CCDCOE

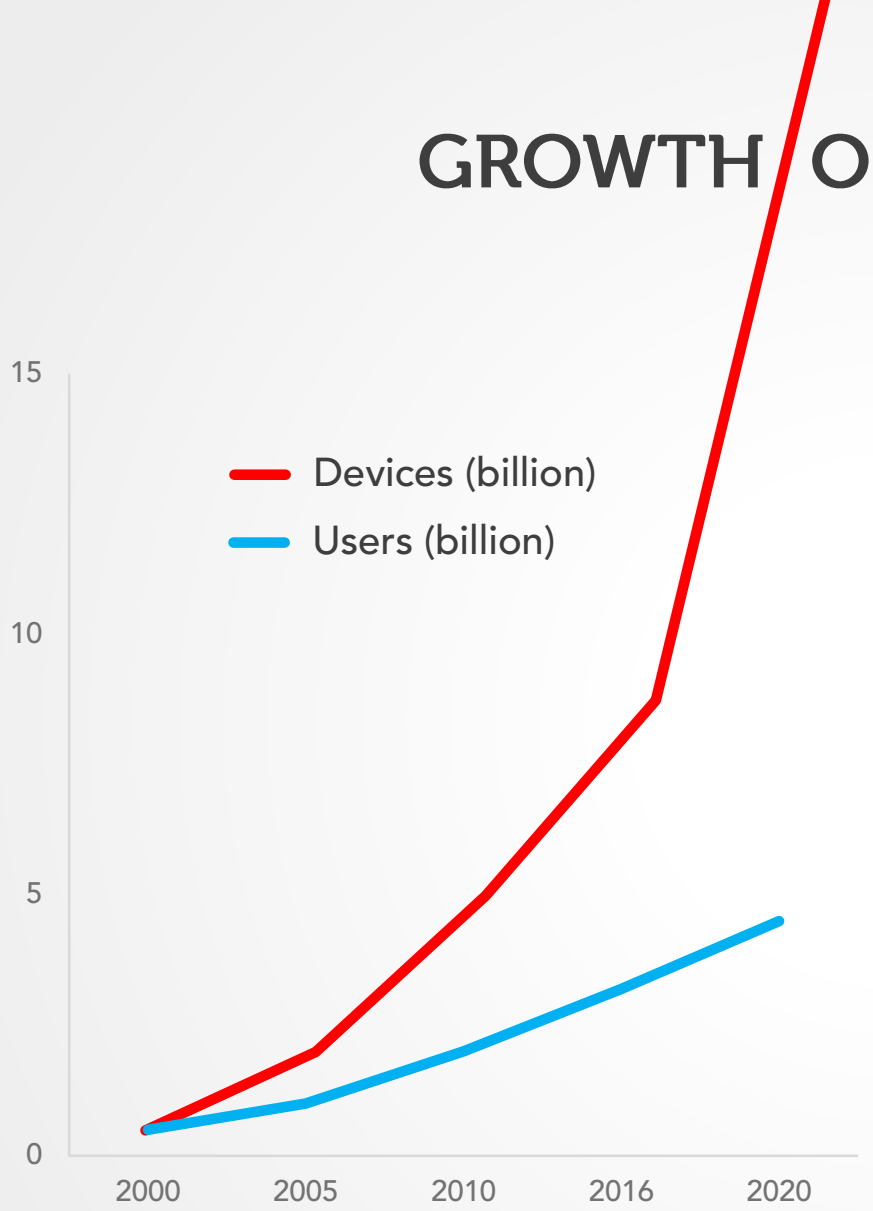
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

CCDCOE

This briefing is a product of the NATO CCD COE. It does not represent the opinions or policies of NATO and is designed to provide an independent position.

GROWTH OF CYBERSPACE

CCDCOE



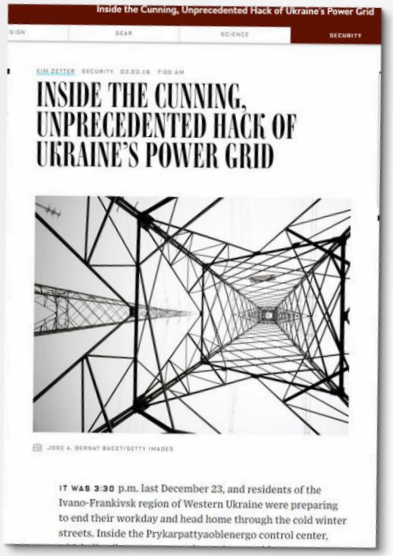
95 Countries developing legislative initiatives

77 Countries with national cybersecurity strategies

30+ Countries with declared offensive capabilities

20+ Cyber commands

EVOLVEMENT OF THREATS – MEDIA VIEW


Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center,


theguardian

news / opinion / sport / arts / life

tech / world / UK / science / cities / global development / more

Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

Nicky Woolf in San Francisco


The Washington Post

Federal Insider

Hacks of OPM databases compromised 22.1 million people, federal authorities say

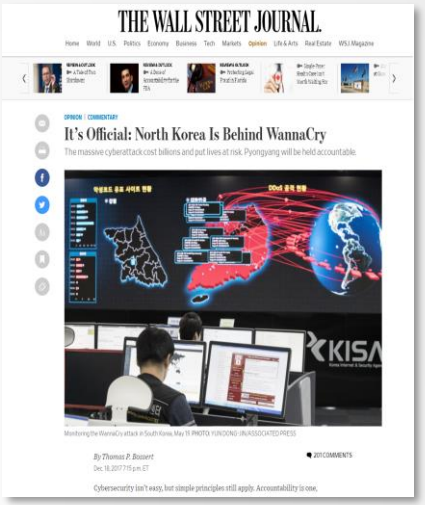
By Ellen Nakashima

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said Thursday.

The total vastly exceeds all previous estimates, and marks the most detailed accounting by the Office of Personnel Management of how many people were affected by cyber intrusions that U.S. officials have privately said were traced to the Chinese government.

[What you need to know about the hack of government background investigations]

But even beyond the rising number of apparent victims, U.S. officials said the breaches rank among the most potentially damaging cyber heists in U.S. government history because of the abundant detail in the files. Officials said hackers accessed not only personnel records


THE WALL STREET JOURNAL.

It's Official: North Korea Is Behind WannaCry

The massive cyberattack cost billions and put lives at risk. Pyongyang will be held accountable.


THE WALL STREET JOURNAL.

FBI Suspects Russia in Hack of John Podesta Emails

Top Russian officials meanwhile shifted away from denying a role in separate hacking of the Democratic Committee


THE WHITE HOUSE BLAMES RUSSIA FOR NOTPETYA, THE 'MOST COSTLY CYBERATTACK IN HISTORY'

IT'S BEEN NEARLY eight months since the malware known


The Telegraph

News

EU governments to warn cyber attacks can be an act of war

By James Crisp, BRUSSELS CORRESPONDENT


Support The Guardian

The Guardian

News | Opinion | Sport | Culture | Lifestyle

Winter Olympics was hit by cyber-attack, officials confirm

South Koreans refuse to comment on rumours Russia was behind the action as revenge for doping ban

EVOLVEMENT OF THREATS – USER'S VIEW

CCDCOE

- Viruses, worms, Trojans and other malware
- E-mail related risks
- Websites with malicious content
- Wireless Access points
- Social networks and engingeering
- BYOD
- Removable media
- Shoulder-surfing
- Portable devices
- Authentication mechanisms
- APT
- Ransomware

WHAT WE DO

CCDCOE

RESEARCH

TRAINING

EXERCISE

TECHNOLOGY

STRATEGY

OPERATIONS

LAW

FLAGSHIPS

CCDCOE

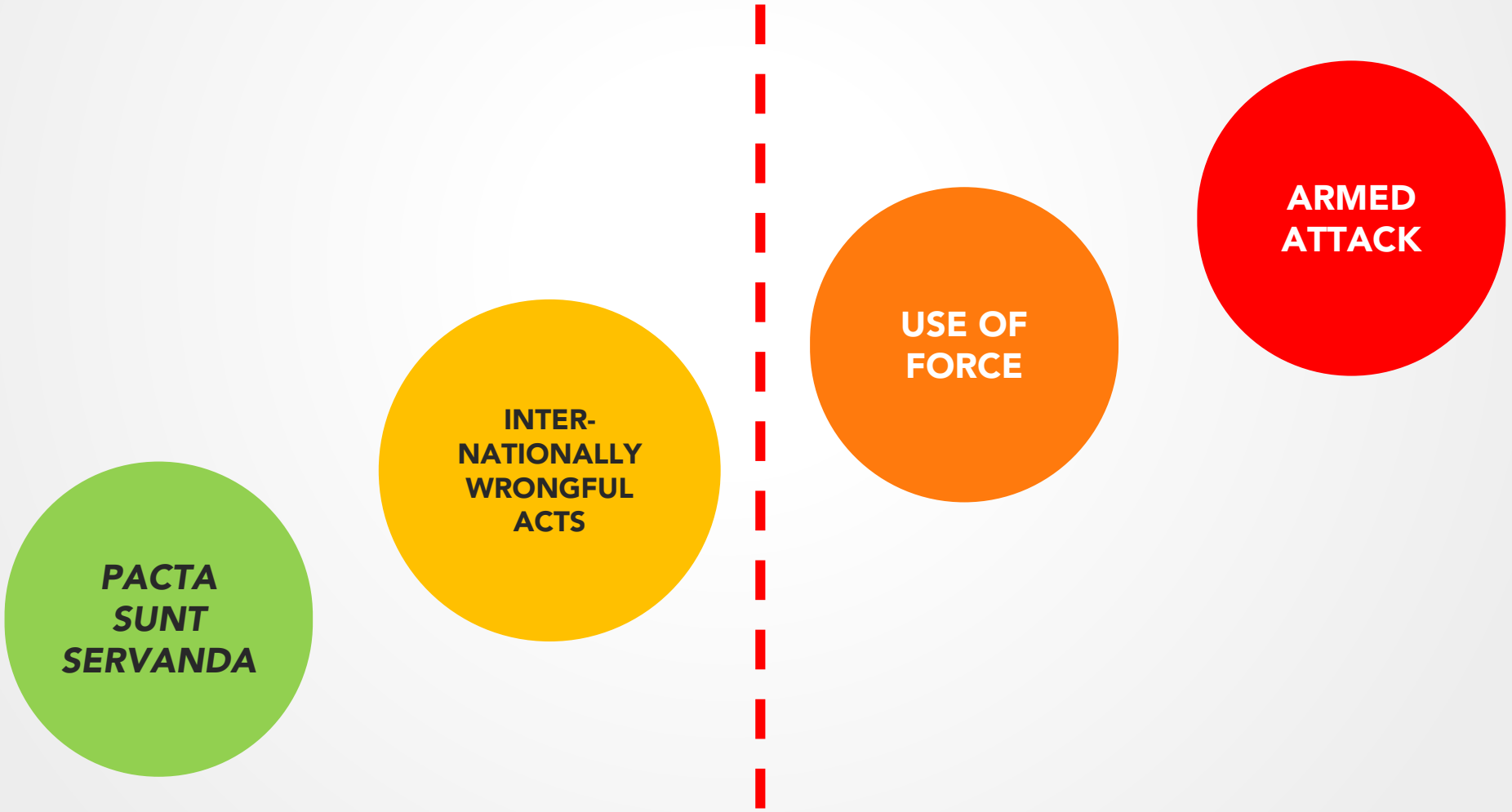
LOCKED SHIELDS

TALLINN MANUAL

CyCon
International Conference on Cyber Conflict

ROAD TO (CYBER) CONFLICT

CCDCOE



CONCLUSIONS

CCDCOE

- Sophistication, scale and tayloring of cyber attacks will only grow
- Maintain situational awareness
- Attribution and follow-up
- Discovery and protection against attacks over IPv6 network
- Keeping up networks and services under intense pressure
- Simultaneous strategic, technical, legal and media challenges
- Security of ICS/SCADA environments
- Cyber hygiene and threats-awareness
- Practical collaboration and information sharing
- Cross-border and cross-domain nature of cyber issues

Thank you!

siim.alatalu@ccdcoe.org