Why do we need a cyber-intelligence capacity?

Miguel De Bruycker

December 2014

Cyber Intelligence

What information about us can be collected openly?

What are our vulnerabilities in cyberspace?

Could someone get access to my private data?

Cyber Intelligence

What information about someone else can be collected openly?

What are their vulnerabilities?

Could I get access to their systems?

Cyber Intelligence

Who is developing what kind of
cyber capabilities?

What are their intentions?

What is the cyber threat to me?

Knowing the threat

Knowing the threat

©BELGA

De spionagesoftware waarmee telecombedrijf Belgacom gehackt werd, is geïdentificeerd. De spyware heet 'Regin' en is van Amerikaanse makelij. Dat blijkt uit gezamenlijk onderzoek van De Standaard, NRC Handelsblad en de Amerikaanse nieuwssite The Intercept.

Knowing the threat

Invisible Russian cyberweapon stalked US and Ukraine since 2005, new research reveals

Sophisticated 'Snake' malware discovered

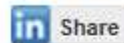By John E Dunn | Techworld | Published: 13:04, 07 March 2014

Knowing the threat

Increasing Sophistication of Iranian Attack Tactics Has Striking Similarities With How Chinese Hacker Groups Have Evolved

Knowing the threat

Hackonomics: 'Cyber Black Market' more profitable than illegal drug trade

Summary: OPINION: A new report by RAND commissioned by Juniper Networks has some eyebrow-raising conclusions about the black market for hacks, cracks, data theft, botnets, and zero days.

By Violet Blue for Zero Day | March 26, 2014 -- 11:24 GMT

Follow @violetblue   Get the ZDNet Security newsletter now

There is an army of thousands of hackers and techniques on Darknet
Attacks, exploits, vulnerabilities, are for sale …. What's next ?

Knowing the threat

Credible Threat: Terrorist Plan Major Cyber Attack

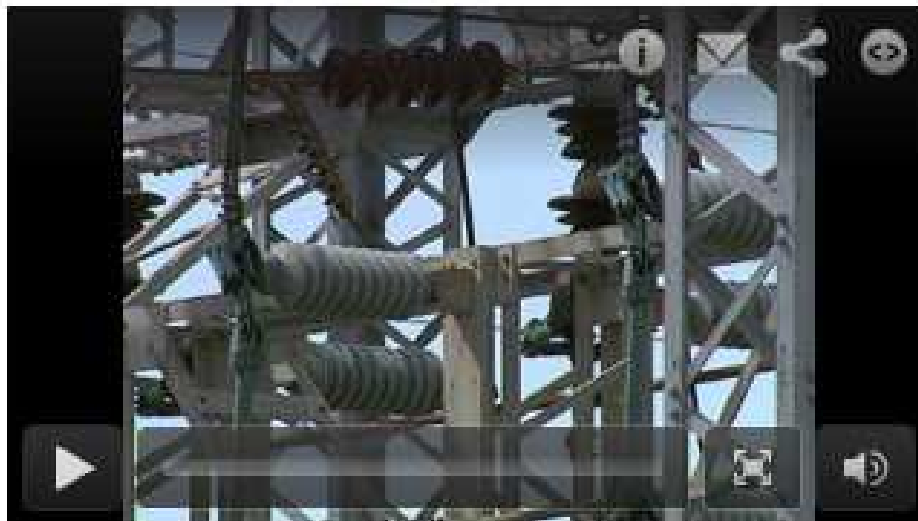| CBNNews.com	Sunday, July 27, 2014

SHARE | Vind ik leuk 17 | Tweet 15 | 8+1 0 | Print 8 Comment(s)

Islamic terrorists, criminals and some countries are getting ready for major cyber-attacks against the United States, according to senior Justice Department officials.

Speaking at the annual Aspen Security Forum in Aspen, Colorado, officials warned that terrorists have openly said they're planning to use electronic attacks to do as much damage as possible to U.S. infrastructure, the *Washington Free Beacon* reported.

Knowing the threat

Cyber sabotage: the new world war?

Given the reliance on technology in today's business environment and the vulnerability of the large volumes of data stored on enterprise networks and in the cloud, cybersecurity has rightfully become a major concern for businesses.

In the US, Defence Secretary Leon Panetta has warned of a 'cyber Pearl Harbour'. As this article was being written, hackers infiltrated the Twitter account of the Associated Press and sent a fake tweet with terror overtones, which caused US financial markets to fluctuate wildly for several minutes. This serves as a sobering example of the domino effect a cyber attack can have and the tenuous nature of our technologically connected world.

http://www.nexia.com/Cybersabotagethenewworldwar

Convinced ?
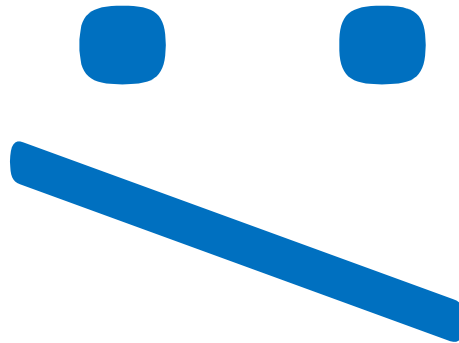
This looks like a Kalashnikov…

Incidents.be

- There are counterparts with advanced capabilities

- Information about the attack method was available in partner services, but …

- Intrusions remain undetected

  - No detection by standard commercial products

  - Present for a long time before detection

- The counterpart has full access

The threat is real, but

is this threat real to us?

Incidents.be

- We hide our incidents & minimize the impact

- Most critical systems remain vulnerable

- There is no monitoring

- Lessons identified, not lessons learned

- No real cyber-security-capability.be

Why ?

It's not about knowing, it's about believing

No context ➜ hard to predict

Cyber Intelligence ➜ Context

Cyber Security

?

Miguel De Bruycker