di 317 milioni di nuovi malware sono stati creati nel 2014 e si sono verificate 312 violazioni in server di informazioni: si tratta del 24% in più rispetto a quanto avvenuto nel 2013 con 252 milioni di malware e 253 violazioni (Internet Security Threat Report 20 2015, pp. 88-90). Se prendiamo in considerazione le statistiche possiamo stimare che entro il 2020 avremmo su internet circa 1 miliardo di nuovi tipi di malware e approssimativamente 1000 mage-violazioni sui server pubblici e privati. Questi dati si applicano tuttavia solo per la attuale generazione di computer basati su processori in silicio.

Se ogni cittadino avesse a disposizione un computer quantistico ci troveremmo ad avere il bisogno di riprogettare il criptaggio delle nostre comunicazioni private. Uno dei primi problemi della futura potenza nel processare informazioni con la tecnologia quantistica sarà quello dell'efficienza della Advanced Encryption Standard 128 o anche la 256 bit key fino ad oggi irraggiungibile ma che non sarebbe più considerata come un criptaggio sicuro (Arora 2012). L'NSA ha confermato che la minaccia riguardo i computer quantistici è reale e rappresenta un incombente pericolo a lungo termine (Simonite 2016). Per conservare la segretezza su internet

risulta vitale elaborare un nuovo algoritmo di criptaggio capace di resistere multipli attacchi quantistici.

No.	Processore Quantistico	Tipo di criptaggio
1	D-wave 1 (2^{128} possibilities per instance)	AES 128 (2^{128} possibilities)
2	D-Wave 2 (2^{512} possibilities per instance)	AES 192 (2^{192} possibilities)
3	D-Wave 2X (2^{1000} possibilities per instance)	AES 256 (2^{256} possibilities)

Comparazione dell'evoluzione dei processori quantistici con le odierne chiavi di criptaggio.

Delineazione dei metodi per rispondere ai cyber attacchi quantistici

Gli attuali metodi utilizzati per proteggere i nostri dati saranno inefficienti con l'introduzione dei computer quantistici e questo significa che dovremo riprogettare i nostri modi di difenderci nel cyber spazio alla luce del fatto che nessuno sarà immune. Finanziare progetti di ricerca con le università sarebbe un importante passo per trasformare le idee teoriche in pratici metodi di sicurezza capaci di resistere ai nuovi cyber attacchi quantistici.

Uno dei modi per reagire ai computer quantistici sarebbe quello di introdurre un nuovo codice di criptaggio per proteggere i nostri dati. Basati sulla nuova generazione di cyber criptaggio come "Quantum key distribution" e "Honey Encryption" (Simonie 2014) vi sono nuove possibilità nelle quali possiamo progettare i nostri cyber algoritmi per renderli impenetrabili (Dillow 2013). Il progettare un criptaggio simile al metodo delle "sabbie mobili" dove quando viene applicata una forza bruta, esso reagisce fornendo una ulteriore protezione sufficiente a scoraggiare gli hacker. Per ogni tentativo fallito, l'aggiungere una ulteriore nuova protezione alla chiave renderebbe, senza dubbio, questo algoritmo più complicato di quelli convenzionali. Non esistono meccanismi di sicurezza capaci di resistere agli hacker per sempre ma, tuttavia, progettare una soluzione impenetrabile per i prossimi 5 anni sarebbe un buon inizio.

Sviluppare una forte partnership tra il settore aziendale e quello pubblico basata su una cooperazione è una delle chiavi fondamentali del futuro. Riunire alcune delle più lodate aziende sulla cyber sicurezza per discutere le priorità ed implementare i cambiamenti nei sistemi di difesa sono considerate questioni urgenti. Come ho già sottolineato nell'ultimo capitolo, l'avere una soluzione economica riguardo la cyber difesa significa che essa verrebbe utilizzata da sempre più persone. Nel far questo è importante mirare allo sviluppo di metodi settoriali di sicurezza e poi concentrarsi su aspetti generali.

Conclusioni

Vi sono molte minacce nel mondo attuale che la NATO deve affrontare ma nessuna è più pericolosa del combattere contro un nemico sconosciuto attraverso il cyber spazio e, per far questo, essa deve essere sempre preparata. Durante gli ultimi due anni per la NATO i cyber attacchi in Estonia, Georgia e Ucraina sono state da lezione di ciò che significa avere una grande capacità difensiva per situazioni non previste. L'esplorare nuove possibilità, il simulare e l'imparare da tali eventi può fornirci un esauriente feedback.

Con il lancio del nuovo processore quantistico D-ware 2X nel 2015, noto anche come il computer più veloce al mondo, le compagnie e le istituzioni, quali Google, la NASA, Lockheed, Martin, USRA e l'Università del Sud Carolina hanno confermato di stare utilizzando il computer per scopi interni (D-wave 2015). La lista continuerà a crescere ogni anno a causa delle tecnologie sempre più innovative che vengono utilizzate e tali istituzioni e compagnie inizieranno probabilmente a sviluppare appropriati software. La NATO dovrebbe essere la prima organizzazione internazionale a sviluppare una adatto criptaggio prima che si verifichi il primo attacco quantistico.

Nel mio lavoro ho fornito alcune soluzioni che possono essere applicate per rispondere all'attività cyber criminale proveniente da internet. Vi sono molte altre iniziative atte a migliorare il nostro cyber sistema difensivo nell'Era Quantistica, come il tenere annuali conferenze o il pubblicare lavori sull'argomento, che aiuteranno senz'altro a far nascere nuove strategie. Per il momento spero di aver contribuito con le mie idee ad aiutare la NATO a trovare nuovi modi per sviluppare la strategia difensiva nel cyber spazio.

Alexandru Ion
PhD Student at the Faculty of Political Science, University of Bucharest, Romania
ion.alexandru@fspub.unibuc.ro

Bibliografia:

AKAMA, Seiki, *Elements of Quantum Computing: History, Theories and Engineering Applications*, Springer, 2015

Joan DAEMEN, Vincent RIJMEN, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, Bruxelles, 2013

GENNARO, Rosario, Matthew ROBSHAW, *Advances in Cryptology -- CRYPTO 2015: 35th Annual Cryptology Conference 2015*, Springer, Santa Barbara, 2015

Internet Security Threat Report 20, Symantec Corporation, 2015

James M. Kaplan, Tucker Bailey, Derek O'Halloran, Alan Marcus, Chris Rezek, *Beyond Cybersecurity: Protecting Your Digital Business*, Wiley Publishers, Hoboken, 2015

Monografia SRI, Editura RAO, Bucuresti, 2015

TAKAGI, Tsuyoshi, *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016*, Springer, Fukuoka, 2016

Siti web:

Asaf Cidon, Info security Magazine, *Government Security and Data Breaches: Problems and Solutions*, 2016. Available from: <http://www.infosecurity-magazine.com/opinions/government-security-data-breaches/>. [16 February 2016]

Clay Dillow, Fortune, 2013, *Unbreakable encryption comes to the U.S.* Available from: <http://fortune.com/2013/10/14/unbreakable-encryption-comes-to-the-u-s/>. [15 February 2016]

D-wave, 2015, *Customers*. Available from: <http://www.dwavesys.com/our-company/customers>. [15 February 2016]

D-wave, 2015, *Introduction to the D-Wave Quantum Hardware*. Available from: <http://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware>. [2 February 2016]

Hackmageddon, *Motives behind the attacks*, 2016, Available from: <http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/>. [16 February 2016]

Internet World Stats, 2016. Available from: <http://www.internetworldstats.com/stats.htm>. [1 February 2016]

John Naughton, The Guardian, 2015, *The quantum computing era is coming… fast*. Available from: <http://www.theguardian.com/commentisfree/2015/dec/13/the-quantum-computing-era-is-coming-qubits-processors-d-wave-google>. [2 February 2016]

Mohit Arora, EE Times, 2012, *How secure is AES against brute force attacks*?. Available from: <http://www.eetimes.com/document.asp?doc_id=1279619>. [14 February 2016]

Tom Simonite, MIT Technology review, 2016, *NSA Says It "Must Act Now" Against the Quantum Computing Threat*. Available from: <https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat/>. [18 February 2016]

Tom Simonite, MIT Technology review, 2014, *"Honey Encryption" Will Bamboozle Attackers with Fake Secrets*. Available from: <https://www.technologyreview.com/s/523746/honey-encryption-will-bamboozle-attackers-with-fake-secrets/>. [15 February 2016]