unite information · innovation · transformation

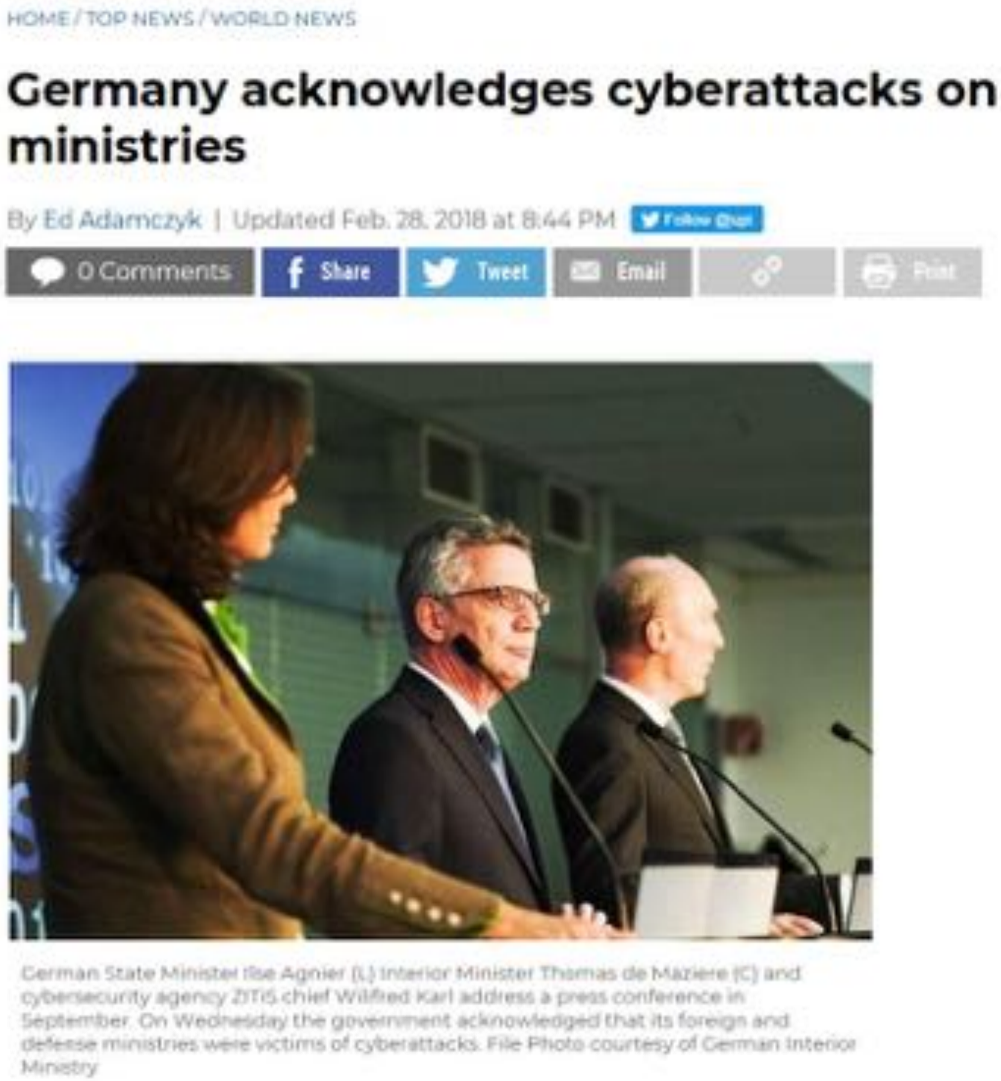
Cyberspace and Cybersecurity Policy, Risks & Strategies

Core Diplomatic Training 2018, a collaboration between OICT, UN-OHRLLS, and UNITAR

Introduction to organizational cybersecurity: vulnerabilities and risk mitigation strategies

Thomas P. Braun, Global Security & Architecture Section, DM/OICT

<insert today's headline>



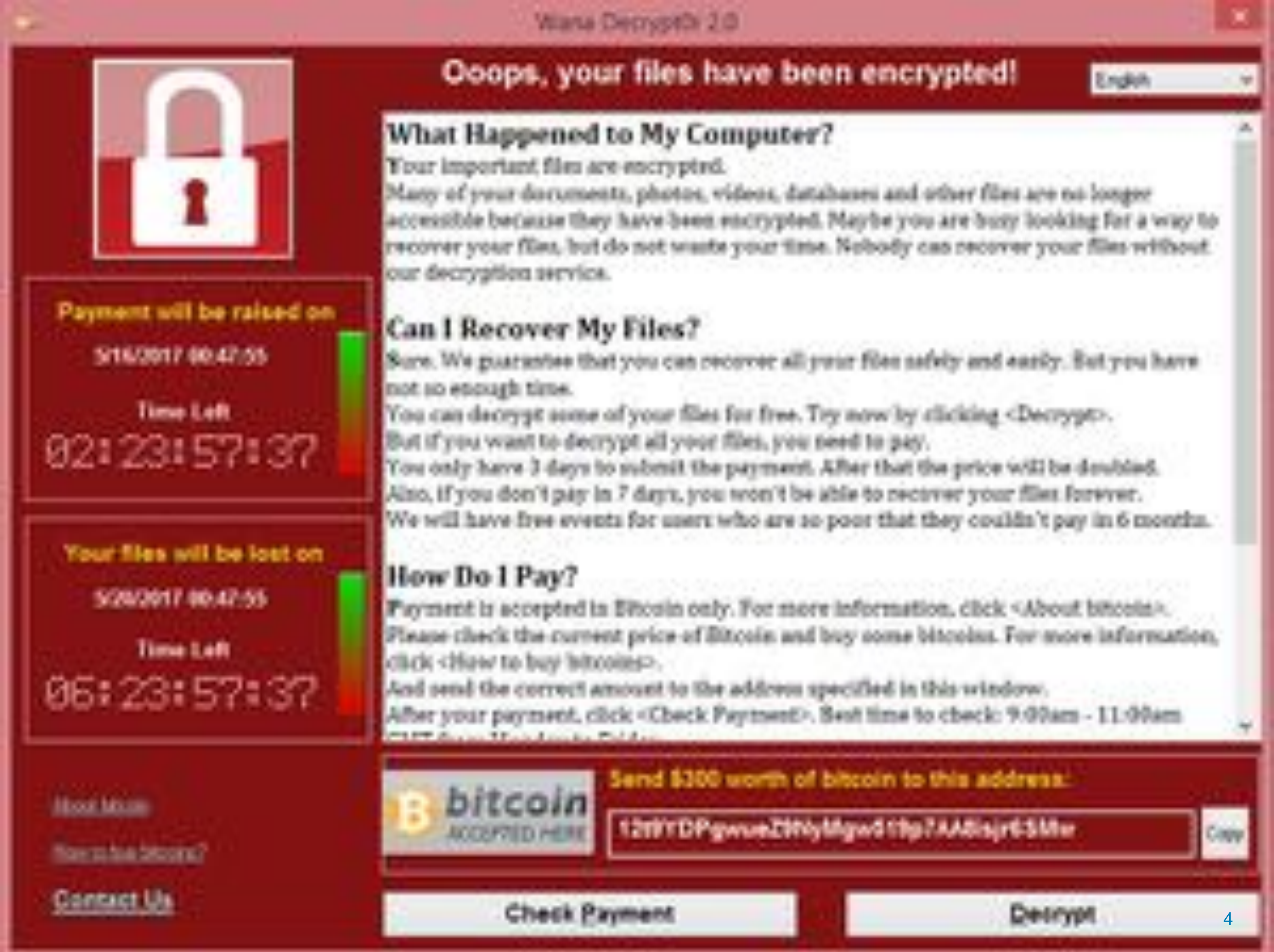
Germany acknowledges cyberattacks on defense, foreign ministries

By Ed Adamczyk | Updated Feb. 28, 2018 at 8:44 PM

German State Minister Ilse Agnier (L) Interior Minister Thomas de Maziere (C) and cybersecurity agency ZITiS chief Wilfried Karl address a press conference in September. On Wednesday the government acknowledged that its foreign and defense ministries were victims of cyberattacks. File Photo courtesy of German Interior Ministry

Critical role of ICT

- Enabler to accomplish SDGs and deliver public services
  - E-governance
  - Education
  - Healthcare
  - Communications
  - Commerce
- Reliable infrastructure and trusted digital ecosystem
- Vulnerabilities, threats, threat actors risk mitigation



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

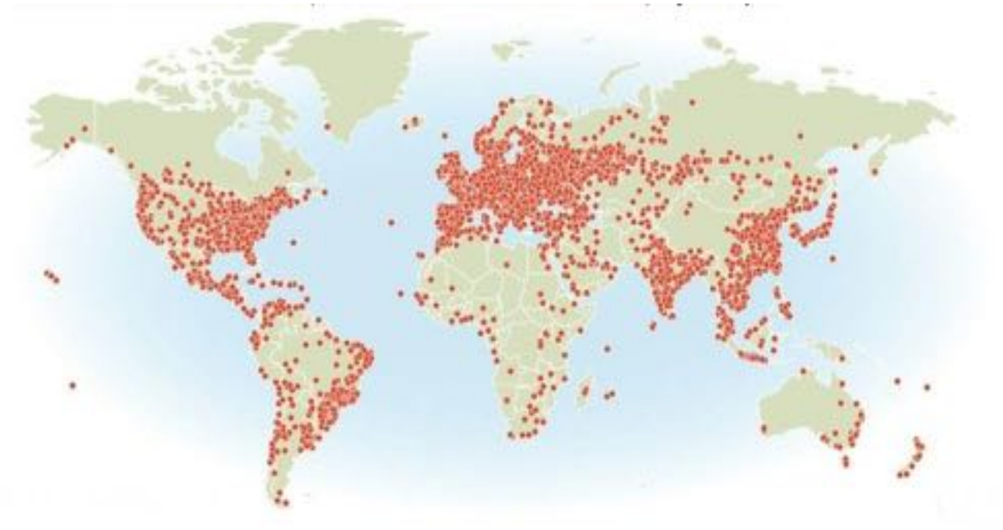
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Attacks on critical infrastructure ('Wannacry' / 'NotPetya')

Infected more than 230,000 computer systems in 150 countries

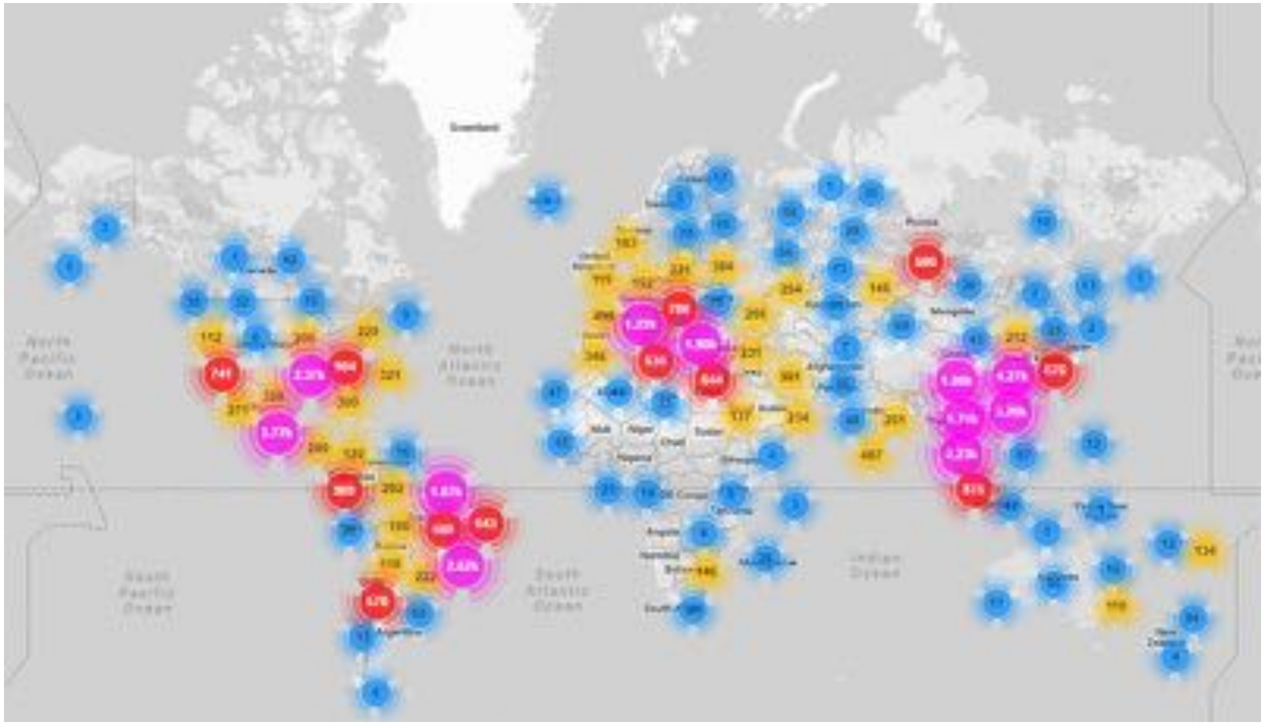


In the UK, up to 70,000 devices belonging to the National Health Service, including computers, MRI scanners, blood-storage refrigerators & theatre equipment, were affected.

Caused approximately 225,000 customers in Ukraine to lose electrical power across various areas for a period from 1 to 6 hours.

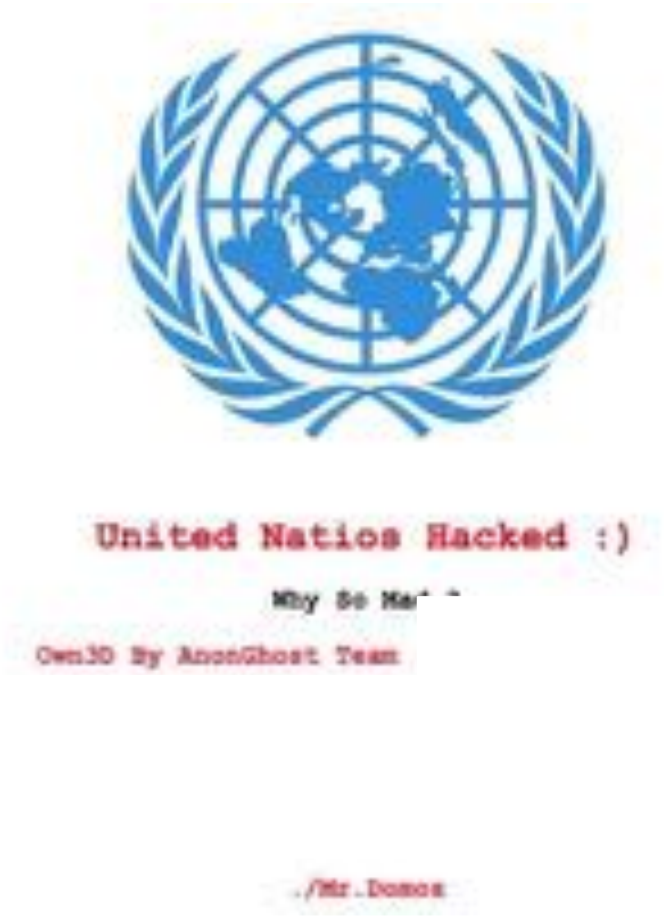
Internet of Things

- “Mirai” botnet used to bring down sites like Twitter, the Guardian, Netflix, Reddit, CNN and many others
- 500,000 compromised devices involved in the attack



DynDNS

Web site defacements



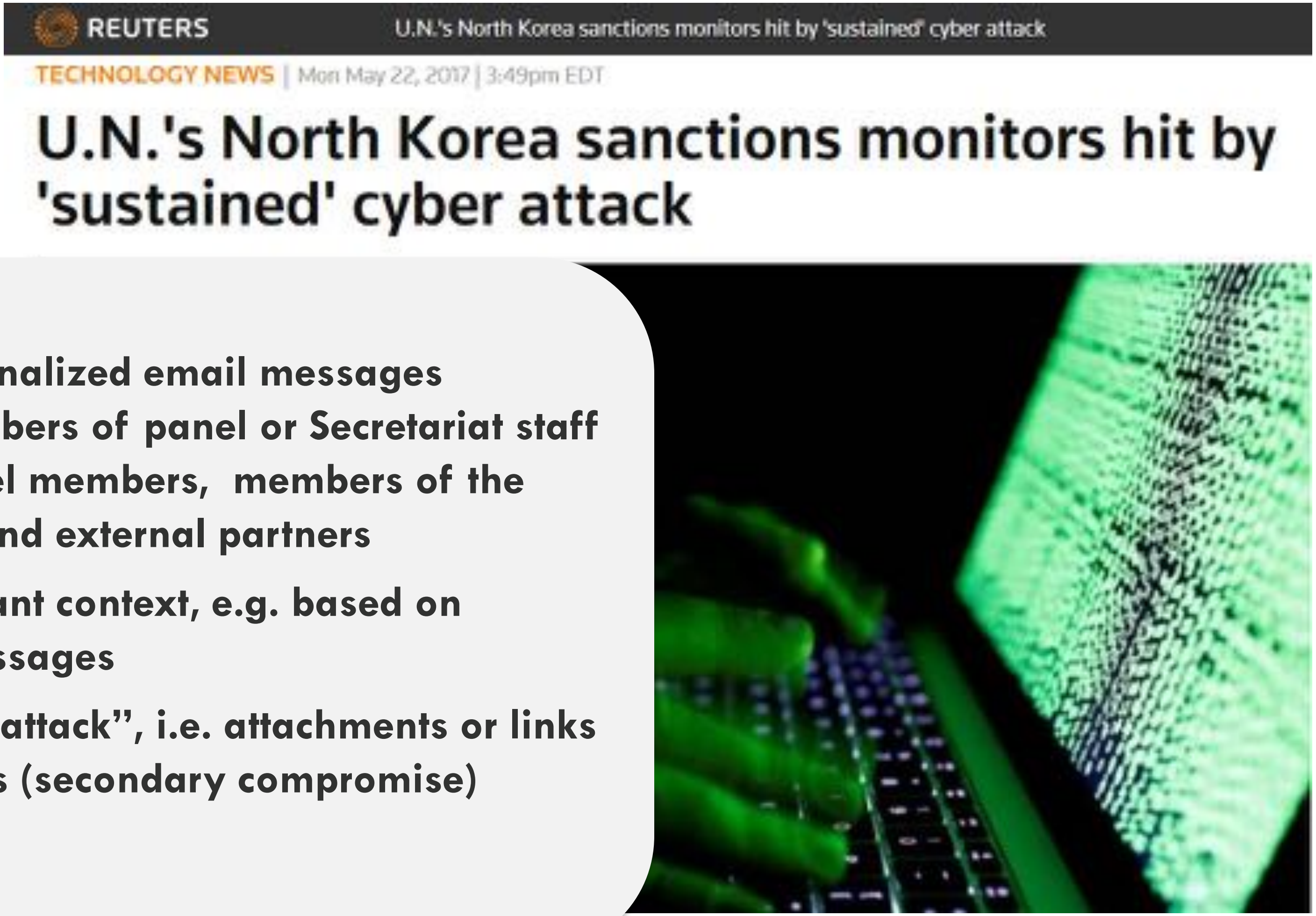
United Natios Hacked :)

Why So Mad ?

Own3D By AnonGhost Team

./Mr.Domos

Targeted attacks – “spear phishing”



REUTERS U.N.'s North Korea sanctions monitors hit by 'sustained' cyber attack

TECHNOLOGY NEWS | Mon May 22, 2017 | 3:49pm EDT

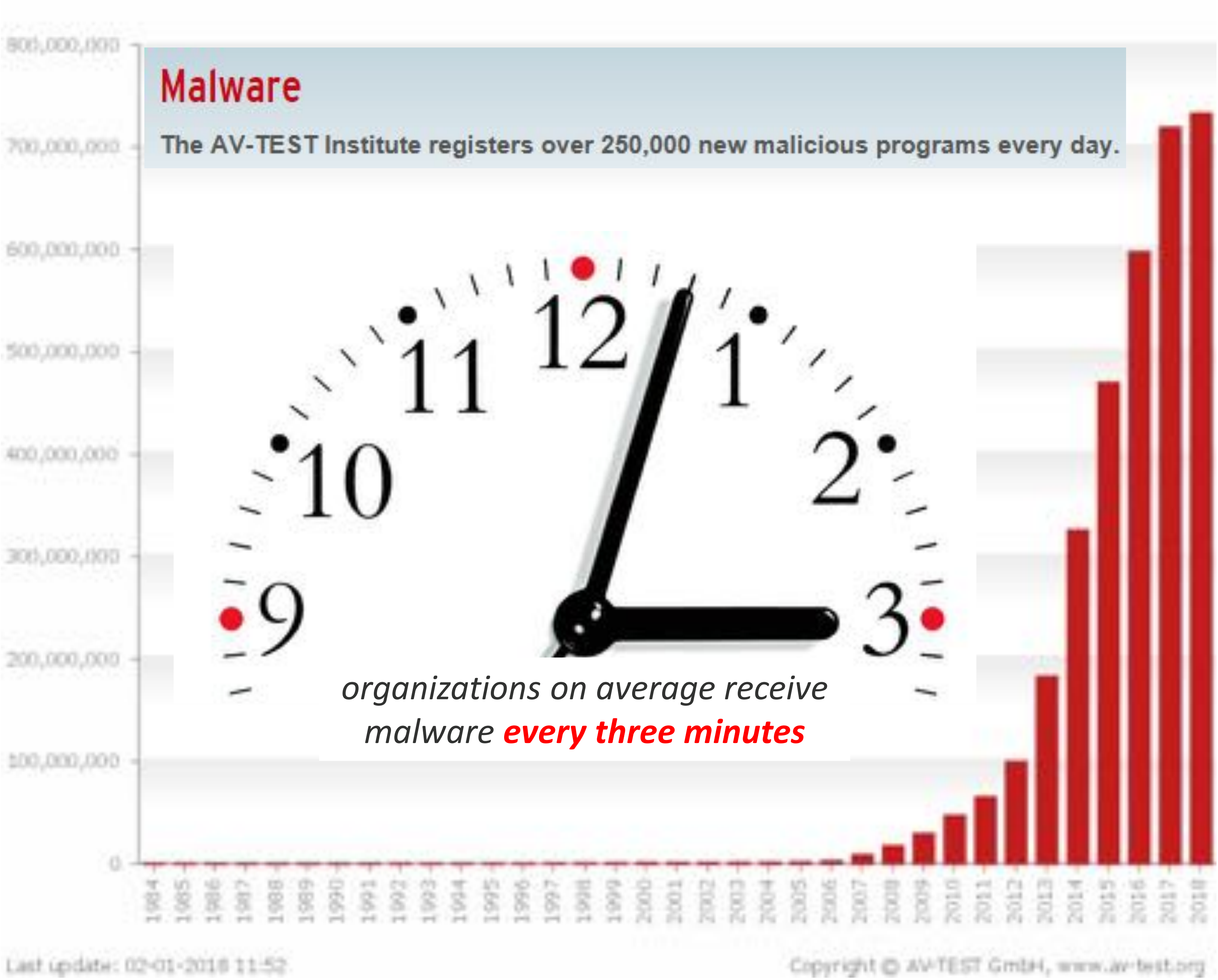
U.N.'s North Korea sanctions monitors hit by 'sustained' cyber attack

- Highly personalized email messages “From” members of panel or Secretariat staff to other panel members, members of the committee, and external partners
- Highly relevant context, e.g. based on previous messages
- “multi-stage attack”, i.e. attachments or links not malicious (secondary compromise)

Identity theft (because "that's where the money is")

Attack taxonomy (simplified)

type	*examples*	*goal*	*victim*	*target*	*method*	*stealthy*
"Internet background noise"	"virus", adware, malware, scareware	"fun"	user	desktops	email, drive-by download	no
cyber crime	malware, Trojan, keylogger, bot, RAT	profit	user organization	desktops	email, drive-by download	yes
intelligence / espionage	malware, Trojan, keylogger, RAT	political	organization	desktops => internal systems	email, drive-by download	yes
"hacktivism"	DoS, defacement, data theft, sabotage	political (profit)	organization	applications / hosts	SQL injection, XSS, DDoS	no



Malware

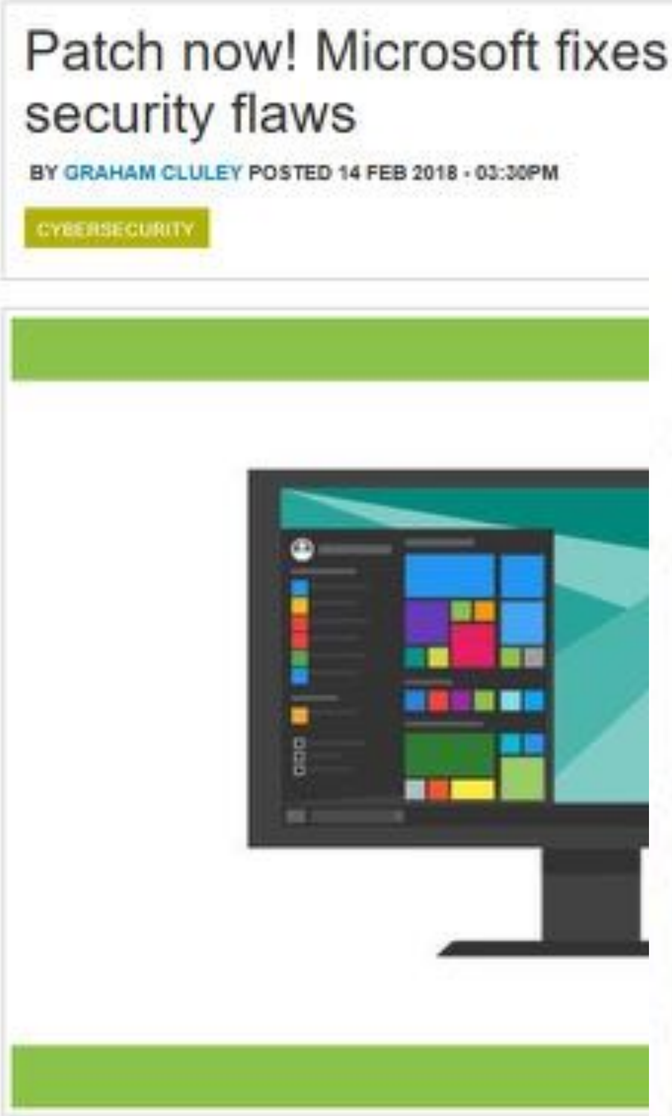
The AV-TEST Institute registers over 250,000 new malicious programs every day.

organizations on average receive malware ***every three minutes***

Last update: 02-01-2018 11:52

Copyright © AV-TEST GmbH, www.av-test.org

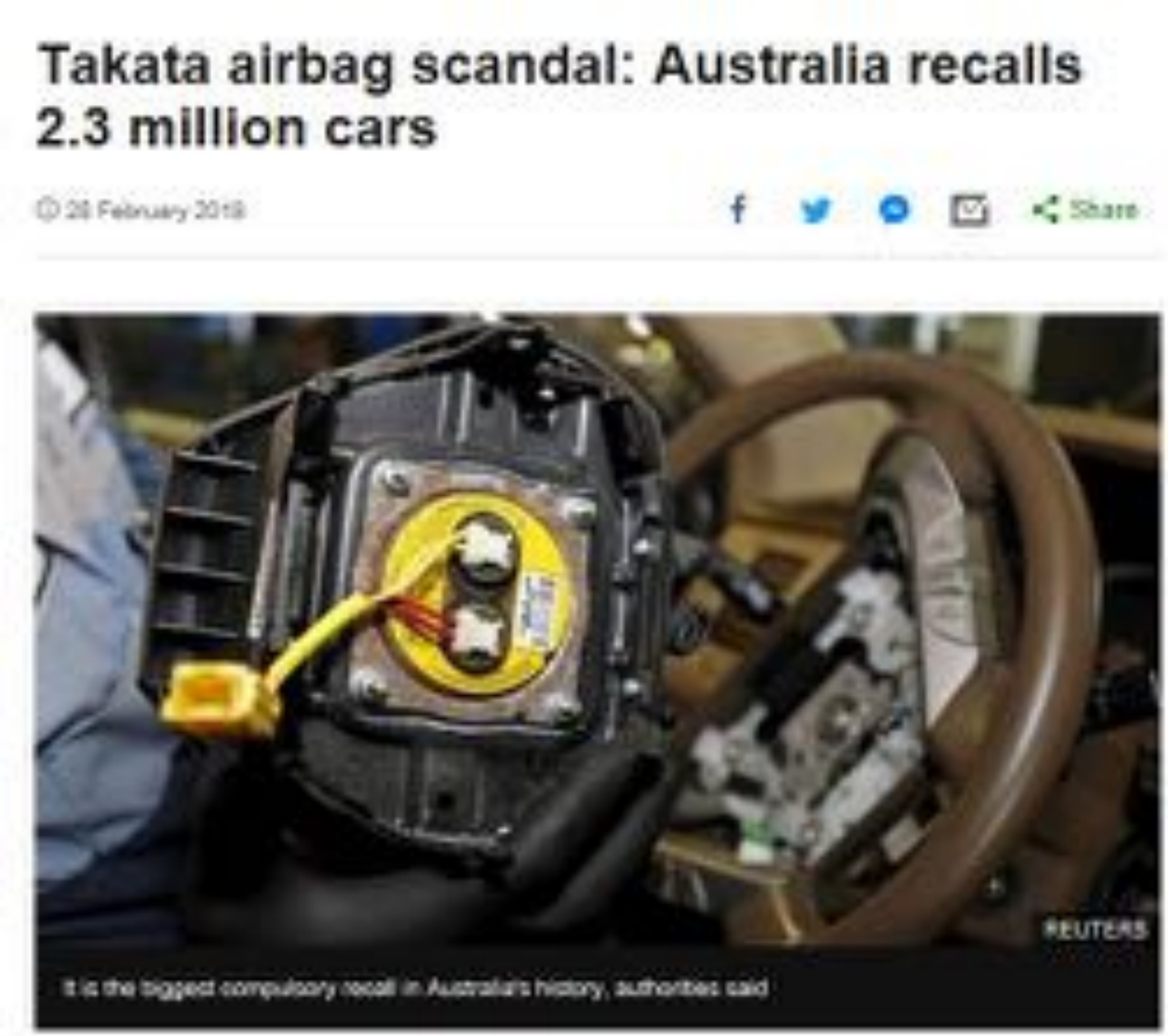
Spectre and Meltdown (2018)



Patch now! Microsoft fixes over 50 serious security flaws

BY GRAHAM CLULEY POSTED 14 FEB 2018 - 03:30PM

CYBERSECURITY

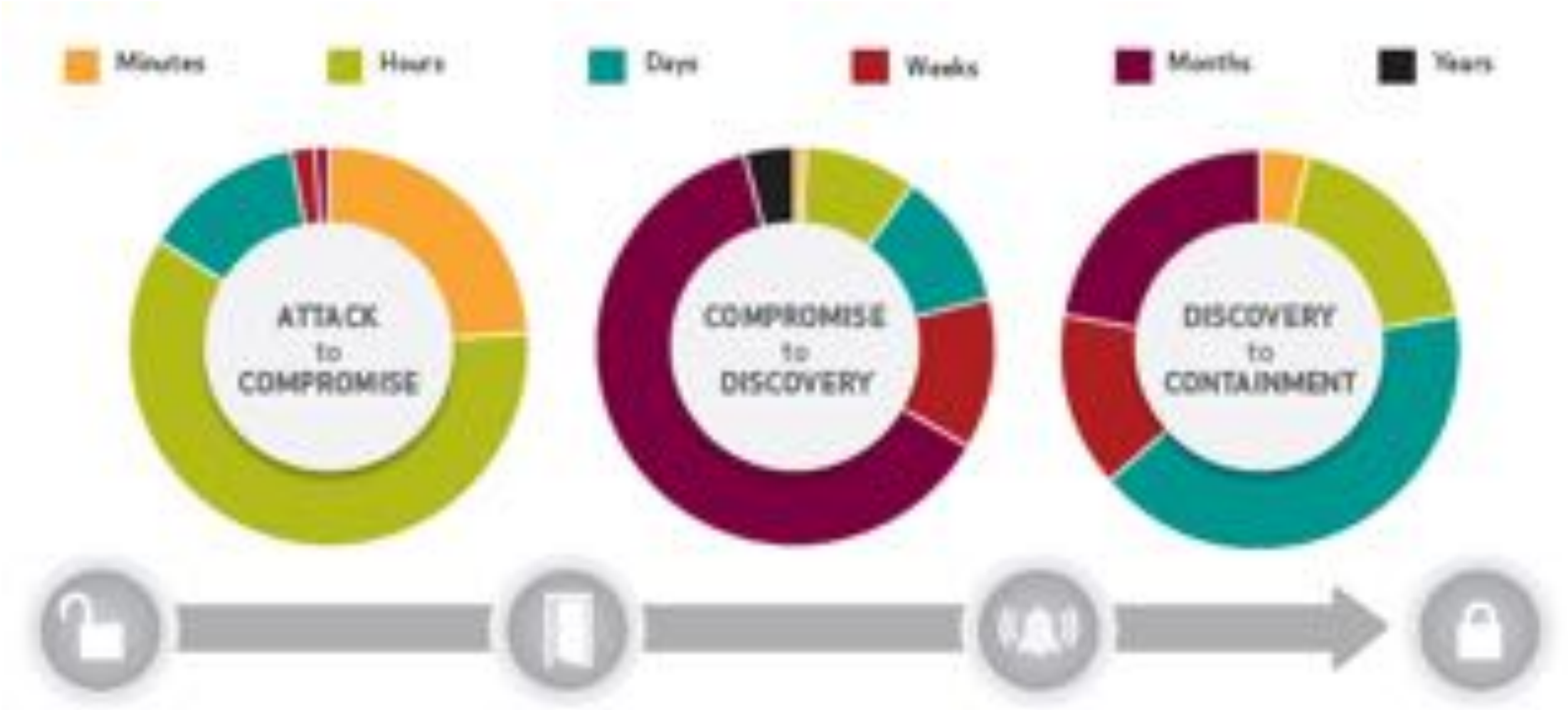


Takata airbag scandal: Australia recalls 2.3 million cars

28 February 2018

It is the biggest compulsory recall in Australia's history, authorities said

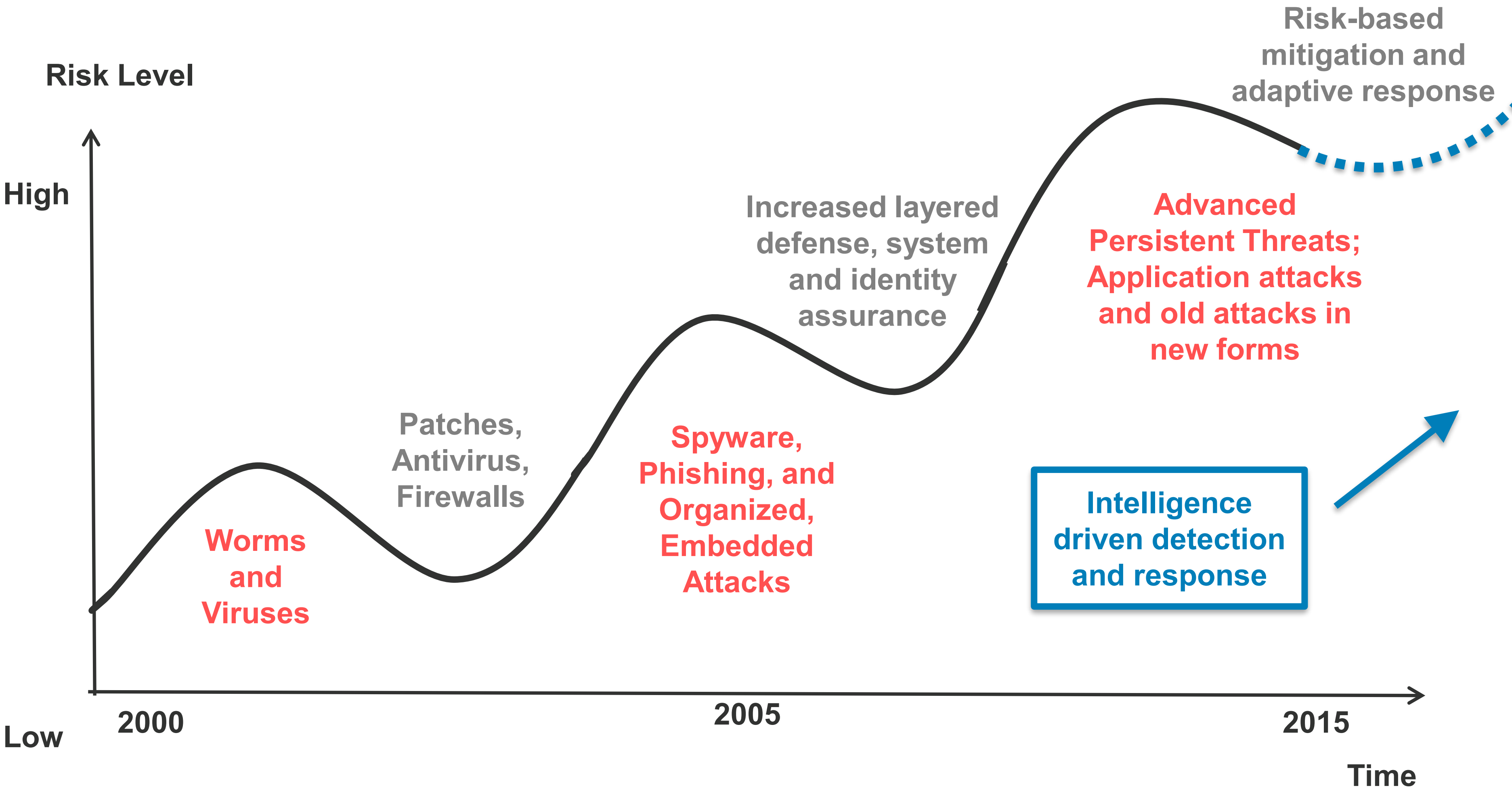
Global challenge: Time to detect (and respond)



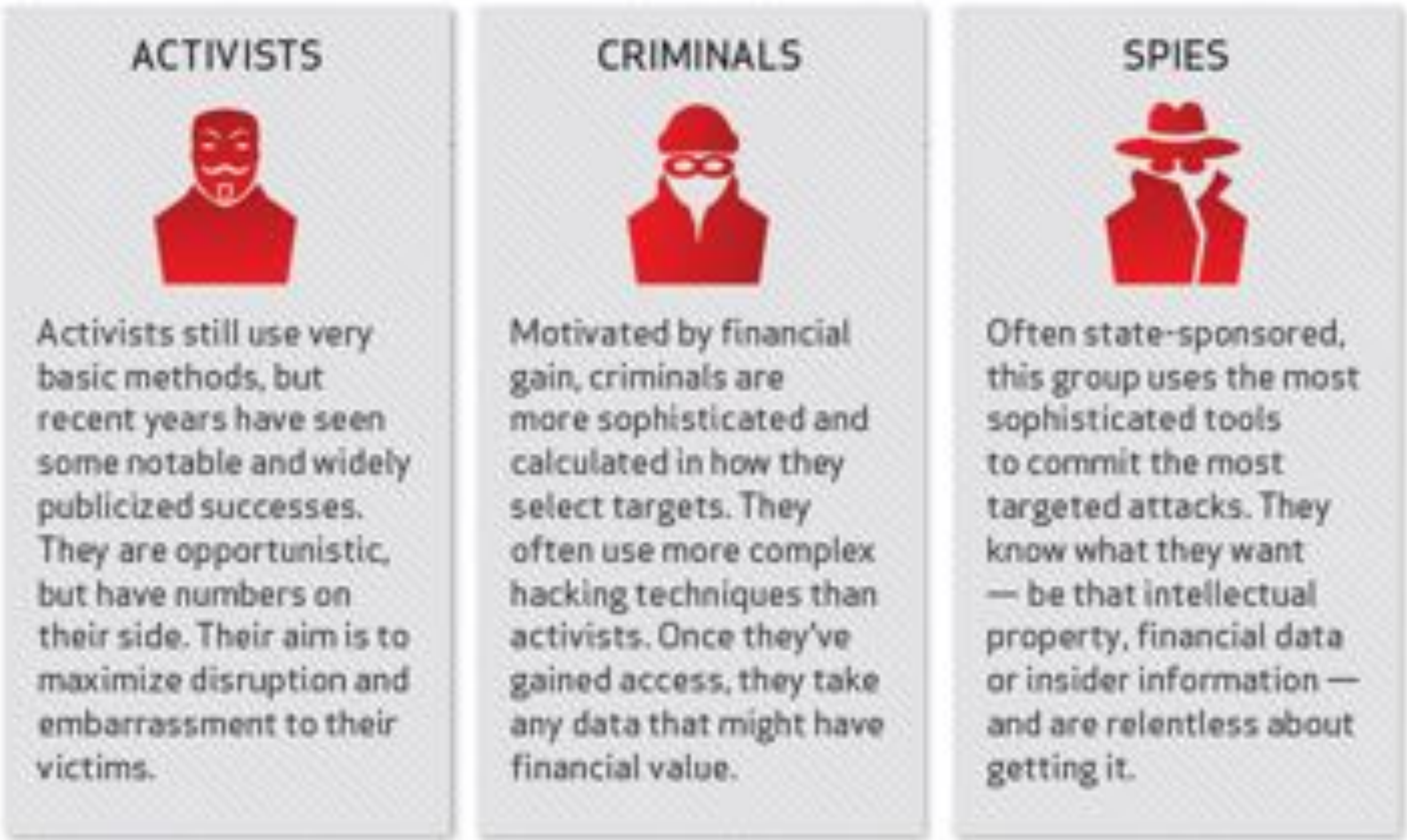
69% informed by third party

“median of 205 days”

Evolution of Risks, Threats, and Responses



Types of actors, and their motivations



ACTIVISTS

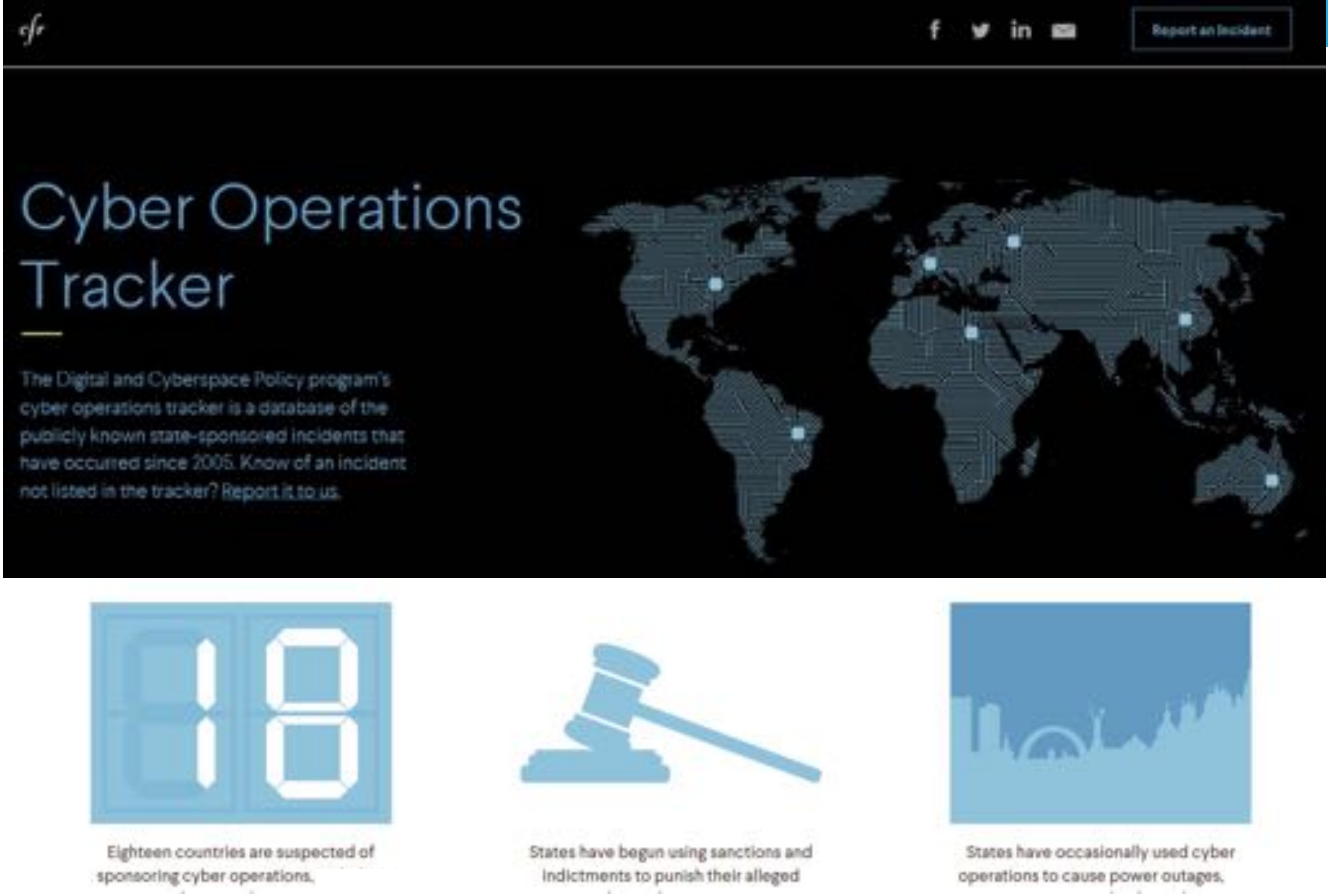
Activists still use very basic methods, but recent years have seen some notable and widely publicized successes. They are opportunistic, but have numbers on their side. Their aim is to maximize disruption and embarrassment to their victims.

CRIMINALS

Motivated by financial gain, criminals are more sophisticated and calculated in how they select targets. They often use more complex hacking techniques than activists. Once they've gained access, they take any data that might have financial value.

SPIES

Often state-sponsored, this group uses the most sophisticated tools to commit the most targeted attacks. They know what they want — be that intellectual property, financial data or insider information — and are relentless about getting it.



Cyber Operations Tracker

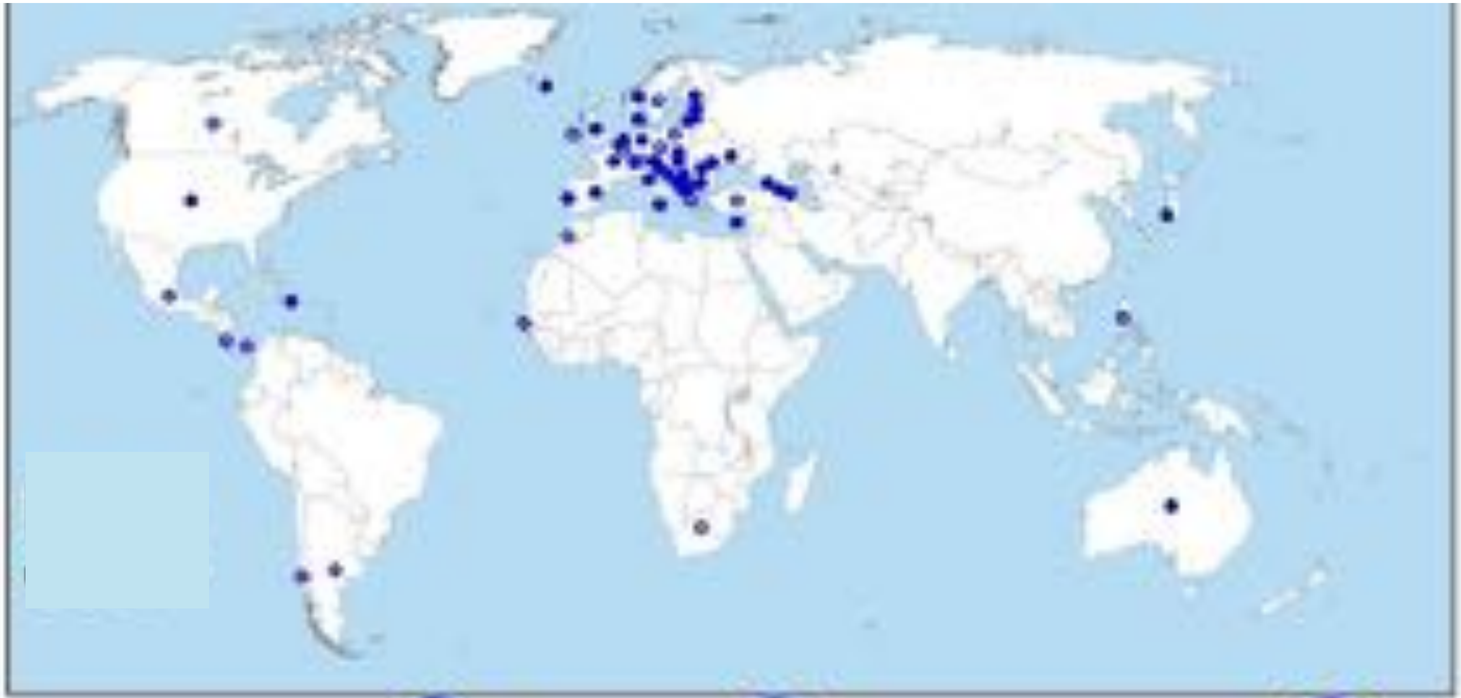
The Digital and Cyberspace Policy program's cyber operations tracker is a database of the publicly known state-sponsored incidents that have occurred since 2005. Know of an incident not listed in the tracker? Report it to us.

Eighteen countries are suspected of sponsoring cyber operations.

States have begun using sanctions and indictments to punish their alleged

States have occasionally used cyber operations to cause power outages.

Budapest Convention on Cybercrime (ETS No. 185)



Ratified/acceded: 39 ●

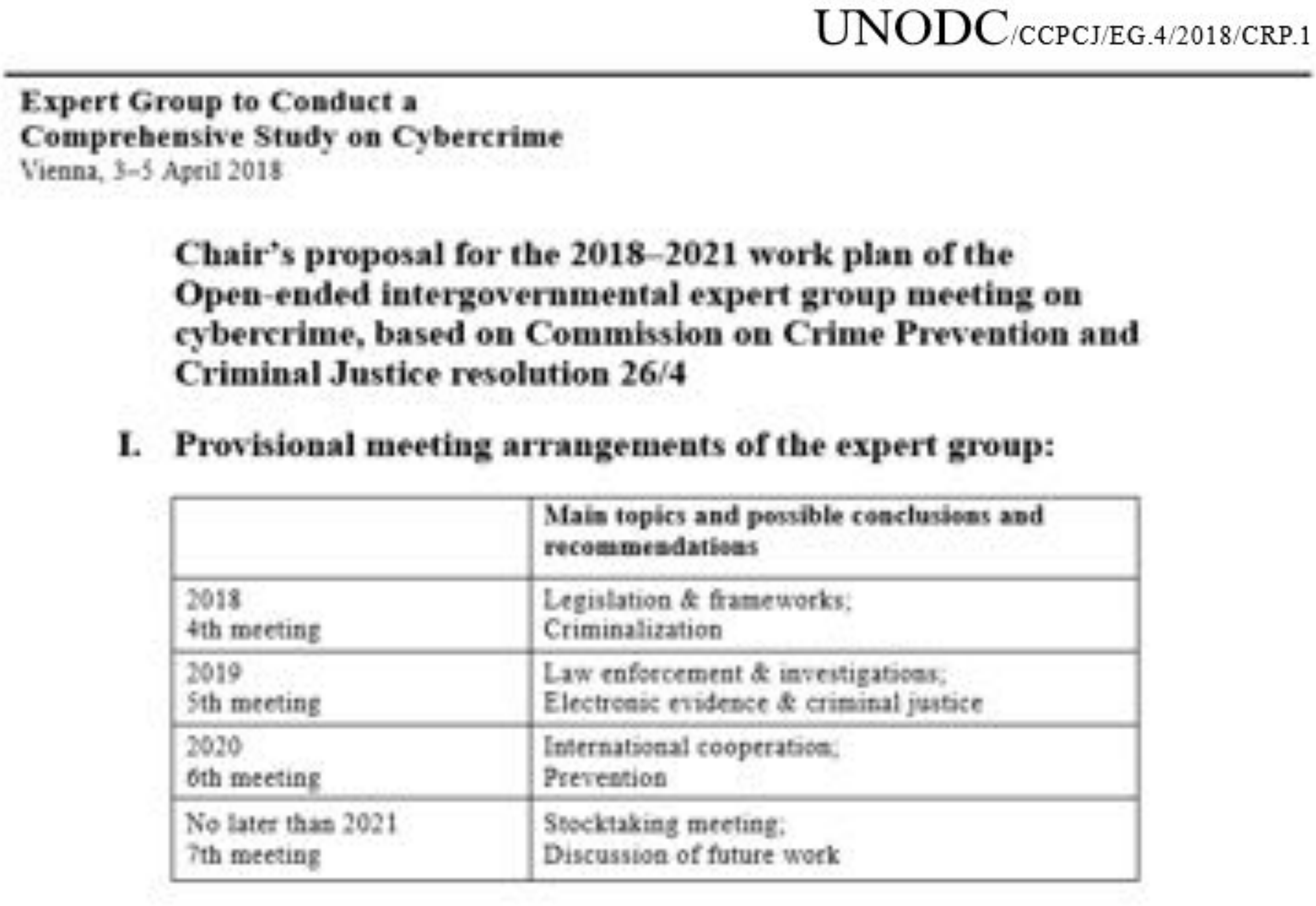
- 35 European
- Australia
- Dominican Republic
- Japan
- USA

Signed: 11 ●

- 9 European
- Canada
- South Africa

Invited to accede: 8 ●

- Argentina
- Chile
- Costa Rica
- Mexico
- Morocco
- Panama
- Philippines
- Senegal



UNODC/CCPCJ/EG.4/2018/CRP.1

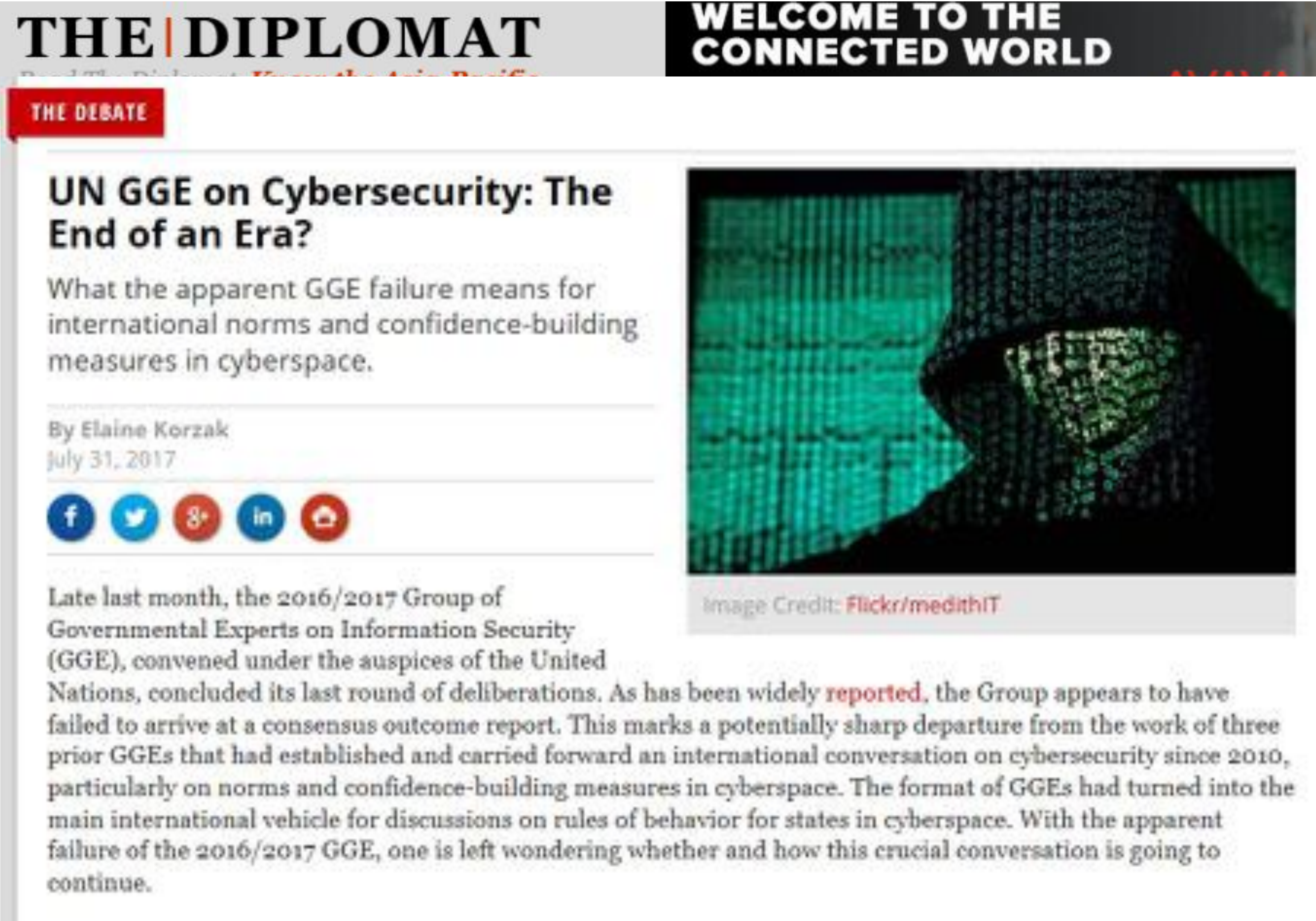
Expert Group to Conduct a Comprehensive Study on Cybercrime

Vienna, 3–5 April 2018

Chair's proposal for the 2018–2021 work plan of the Open-ended intergovernmental expert group meeting on cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4

I. Provisional meeting arrangements of the expert group:

	Main topics and possible conclusions and recommendations
2018 4th meeting	Legislation & frameworks; Criminalization
2019 5th meeting	Law enforcement & investigations; Electronic evidence & criminal justice
2020 6th meeting	International cooperation; Prevention
No later than 2021 7th meeting	Stocktaking meeting; Discussion of future work



THE DEBATE

UN GGE on Cybersecurity: The End of an Era?

What the apparent GGE failure means for international norms and confidence-building measures in cyberspace.

By Elaine Korzak
July 31, 2017

Image Credit: Flickr/medithIT

Late last month, the 2016/2017 Group of Governmental Experts on Information Security (GGE), convened under the auspices of the United Nations, concluded its last round of deliberations. As has been widely reported, the Group appears to have failed to arrive at a consensus outcome report. This marks a potentially sharp departure from the work of three prior GGEs that had established and carried forward an international conversation on cybersecurity since 2010, particularly on norms and confidence-building measures in cyberspace. The format of GGEs had turned into the main international vehicle for discussions on rules of behavior for states in cyberspace. With the apparent failure of the 2016/2017 GGE, one is left wondering whether and how this crucial conversation is going to continue.

Mitigation approaches

Individual

- Protect digital identities
- Don’t fall for phishing (and other) scams
- Keep systems updated
- Change passwords on home systems

Organizational

- Risk based approach
- Int’l best practices
- Baseline of technical controls
- Prevention + detection & response
- Focus on user awareness

Stop, think, click

Stop

Think

Click

… or don’t