De Digitale Oorlog

Don Eijndhoven, 28 November SIDN Connect

Argent Consulting B.V.

Don Eijndhoven

- Eigenaar Argent Consulting B.V.
- Interim Chief Information Security Officer (CISO), Enterprise Security Architect
- Gastlector Nyenrode Business University
- Oprichter Dutch Cyber Warfare Community
- Schrijft en spreekt op conferenties

NO-FUD DISCLAIMER

Onderzoek wijst uit dat overheden tot dusver zeer terughoudend zijn in digitale oorlogsvoering. De schade is afgemeten beperkt en aanvallen blijven veelal beperkt tussen landen die al in conflict met elkaar zijn.

‘Super Powers’ vormen hierop de enige uitzondering.

Waar hebben we het nu eigenlijk over?

Even wat definities voor de duidelijkheid:

Cyber Warfare is het gebruik van digitale middelen om een andere natie jouw politieke wil op te leggen.

(Acties tegen een niet-statelijke groep noemen we terreurbestrijding, en acties tegen een individu noemen we doorgaans eenvoudigweg ‘de rechtsgang’ of misdaadbestrijding.)

Cyber Intelligence is het gebruik van digitale middelen om inlichtingen te vergaren waar daadwerkelijk op gehandeld kan worden.

Cyber Crime is het gebruik van digitale middelen om jezelf te verrijken op een wijze die in strijd is met de wet.

Hoe gaat dat dan allemaal?

Een greep uit zeer recente voorbeelden van overheidsoperaties online

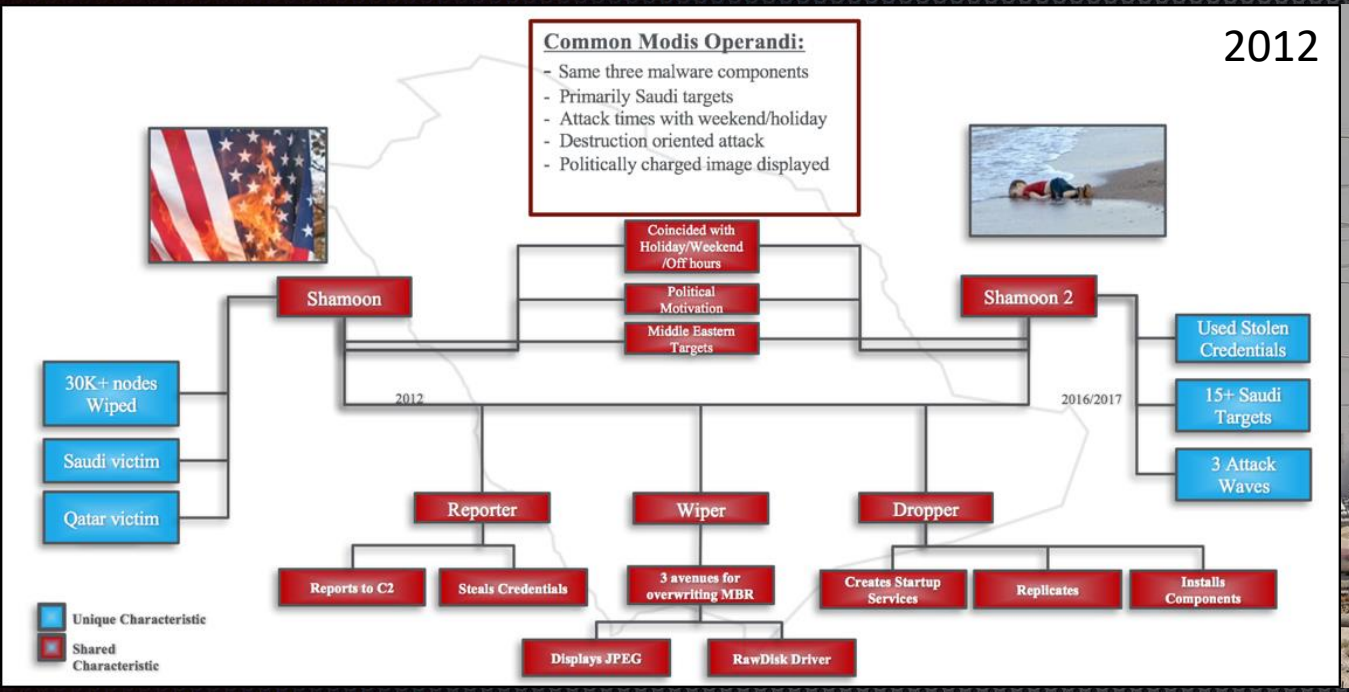
Stuxnet revisited (2009)

HET IS OORLOG
MAAR NIEMAND DIE HET ZIET
HUIB MODDERKOLK

We weten dus nu, dankzij Huib Modderkolk, dat dit een AIVD mol is geweest.

Saudi Aramco (2019 / 2012)

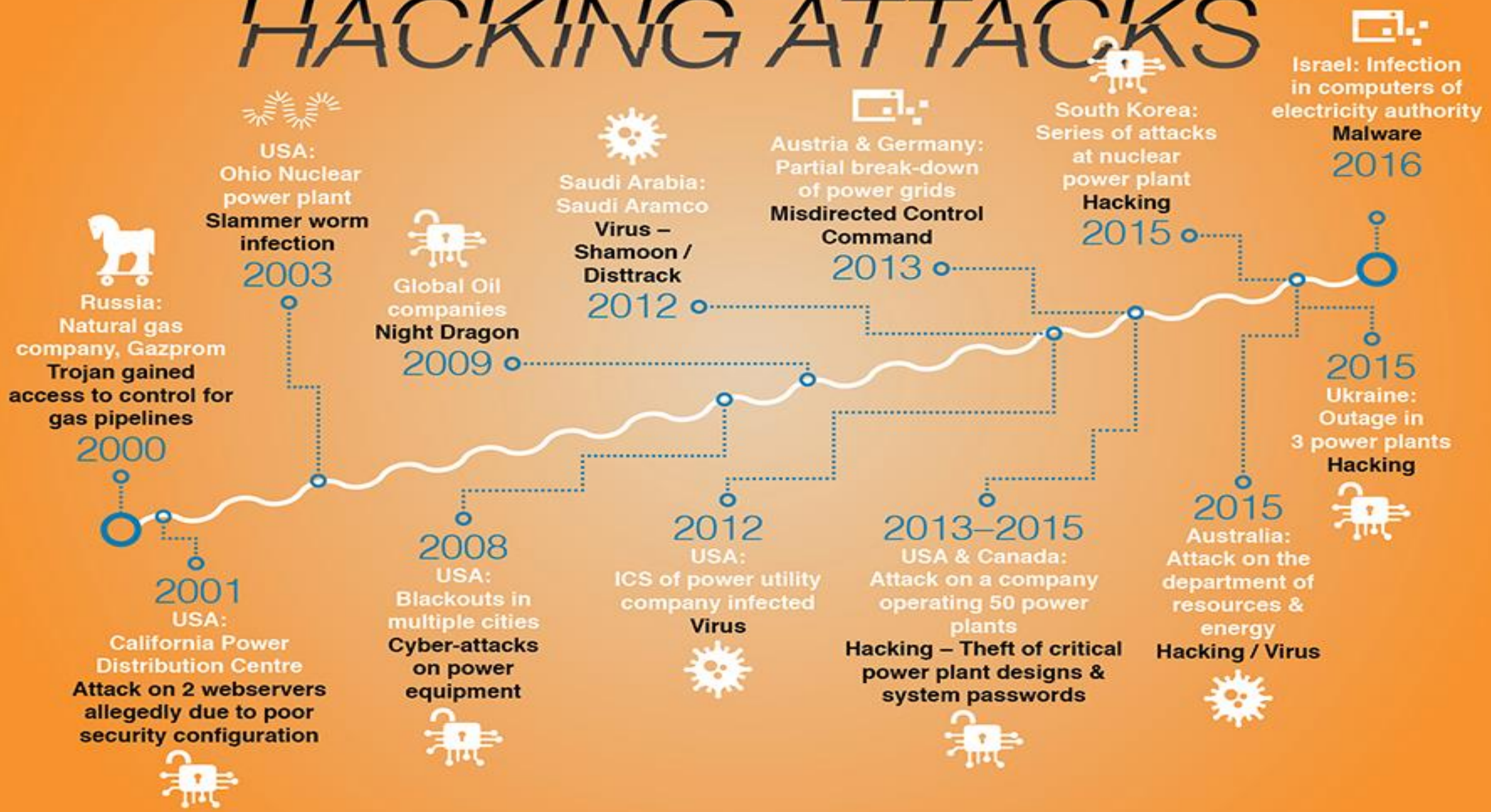
2012



2019

"[Het is] niet heel waarschijnlijk, om het zacht uit te drukken, [dat Iran achter de aanval op Aramco zit]" – Paul Aarts tijdens Nieuwsuur

HISTORY OF MAJOR HACKING ATTACKS



Het Digitale Slagveld in de media

"Nederland is slecht voorbereid op grootschalige digitale ontwrichtingen" – Wetenschappelijke Raad Regeringsbeleid

"De Amerikanen lieten taart en bloemen bezorgen bij de AIVD in Zoetermeer. " – Huib Modderkolk over de Stuxnet AIVD mol

"We zijn in een cyber oorlog verwikkeld met Rusland" – Minister Ank Bijleveld (parafrasering)

"Het is al twintig jaar oorlog. Het zijn geen op zichzelf staande incidenten." – Inge Philips in *Buitenhof*

Maersk / APN Terminals shutdown (2017)

Russische ransomware met de naam NotPetya, gericht op Oekraine, komt via Maersk het havenbedrijf binnen en legt containerbedrijf APN en twee terminals wekenlang geheel plat. Inmiddels is de wereldwijde schade geschat op 10 miljard euro.

„De overheid moet zich afvragen of het onderscheid nog houdbaar is, nu allerlei instanties via digitalisering steeds meer verknoopt zijn. Bedrijven buiten de vitale sector kunnen voor grote problemen binnen de vitale sector zorgen. Maersk behoorde tot een deel van de Rotterdamse haven dat niet tot de vitale infrastructuur werd gerekend. Dat betekent dat ze daar bij een calamiteit niet eens de telefoon hoeven op te nemen als ze door de overheid worden gebeld.” - Corien Prins, Hoogleraar Recht en Informatisering UvT over Vitale Infrastructuur

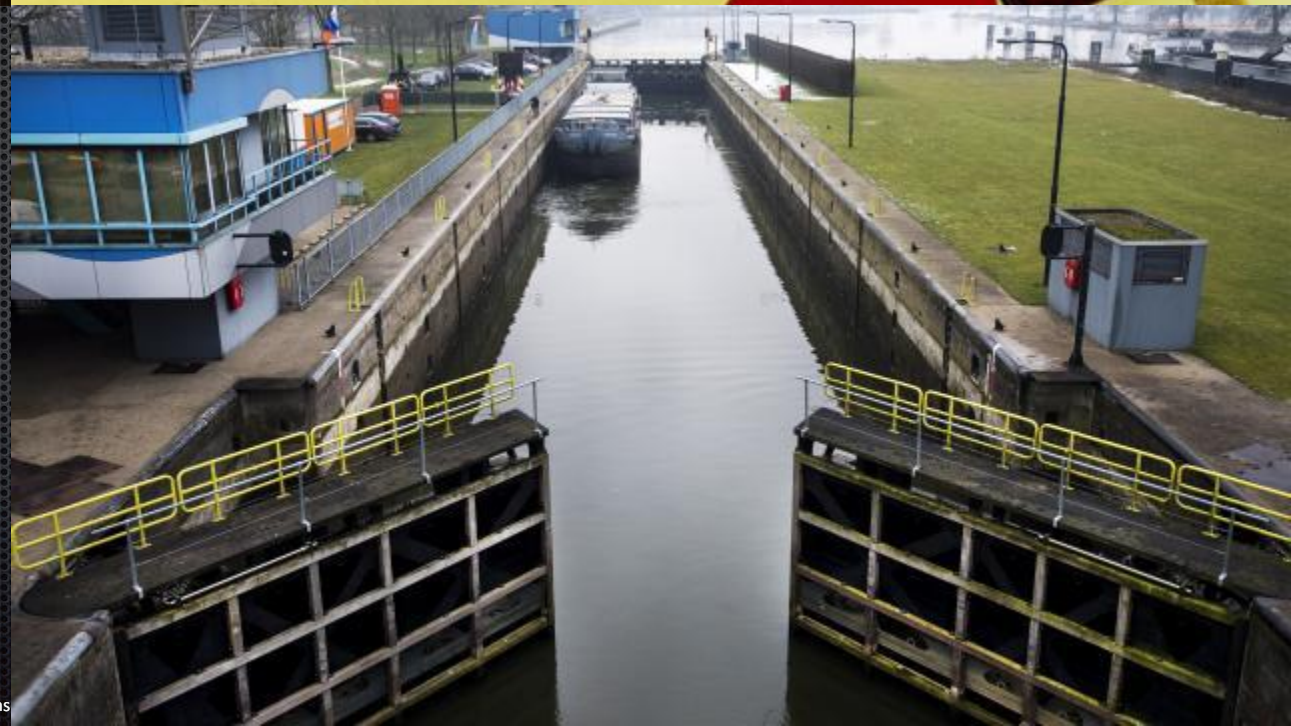
Russische invloed op Nederland

Wat hebben Sergej Skripal, de OPCW, MH-17, de GRU en die 4 Russen met elkaar te maken?

OPCW

Organisation for the Prohibition of Chemical Weapons

"Ja, er is één bedrijf waar Nederland erg van afhankelijk is, maar dat ga ik niet noemen. Dat is zo ver gedigitaliseerd dat analoog niet meer kan, maar een volledig alternatief digitaal systeem is vanwege de omvang ook niet mogelijk. Dat bedrijf beraadt zich nu op de vraag welke kerntaken het bij een digitale crisis wil kunnen voortzetten." - Corien Prins, Hoogleraar Recht en Informatisering UvT over Vitale Infrastructuur



Informatie Operaties

Het nieuwe Goud

Een kleine set aan voorbeelden waarom onze verkiezingen nooit meer volledig veilig zullen zijn.

Amerikaanse Presidentsverkiezingen (2016)

Over die Troll Factory gesproken…

The US launched a cyberattack on a Russian troll factory during the 2018 midt

The Washington Post reports that the US blocked internet access to Russian trolls trying to spread misinformation during the election.

By Jen Kirby | jen.kirby@vox.com | Feb 26, 2019, 6:20pm EST

SHARE

Russian President Vladimir Putin in December 2018. The Russian troll factory, the Internet Research Agency, has ties to the Kremlin. | Ricardo Ceppi/Getty Images

NEWS

IMPEACHMENT INQUIRY POLITICS U.S. NEWS BUSINESS WORLD TECH & ME

NATIONAL SECURITY

Trump approved operation th Russian troll farm during 201

The action against the Internet Research Agency was part of a interfere in U.S. politics ahead of the elections.

CNN World Africa Americas Asia Australia China Europe India Middle East United Kingdom Edition

Russia's 'troll factory' is alive and well in Africa

By Mary Ilyushina, CNN

Updated 1131 GMT (1931 HKT) November 1, 2019

Now Playing
Putin entices African leaders with military hardware

02:21
Uber loses London license again but can keep driving for now

01:41
Cut diamonds and treasure haul stolen in vault heist

01:02
Egypt hails rare find of mummified lion cubs, crocodiles, cats

02:46
Record nur voters part Hong Kong

Moscow (CNN) — In the runup to the 2020 election, the graduates of Russia's infamous "troll factory" are honing their fake-news skills. This time, they are doing it openly, using Africa as a proving ground — and with the help of Alexander Malkevich, a Russian propagandist exiled from the US.

Paid Content by Outbrain

Mansion Global Daily: Celebs in the New York Suburbs, the Affordability Crisis and More
Mansion Global

Gamers overal ter wereld hebben naar dit spel uitgekeken
Elvenar

Learn to invest in Amazon for only € 200. Invest in the future, today.
TradeFixd

More from CNN

Hong Kong leader Carrie Lam: 'We are questioning…'

NASA has found sugar in meteorites that crashed…

China hackt Australische overheid (2019)

In februari van dit jaar bleek het Australisch parliament hackers op het netwerk te hebben. Nader onderzoek door het Australian Signals Directorate (ASD) wees uit dat de netwerken van de regerende Liberals, maar ook coalitiepartner de Nationals en de oppositie (Labor) gepenetreerd waren. Hoewel dit onder de pet werd gehouden hebben inmiddels 5 mensen met directe kennis van het onderzoeksrapport aan Reuters erkend dat China de dader is.

Met de Amerikaanse presidentsverkiezingen (2016) nog vers in het geheugen lijkt politieke inmenging op verkiezingen door vreemde mogendheden definitief een probleem te zijn.

Daar is geen woord Chinees bij…

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERAT

ATTACKS/BREACHES

10/31/2019
04:20 PM

Jai Vijayan
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login

50% 50%

Like
Tweet
Share

Is the Chinese army hacking American computers?

BY LAURIE L. DOVE

« PREV NEXT »

Chinese Cyber Attacks and U.S. Targets

This Shanghai tower is believed to be the origin point of recent cyberattacks.
© IMAGINECHINA/CORBIS

Despite the recent outcry that Chinese hackers have targeted U.S. companies and government entities, the attempts aren't isolated to one nation. Chinese hackers have reportedly infiltrated the Australian Reserve Bank, as well as government entities in Taiwan, Brunei, Myanmar, Vietnam and other countries [sources: Saarinen, Taipei Times].

In a method markedly similar to attacks characteristic of the Chinese military, a group of hackers targeted the New York Times by routing e-mails through computers at U.S. universities. American intelligence officials confirmed the cyberattacks were traced to a specific IP address -- a point of origin so narrow, that in the whole of China and its 1.3 billion residents, it could be pinpointed to a 12-story office building on the edge of Shanghai. Not only did the attacks on the New York Times launch from this building, so did the majority of malware targeting U.S. companies and government entities. Interestingly, the same building houses the People's Liberation Army Unit 61398, which has led to speculation that an elite group of hackers, known as the Comment Crew or the Shanghai Group, are actually sponsored by the Chinese army.

China. But FireEye would not disclose just where the targets are located.

FireEye's disclosure on MESSAGETAP is the second development this week involving individuals being targeted via malware placed on service provider

NOS | Nieuws | Sport | Uitzendingen | TELETEKST

NOS NIEUWS • BUITENLAND • TECH • ZATERDAG, 13:46

'China bestookt Belgen op handelsmissie met cyberaanvallen'

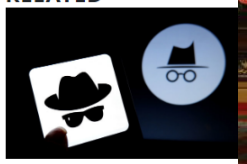
tijdens het bezoek van de Belgische handelsmissie aan

a is bestookt met massale
van het bedrijf Secutec tegenover het
reisde zelf mee naar China en hij
anvallen per uur.

id, verschillende ministers en tientallen bedrijven, was van afgelopen zondag tot en met donderdag in China. Ze brachten onder meer een bezoek aan Peking en Shanghai en aan pakjesdienst Alibaba.

De aanvallen zouden zijn uitgevoerd met robots. Secutec, dat de Belgische

RELATED



What Does Browsing in Incognito Mode Really Do?

Private Browsers Aren't All Equally Private

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS GRAPHICS OPINION WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

Get a fresh start. Choose your FT trial

Latest on Cyber warfare

Retailers brace for cyber attacks in peak shopping season

Sandworm — Russia, America and the new era of cyber war

International Governance

Cyber warfare + Add to myFT

India confirms cyber attack on nuclear power plant

Experts say hack has similar fingerprints to attacks by North Korea's Lazarus Group

Save

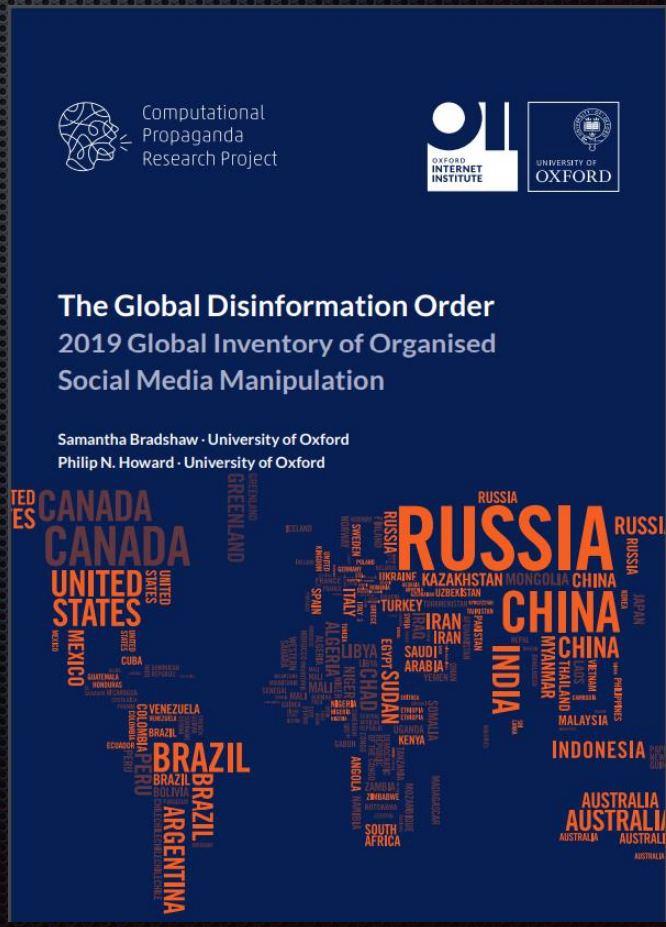
Indian security officials have known about the hack at the Kudankulam nuclear power plant since September, according to Pukhraj Singh, a private cyber security consultant © Bloomberg

Stephanie Findlay in New Delhi and **Edward White** in Seoul OCTOBER 31 2019

93

Disinformatie Operaties galore!

- In 2019 zijn in 70 landen ‘informatie operaties’ vastgesteld
  - Dit waren er 48 in 2018 en slechts 28 in 2017
- Social Media is vooral populair bij authoritaire regimes (China koploper dit jaar dankzij de rellen)
- Een “handvol” landen doet het ook bij andere landen: China, India, Iran, Pakistan, Rusland, Saudi Arabie en Venezuela.



VRAGEN?

Links

- https://fd.nl/opinie/1316434/het-is-tijd-voor-een-deltaplan-cybersecurity#
- https://www.wrr.nl/onderwerpen/digitale-ontwrichting
- https://www.nen.nl/NEN-Shop/ICTnieuwsberichten/Waterwerken-kwetsbaar-voor-cyberaanvallen.htm
- https://www.aljazeera.com/ajimpact/oil-prices-surge-attack-saudi-oil-facilities-190916003344259.html
- https://securingtomorrow.mcafee.com/other-blogs/executive-perspectives/state-shamoon-actor-different-lines/
- https://www.rtlnieuws.nl/nieuws/nederland/artikel/4798426/storing-schiphol-brandstof-afs-tno-onderzoek
- https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF
- https://tweakers.net/nieuws/154402/kpn-verkeerde-routering-verkeer-leidde-tot-112-storing.html
- https://www.nrc.nl/nieuws/2019/09/08/door-digitalisering-nemen-risicos-toe-a3972656
- https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf
- https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6
- https://www.youtube.com/watch?v=zdR-I35Ladk

Contactgegevens

Argent Consulting B.V.

Don Eijndhoven

D.Eijndhoven@argentconsulting.nl

Twitter: @argentconsultin

+31 6 450 850 21

(Acquisitie wordt niet op prijs gesteld)