

## **La difficile situazione della cyber-security nei paesi ASEAN**

Cyber-terrorismo, crimine e frodi informatiche sono l'effetto secondario dei cambiamenti introdotti dallo sviluppo tecnologico. C'è una connessione naturale tra la tecnologia, la sua diffusione e il crimine informatico e tale connessione è tanto più evidente se lo sviluppo tecnologico brucia le tappe, come discusso da molti analisti (possiamo citare, ad esempio, alcune pubblicazioni RAND)<sup>1</sup>. Alcuni paesi in via di sviluppo hanno avuto un rapido aumento dell'utilizzo della tecnologia negli ultimi decenni e un parallelo aumento dei crimini informatici.

La comunità economica di ASEAN, denominata AEC (Asean Economic Community), è un interessante caso di studio per osservare lo sviluppo economico / lo sviluppo tecnologico / l'aumento della criminalità informatica dal 2010 ad oggi. AEC consente ai paesi membri l'opportunità di avere un mercato più ampio per lo sviluppo e la vendita delle produzioni, ma offre altresì un ambiente tecnologico più ampio per mettere in atto frodi informatiche. Cercherò di esaminare la situazione del rischio informatico connesso allo sviluppo economico nei paesi importanti AEC: Indonesia, Filippine, Myanmar, Thailandia e Singapore.

L'Indonesia è uno dei paesi più influenti del ASEAN e del AEC. Il suo PIL è aumentato del 5,02% lo scorso anno (2016)<sup>2</sup>, contro il 4,88% nel 2015, come riportato dall'Agenzia centrale di statistica (BPS)<sup>3</sup>. In generale, negli ultimi 17 anni (dopo la crisi economica regionale 1997-1998), l'Indonesia ha avuto una crescita del PIL tra il 3,6% e il 6,3% ma le politiche energetiche e le politiche di sostenibilità hanno avuto problemi nel seguire il ritmo dell'incremento.<sup>4</sup> Una valutazione generale della sicurezza informatica mostra un aumento chiaro, drammatico ed esponenziale degli attacchi, specialmente nel 2015 e nel 2016. I cyber-attacchi si sono concentrati soprattutto verso le famiglie della classe media (urbana), causando perdite straordinarie anche per il mercato e il consumo.

La minaccia è aumentata a tal punto che il governo ha ritenuto necessario istituire una nuova «agenzia nazionale di cyber-sicurezza»<sup>5</sup> in febbraio, da implementare nel quadro della sicurezza nazionale. L'agenzia è stata finalmente istituita da un regolamento presidenziale in maggio.

Le Filippine di Rodrigo Duterte, dal 2000, hanno avuto un valore altalenante del PIL. La crescita è stata un impressionante 7,6% nel 2010 e 7,1% nel 2013, mentre nel 2009 è stata solo 1,1%. Il nuovo presidente, eletto circa un anno fa, ha visto un aumento positivo del 6,9% del PIL nel suo primo anno (2016) di governo, mentre la tecnologia informatica si è diffusa in tutte le isole (soprattutto nell'area settentrionale). Il settore finanziario è uno dei più influenzati "dall'esplosione informatica" nelle Filippine. L'industria del *Business Project Management* (BPM) ha impiegato circa 1,3 milioni di persone e ha generato 25 milioni di dollari di profitti nel 2016.<sup>6</sup>

---

1 Cfr. Lynn E. Davis, *Globalization's Security Implications*, in "Issue Paper" 2003, Santa Monica, RAND, consultato on-line a: [https://www.rand.org/content/dam/rand/pubs/issue\\_papers/2005/IP245.pdf](https://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP245.pdf) il 17 agosto 2017.

2 Per i dati economici riguardanti la crescita del PIL vedi: <https://tradingeconomics.com> consultato on-line il 9 settembre 2017.

3 Cfr. Grace D. Amianti, *Indonesian economic growth accelerates to 5.02%*, in "The Jakarta Post" 29 agosto 2017, consultato on-line at: <http://www.thejakartapost.com/news/2017/02/06/indonesian-economic-growth-accelerates-to-5-02.html> il 29 agosto 2017.

4 Cfr. Ertugurul Yildirim, Deniz Sukruoglu, Alper Aslan, *Energy consumption and economic growth in the next 11 countries: The bootstrapped autoregressive metric causality approach*, in "Energy Economics", volume 44, luglio 2014, pp.14-21.

5 Cit. Prashanth Parameswaran, *Is Indonesia ready for a new Cyber Agency?*, in "The Diplomat" 11 febbraio 2017, consultato on-line a: <http://thediplomat.com/2017/02/is-indonesia-ready-for-new-cyber-agency/> il 29 agosto 2017.

6 Cfr. Yna C. Quiambao, *Philippines - Information and Communications Technology*, in "Export.gov", consultato on-line a: <https://www.export.gov/article?id=Philippines-Information-and-Communications-Technology> il 18 agosto 2017.

Anche in questo caso i cyber-attacchi hanno causato enormi danni al settore finanziario e commerciale, con una perdita di ricavi di milioni di dollari USA. Nonostante la situazione sia critica, l'esecutivo delle Filippine non dispone ancora di una rete organizzata di *cyber-security* e non è ancora orientato ad affrontare la minaccia in maniera diretta.

Myanmar sta uscendo in questi anni da un lungo periodo di governo militare che dura dal 1962. Il paese sta contemporaneamente passando ad una economia capitalista ed è un nuovo arrivato nell'economia di mercato, particolarmente interessato al turismo. La crescita del PIL in Birmania ha registrato dati notevoli dal 2000. Se pensiamo che la crescita peggiore è stata quella del 2011 con un abbondante 5,6%, non possiamo essere impressionati dal 13,7% nel 2000 e dal 13,8% nel 2003. Anche in questo caso l'impiego dell'IT è cresciuto in parallelo con l'economia ad un impressionante ritmo. I cyber-attacchi in questo paese sono diventati importanti nel 2005 e da quel momento sono aumentati drammaticamente, creando una situazione davvero complessa. Il governo di Myanmar sta cercando di contrastare il fenomeno con la nuova legge contro il terrorismo, ma non ha ancora implementato una specifica risposta alla minaccia *cyber*.<sup>7</sup>

Arrivando alla Thailandia, dove la crisi economica del 1997-1998 ha sconvolto l'economia, possiamo notare una situazione veramente instabile, abbiamo avuto picchi negativi nel 2009, 2011 e 2014 e una crescita di circa il 6,8%, ma mai superiore al 7,2%. Bangkok ha visto una diffusione dell'informatica meno "esplosiva" rispetto agli esempi precedenti, fondamentalmente per due fattori: lo sviluppo economico thailandese è stato meno sicuro rispetto alle altre situazioni esaminate e con una diffusione tecnologica a macchia di leopardo, più consistente nelle aree turistiche (città, coste e parte settentrionale il paese). In Thailandia, il crimine informatico sembra ancora allo stato embrionale.<sup>8</sup> Anche se la crescita della minaccia *cyber* è divenuta importante, la Thailandia è ancora il 72° paese nel mondo per il numero di utenti connessi.

Alla fine esaminiamo Singapore: Questo HUB internazionale ha tradizionalmente avuto uno sviluppo economico paragonabile agli Stati occidentali. Questo paradigma di sviluppo ha causato una introduzione IT lenta e più sostenibile. A Singapore gli attacchi informatici sono generalmente rivolti ai mercati finanziario alla raccolta d'informazioni, come i due avvenuti nell'ottobre 2016 alla banda larga di Starhub, o come gli attacchi dimostrativi del 2013.<sup>9</sup> Anche se le autorità di Singapore hanno la necessità di potenziare le agenzie di sicurezza, il paese parte da un background già coerente, grazie ad un'economia consolidata, dando l'opportunità ad una risposta migliore, più solida e più coordinata fra le varie agenzie.

### **Analisi, valutazioni e previsioni**

Dall'esame del caso ASEAN possiamo concludere che il rischio di cyber-attacchi, ed un più generale rischio conseguente all'uso sbagliato della rete, è generalmente collegato al veloce sviluppo tecnologico così come alla disomogenea distribuzione delle risorse economiche e tecnologiche. Gli stati devono affrontare questa situazione perseguendo adeguati progetti di *cyber-security*. Una forte politica di *cyber-security* viene tendenzialmente esercitata da Indonesia e Singapore ma dovrebbe essere certamente introdotta in tutta l'ASEAN, organismo fortemente interconnesso.

---

7 Cfr. Editor, *Many PH firms unprepared for cyber attacks* – SGV, in "Rappler" 17 marzo 2017, consultato on-line at: <https://www.rappler.com/business/164503-global-information-security-survey-2017> , il 1 settembre 2017.

8 Cfr. Staff, *Kaspersky report nearly 62,000 cyberattacks in Thailand in second quarter of 2017*, in "Thaitech", consultato on-line a: <https://www.tech.thaivisa.com/kaspersky-report-nearly-62000-cyber-attacks-thailand-second-quarter-2017/23490/> il 3 settembre 2017.

9 Cfr. Staff, *'Anonymous' hack Singapore newspaper's website*, in "BBC" 1 novembre 2013, consultato on-line a <http://www.bbc.com/news/technology-24768053> , il 9 settembre 2017.

Un secondo importante punto da considerare è l'accessibilità alla rete che, in molti casi nell'area ASEAN, è stata frettolosamente garantita a larghi strati della popolazione come un "bisogno indotto".

L'utilizzo di internet da parte di classi sociali non adeguatamente preparate può portare a comportamenti devianti e superficiali che espongono alla minaccia *cyber*, come si evidenzia per Thailandia e Filippine. In generale questo mette in luce la necessità di una migliore educazione ai rischi di cyber-attacchi che proceda di pari passo con lo sviluppo economico in particolare laddove il ritmo di tale sviluppo è molto elevato.