Patrik Fältström
paf@netnod.se

Head of Security

About Netnod

Key Facts
Founded: 1996
Main office: Stockholm, Sweden
Employed: 35
Owner: TU-Stiftelsen[1]

1. TU-Stiftelsen is a not for profit foundation with a goal that *the internet should work*

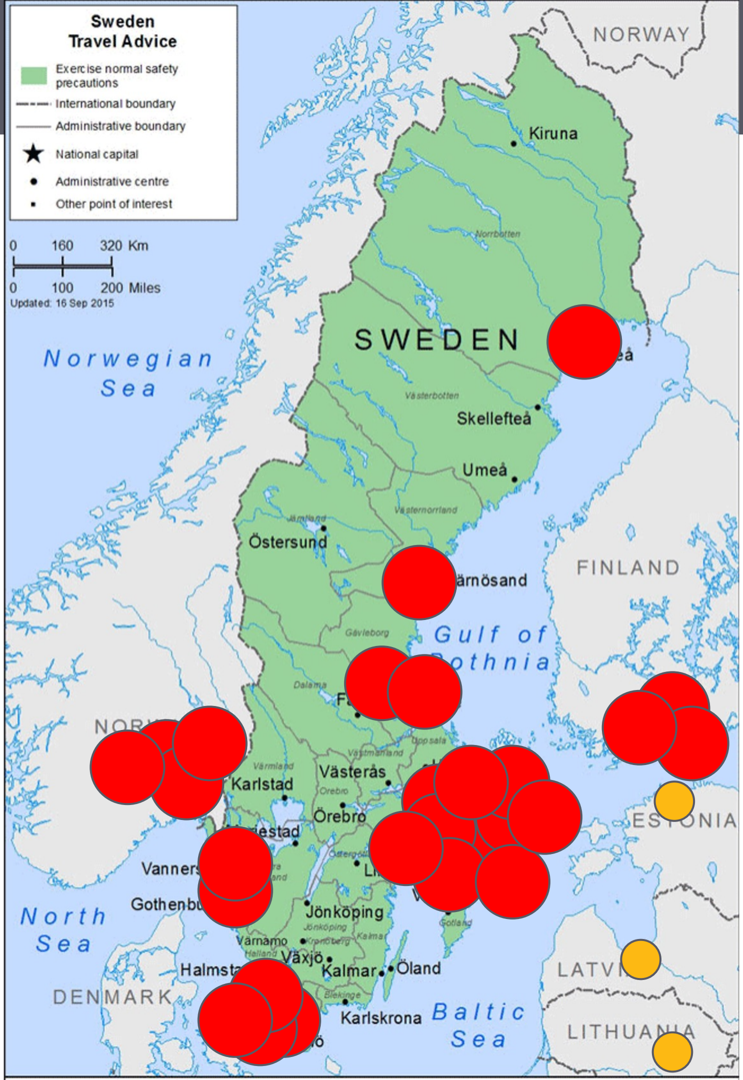
- A neutral organisation working with internet infrastructure
- The largest IXP in the Nordics
  - More than 250 connected networks https://www.netnod.se/ix/connected-networks
- Operates i.root-servers.net, one of 13 root servers in the world
- Offers DNS anycast to ccTLDs, enterprises and partners
- Responsible for distribution of time and frequency in Sweden
  - NTP, NTS and PTP - traceable to Swedish time UTC(SP)

Points of presence

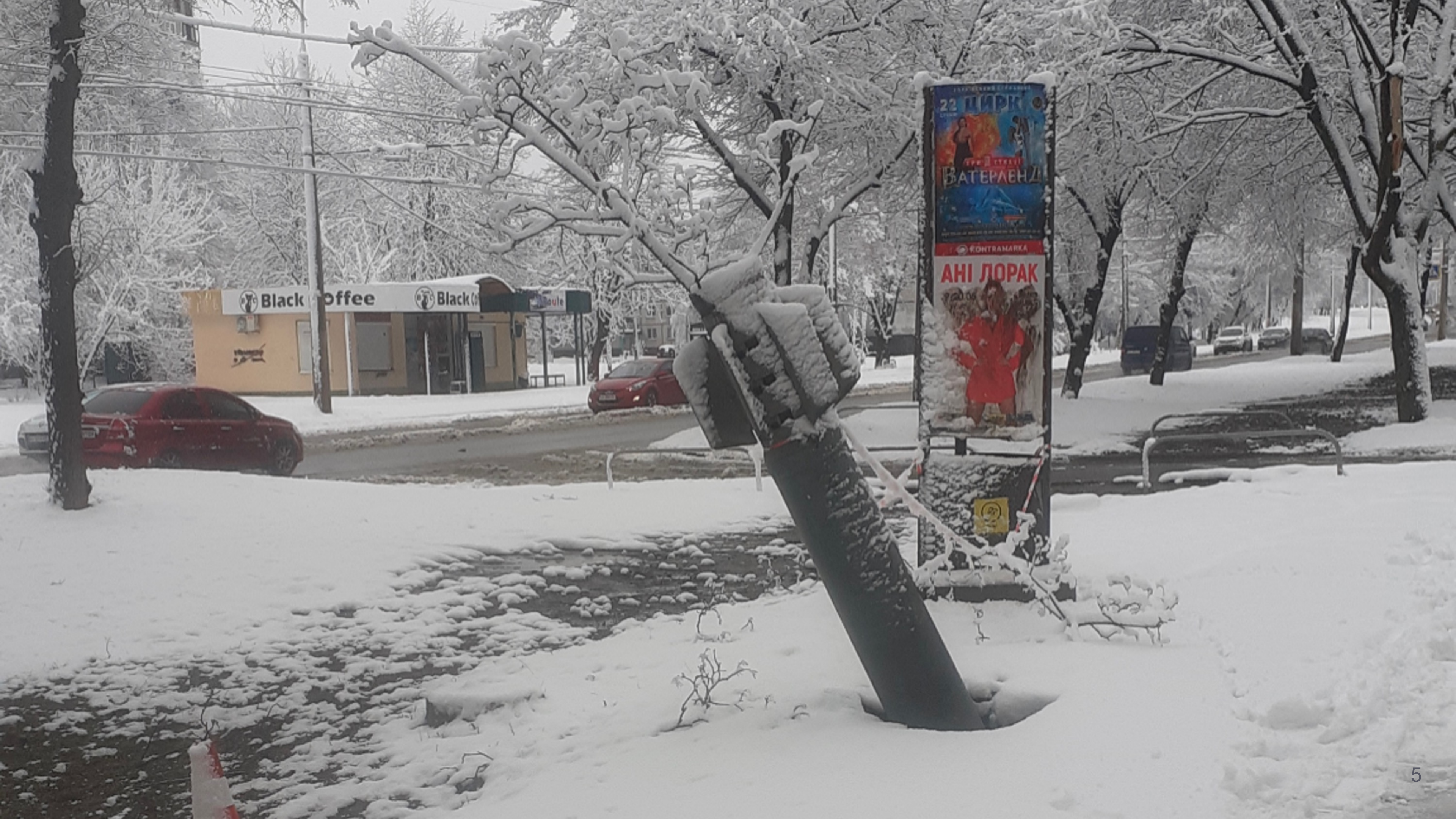
- Stockholm (10 locations)
- Gothenburg (2 locations)
- Copenhagen / Malmö (4 locations)
- Oslo (4 locations)
- Helsinki (3 locations)
- Sundsvall / Gävle (3 locations)
- Luleå (1 location)

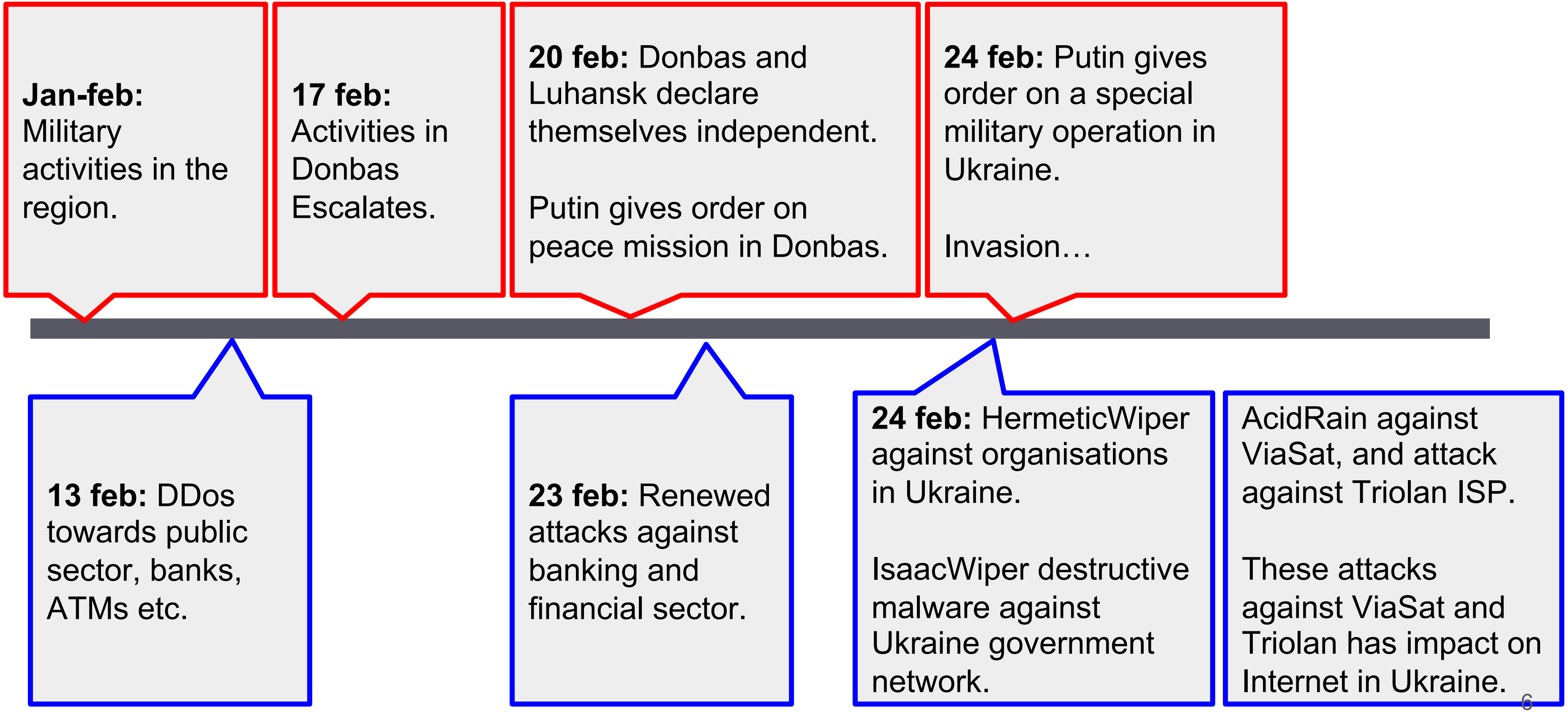
- Riga - DNS Only
- Vilnius - DNS Only
- Tallinn - DNS Only

~75 more locations around the world



“Everyone thinks they have a plan until they get punched in the face.”


Black Coffee
Black Co
22
ЦИРК
ВАТЕРЛЕНД
CONTRAMARKA
АНІ ЛОРАК



Jan-feb: Military activities in the region.

13 feb: DDos towards public sector, banks, ATMs etc.

17 feb: Activities in Donbas Escalates.

20 feb: Donbas and Luhansk declare themselves independent.

Putin gives order on peace mission in Donbas.

23 feb: Renewed attacks against banking and financial sector.

24 feb: Putin gives order on a special military operation in Ukraine.

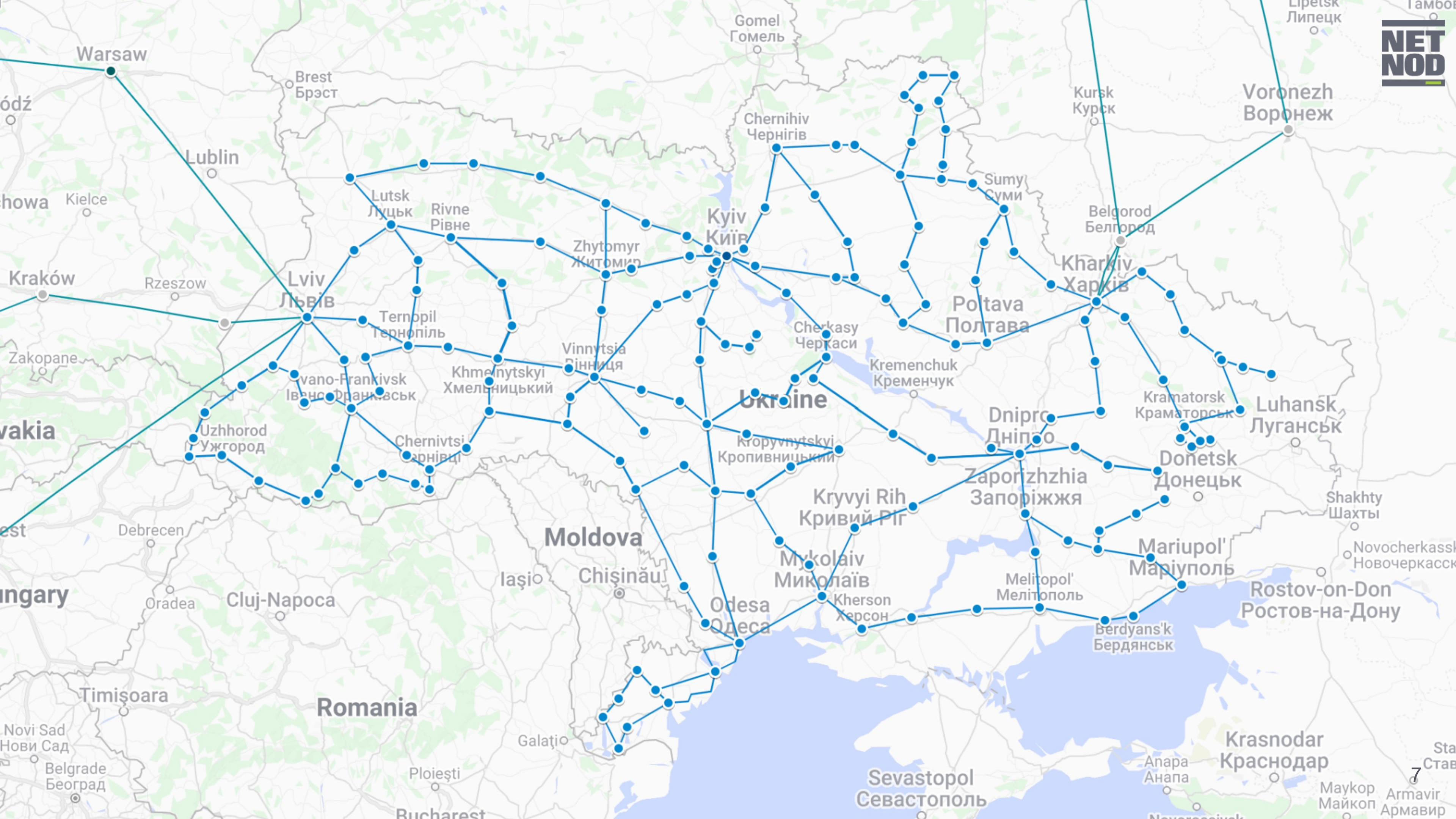
Invasion…

24 feb: HermeticWiper against organisations in Ukraine.

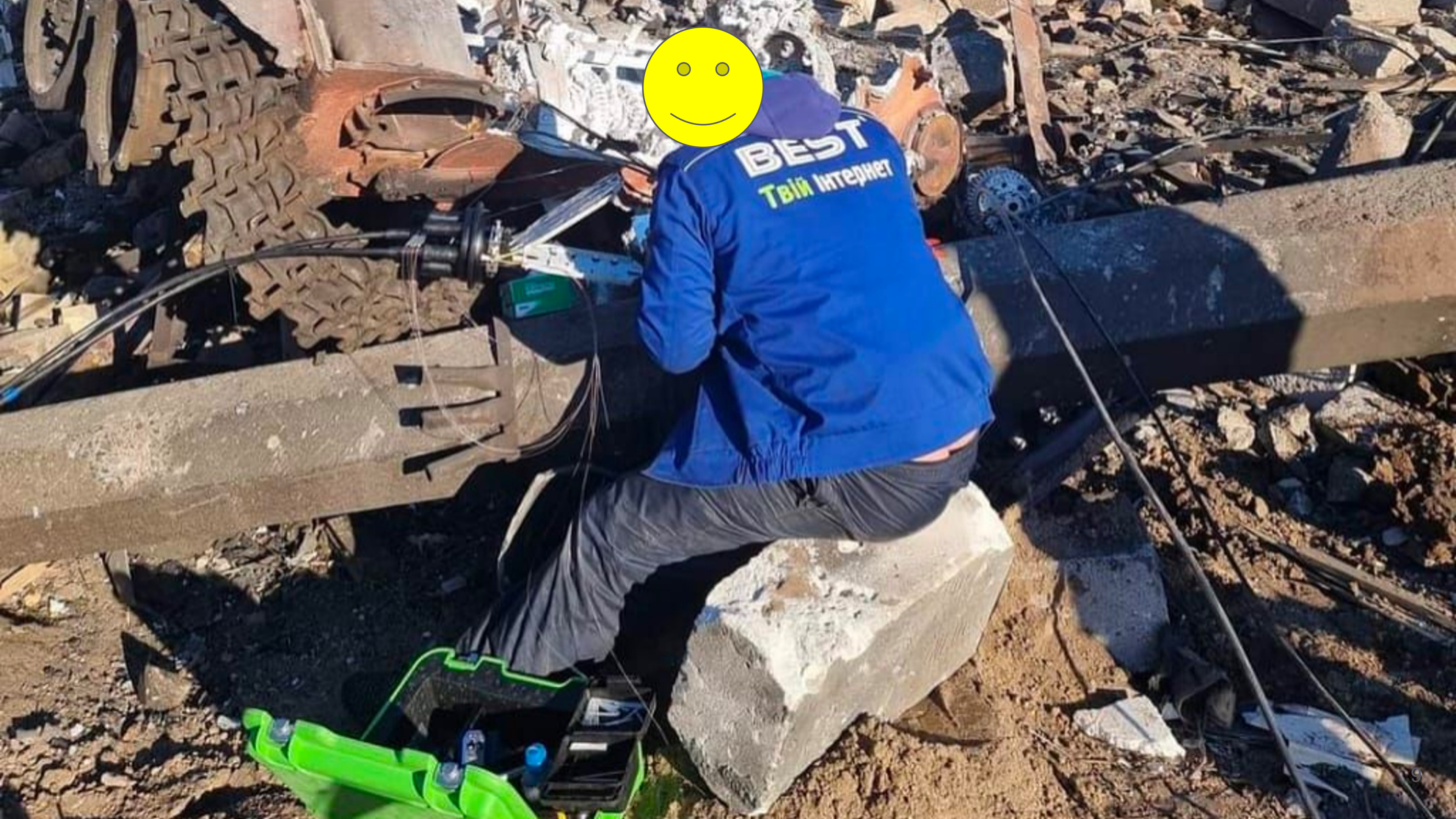
IsaacWiper destructive malware against Ukraine government network.

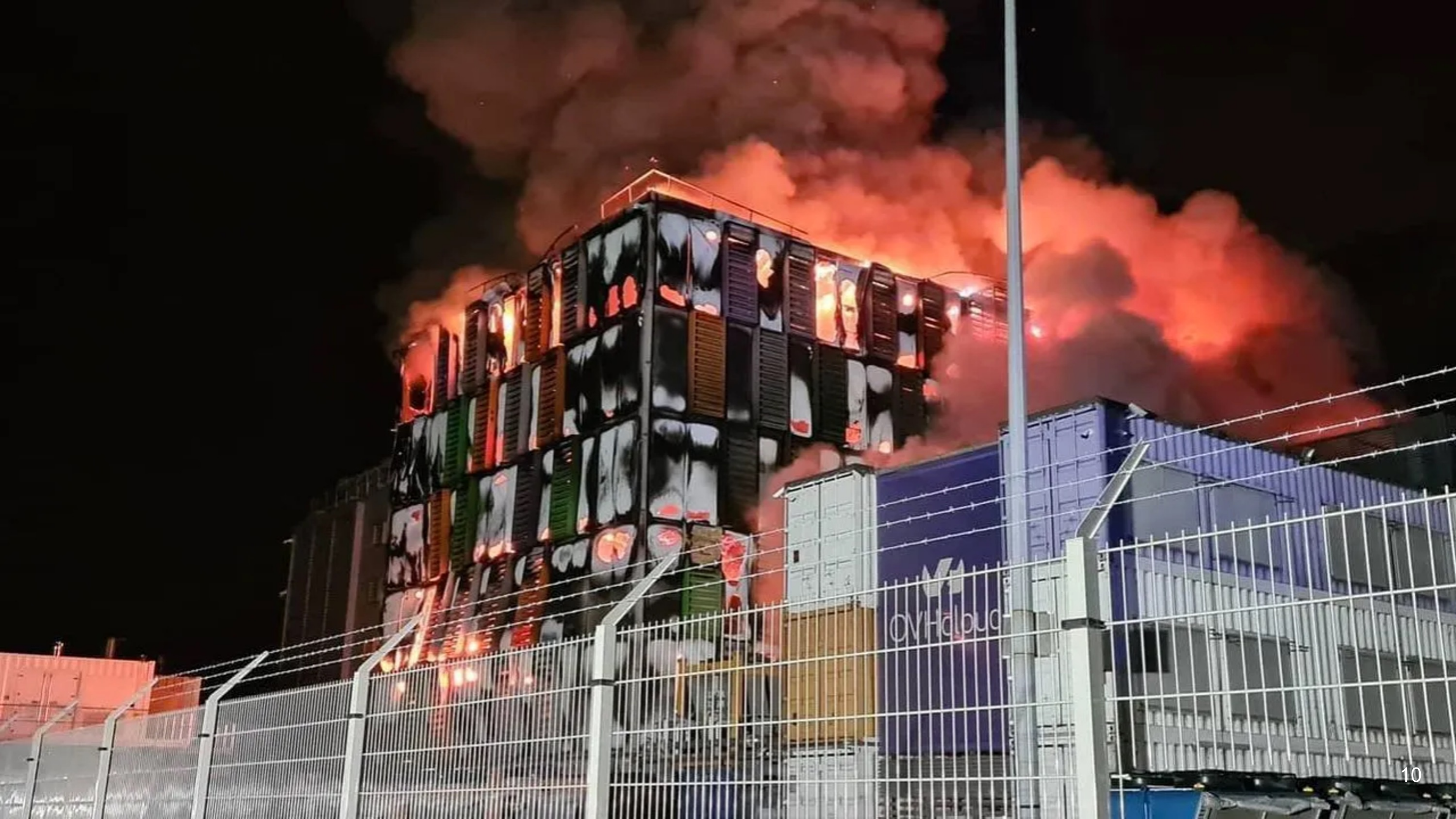
AcidRain against ViaSat, and attack against Triolan ISP.

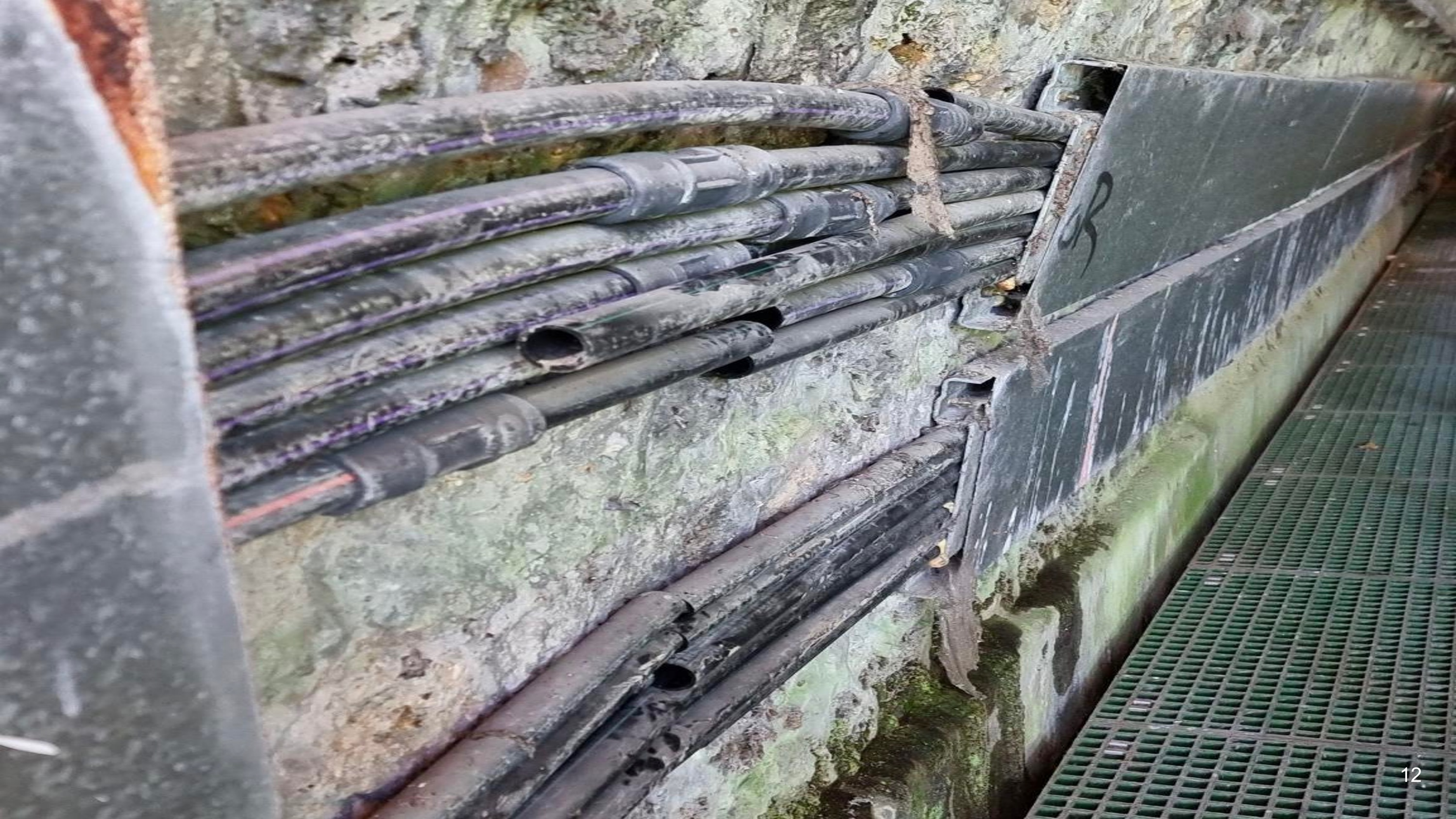
These attacks against ViaSat and Triolan has impact on Internet in Ukraine.

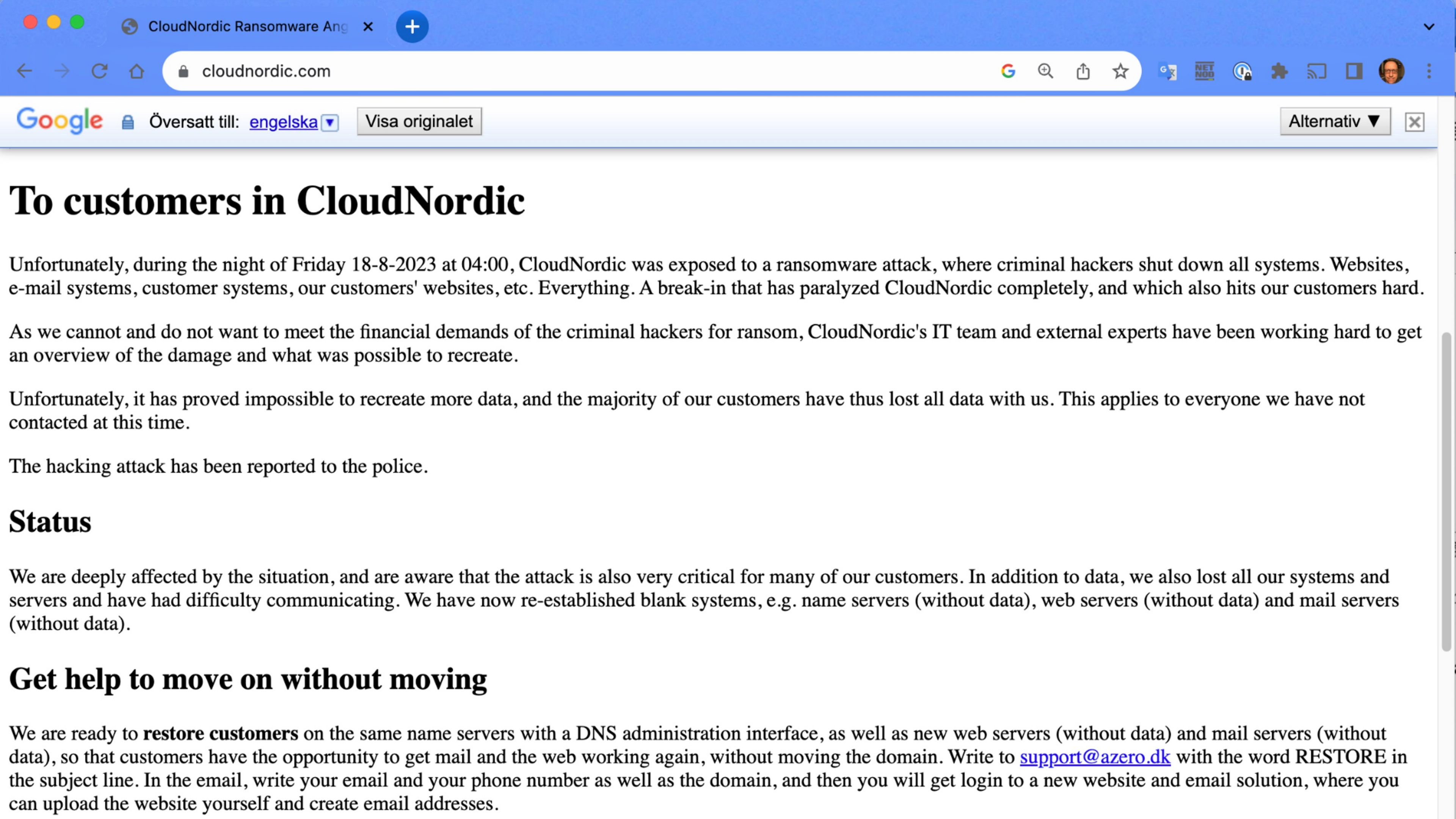

Warsaw
ódź
Brest
Брэст
Gomel
Гомель
Lipetsk
Липецк
Тамбо
Kursk
Курск
Voronezh
Воронеж
Chernihiv
Чернігів
Sumy
Суми
Belgorod
Белгород
Lublin
howa
Kielce
Lutsk
Луцьк
Rivne
Рівне
Kyiv
Київ
Zhytomyr
Житомир
Kraków
Rzeszow
Lviv
Львів
Ternopil
Тернопіль
Kharkiv
Харків
Poltava
Полтава
Cherkasy
Черкаси
Kremenchuk
Кременчук
Zakopane
Ivano-Frankivsk
Івано-Франківськ
Khmelnytskyi
Хмельницький
Vinnytsia
Вінниця
Ukraine
Kramatorsk
Краматорськ
Luhansk
Луганськ
vakia
Dnipro
Дніпро
Uzhhorod
Ужгород
Chernivtsi
Чернівці
Kropyvnytskyi
Кропивницький
Donetsk
Донецьк
Zaporizhzhia
Запоріжжя
Kryvyi Rih
Кривий Ріг
Shakhty
Шахты
est
Debrecen
Moldova
Mariupol'
Маріуполь
Novocherkassk
Новочеркасск
ngary
Iași
Chișinău
Mykolaiv
Миколаїв
Oradea
Cluj-Napoca
Odesa
Одеса
Kherson
Херсон
Melitopol'
Мелітополь
Rostov-on-Don
Ростов-на-Дону
Berdyans'k
Бердянськ
Timișoara
Romania
Novi Sad
Нови Сад
Belgrade
Београд
Galați
Krasnodar
Краснодар
Sta
Став
Anapa
Анапа
Ploiești
Sevastopol
Севастополь
Maykop
Майкоп
Armavir
Армавир
Bucharest

VEST


BEST
Твій Інтернет


OVHcloud





To customers in CloudNordic

Unfortunately, during the night of Friday 18-8-2023 at 04:00, CloudNordic was exposed to a ransomware attack, where criminal hackers shut down all systems. Websites, e-mail systems, customer systems, our customers' websites, etc. Everything. A break-in that has paralyzed CloudNordic completely, and which also hits our customers hard.

As we cannot and do not want to meet the financial demands of the criminal hackers for ransom, CloudNordic's IT team and external experts have been working hard to get an overview of the damage and what was possible to recreate.

Unfortunately, it has proved impossible to recreate more data, and the majority of our customers have thus lost all data with us. This applies to everyone we have not contacted at this time.

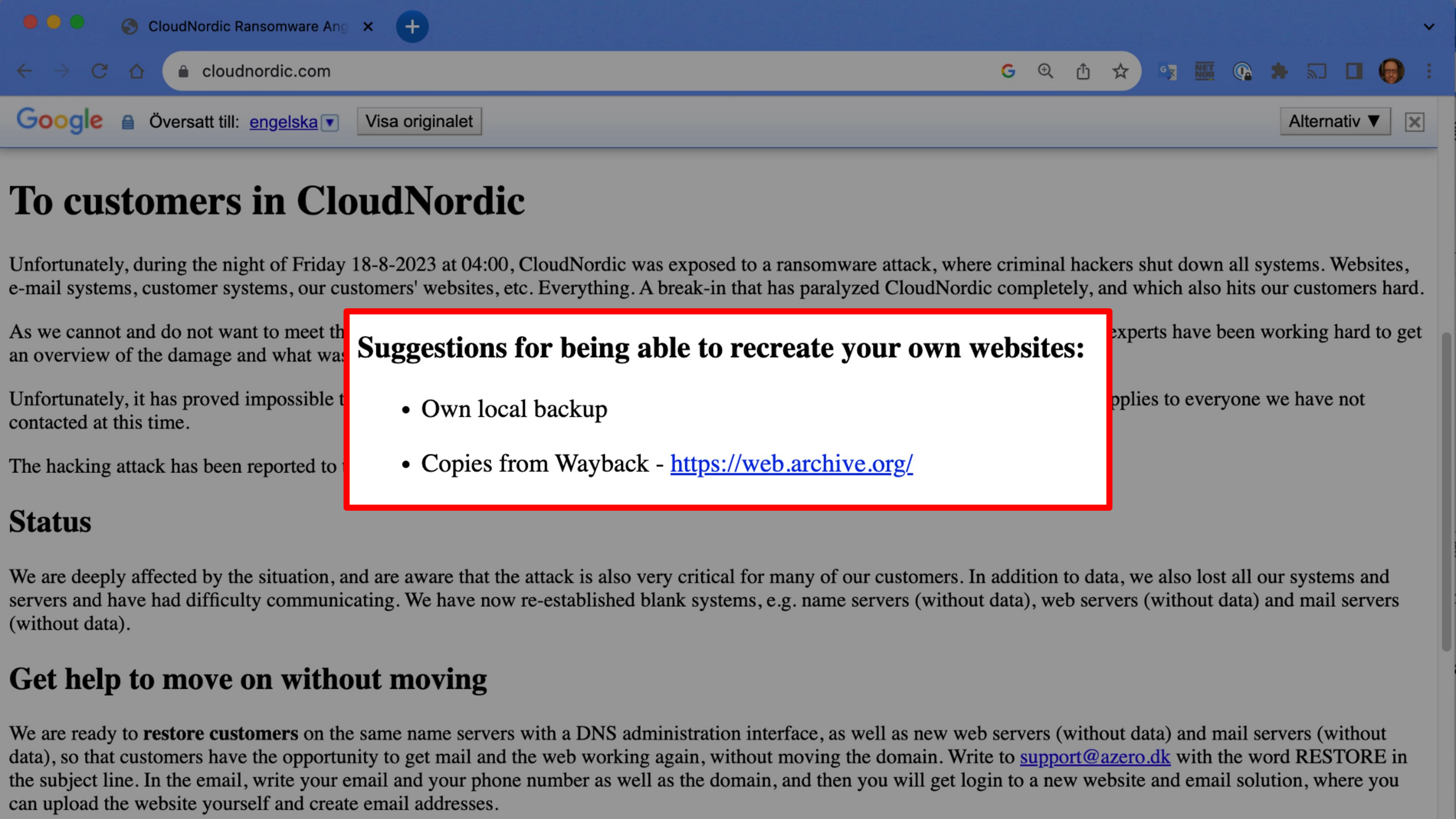
The hacking attack has been reported to the police.

Status

We are deeply affected by the situation, and are aware that the attack is also very critical for many of our customers. In addition to data, we also lost all our systems and servers and have had difficulty communicating. We have now re-established blank systems, e.g. name servers (without data), web servers (without data) and mail servers (without data).

Get help to move on without moving

We are ready to **restore customers** on the same name servers with a DNS administration interface, as well as new web servers (without data) and mail servers (without data), so that customers have the opportunity to get mail and the web working again, without moving the domain. Write to support@azero.dk with the word RESTORE in the subject line. In the email, write your email and your phone number as well as the domain, and then you will get login to a new website and email solution, where you can upload the website yourself and create email addresses.



To customers in CloudNordic

Unfortunately, during the night of Friday 18-8-2023 at 04:00, CloudNordic was exposed to a ransomware attack, where criminal hackers shut down all systems. Websites, e-mail systems, customer systems, our customers' websites, etc. Everything. A break-in that has paralyzed CloudNordic completely, and which also hits our customers hard.

As we cannot and do not want to meet th … xperts have been working hard to get an overview of the damage and what was …

Unfortunately, it has proved impossible t … pplies to everyone we have not contacted at this time.

The hacking attack has been reported to t …

Suggestions for being able to recreate your own websites:

- Own local backup
- Copies from Wayback - https://web.archive.org/

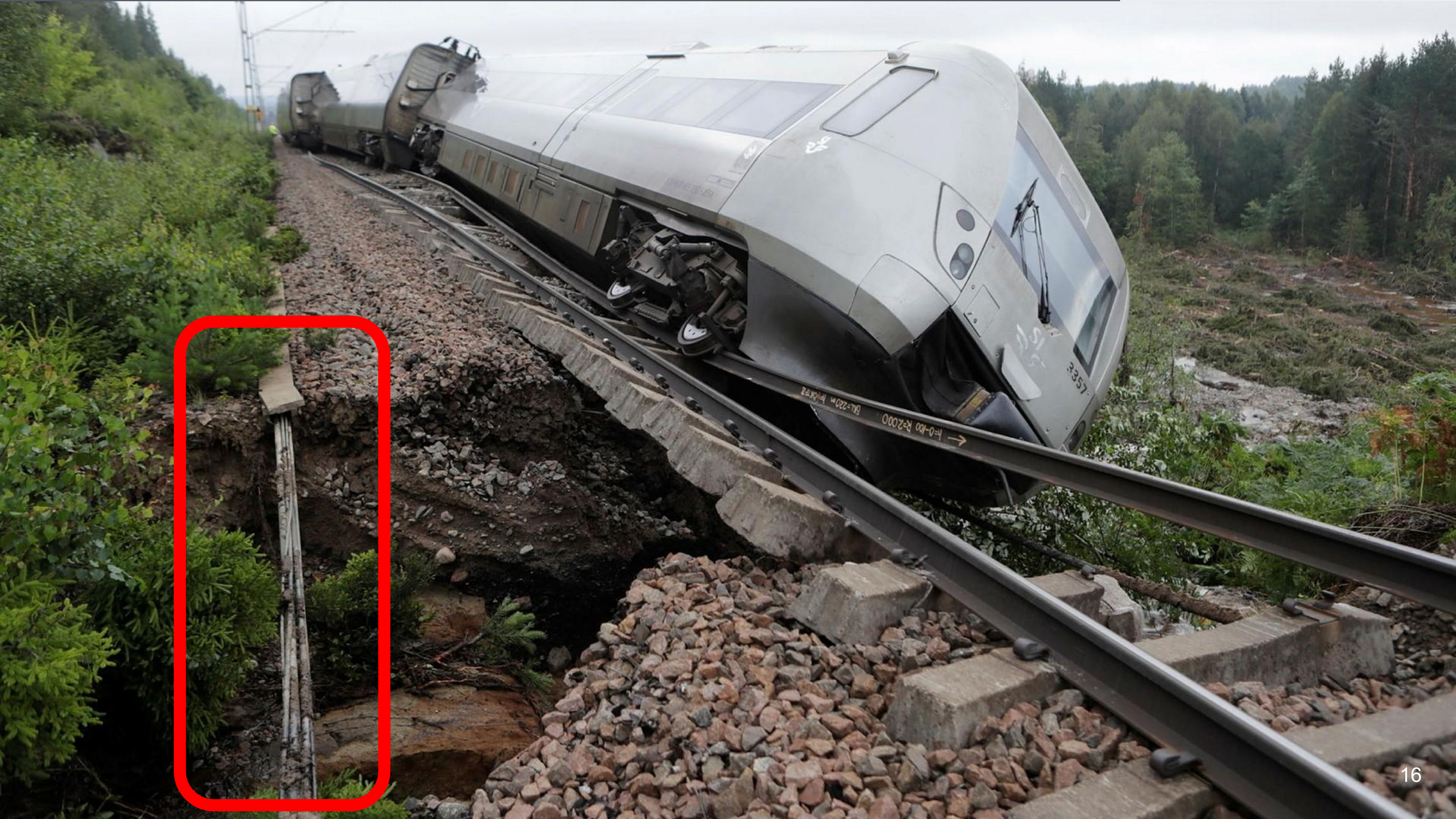
Status

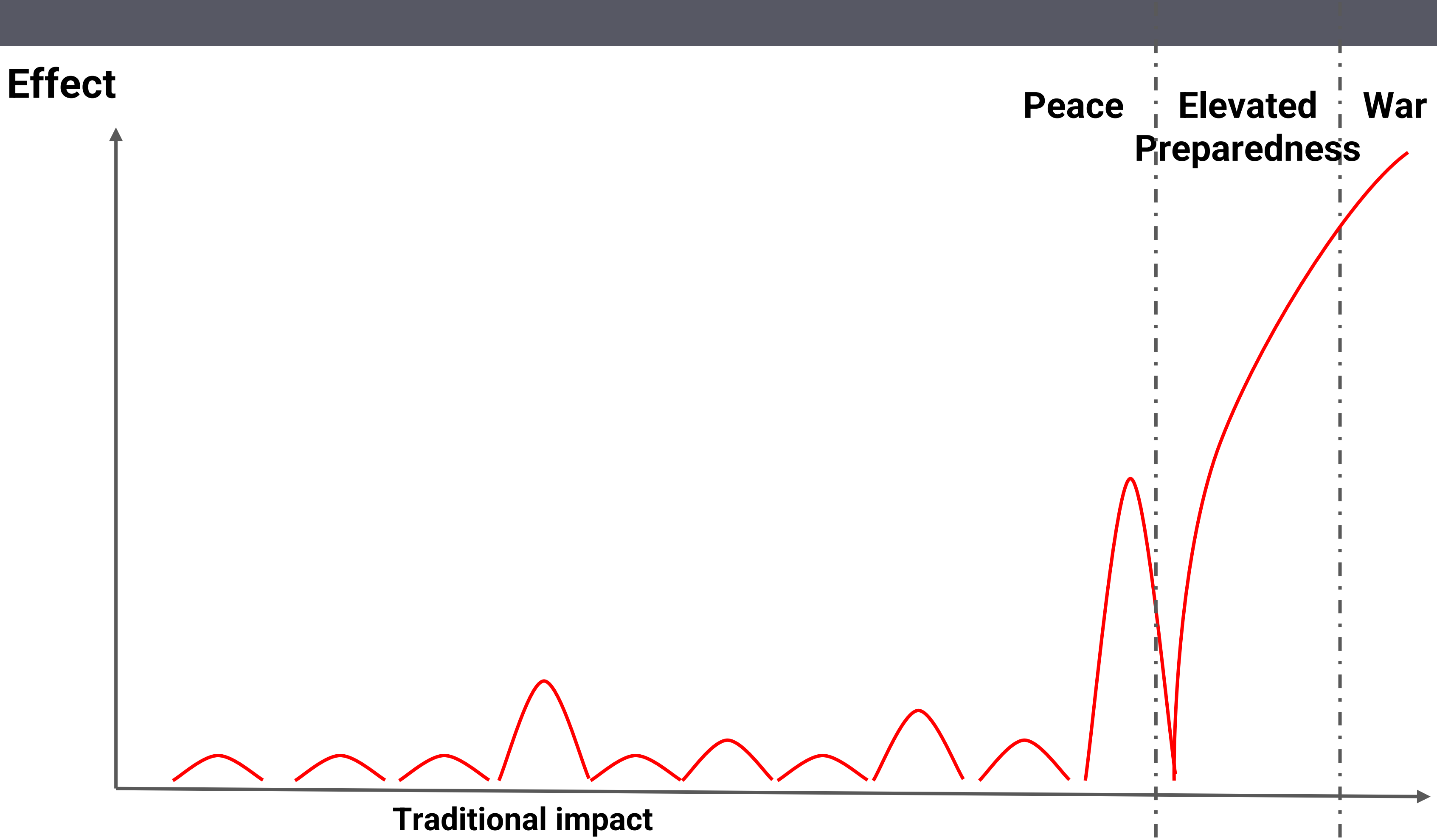
We are deeply affected by the situation, and are aware that the attack is also very critical for many of our customers. In addition to data, we also lost all our systems and servers and have had difficulty communicating. We have now re-established blank systems, e.g. name servers (without data), web servers (without data) and mail servers (without data).

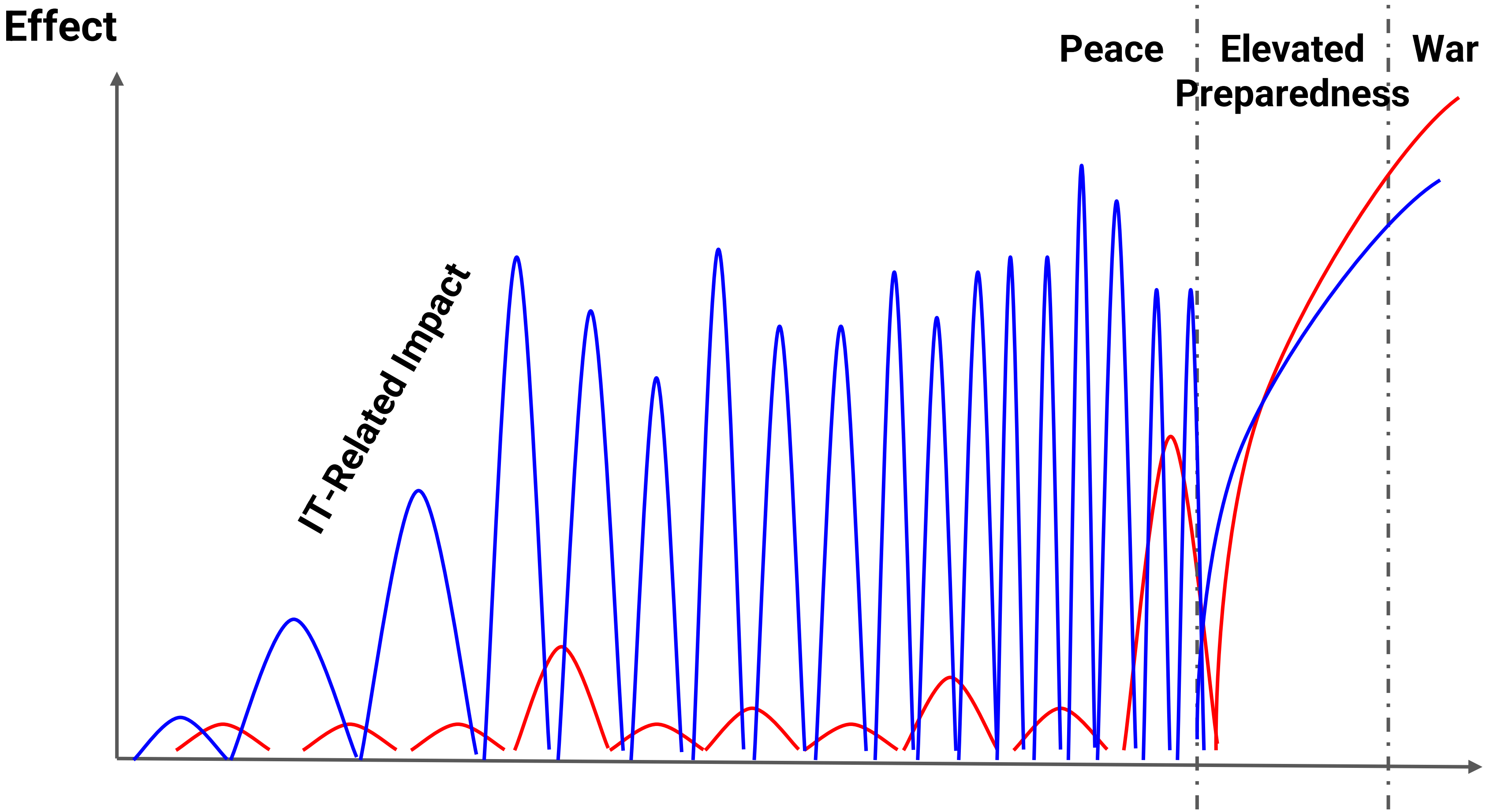
Get help to move on without moving

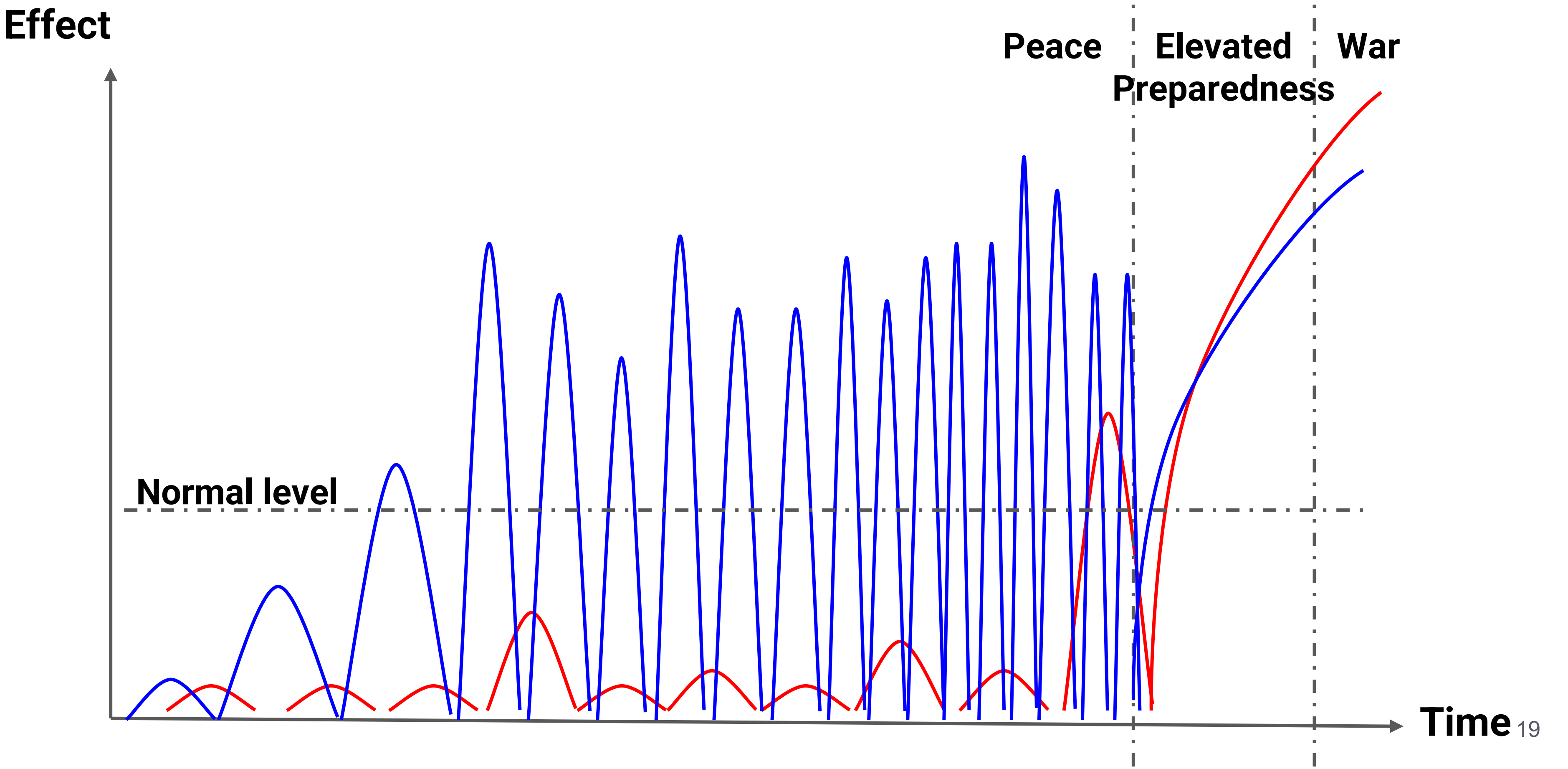
We are ready to **restore customers** on the same name servers with a DNS administration interface, as well as new web servers (without data) and mail servers (without data), so that customers have the opportunity to get mail and the web working again, without moving the domain. Write to support@azero.dk with the word RESTORE in the subject line. In the email, write your email and your phone number as well as the domain, and then you will get login to a new website and email solution, where you can upload the website yourself and create email addresses.

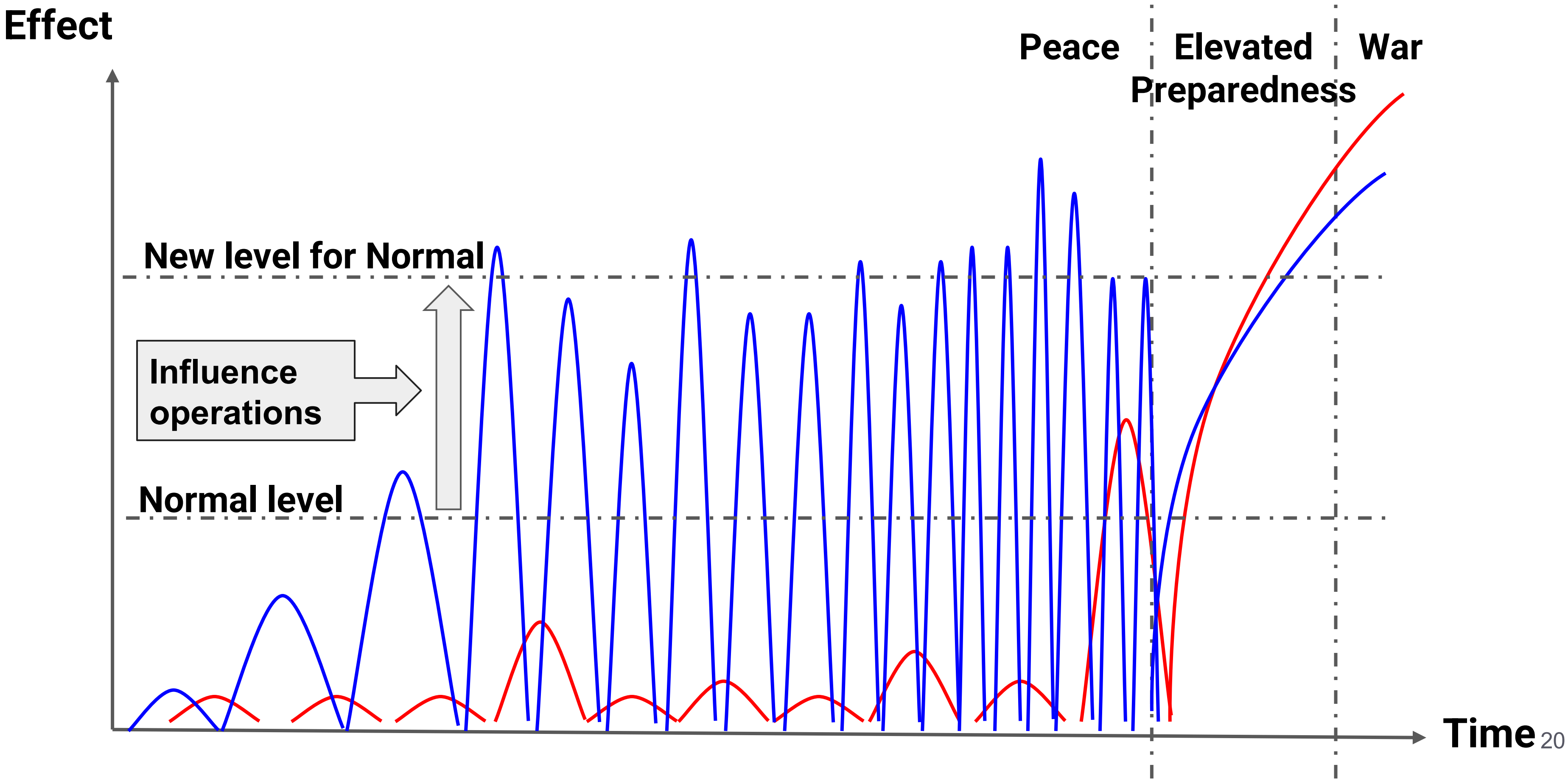
3357
BKL=220 m
h=0-100 R=2000

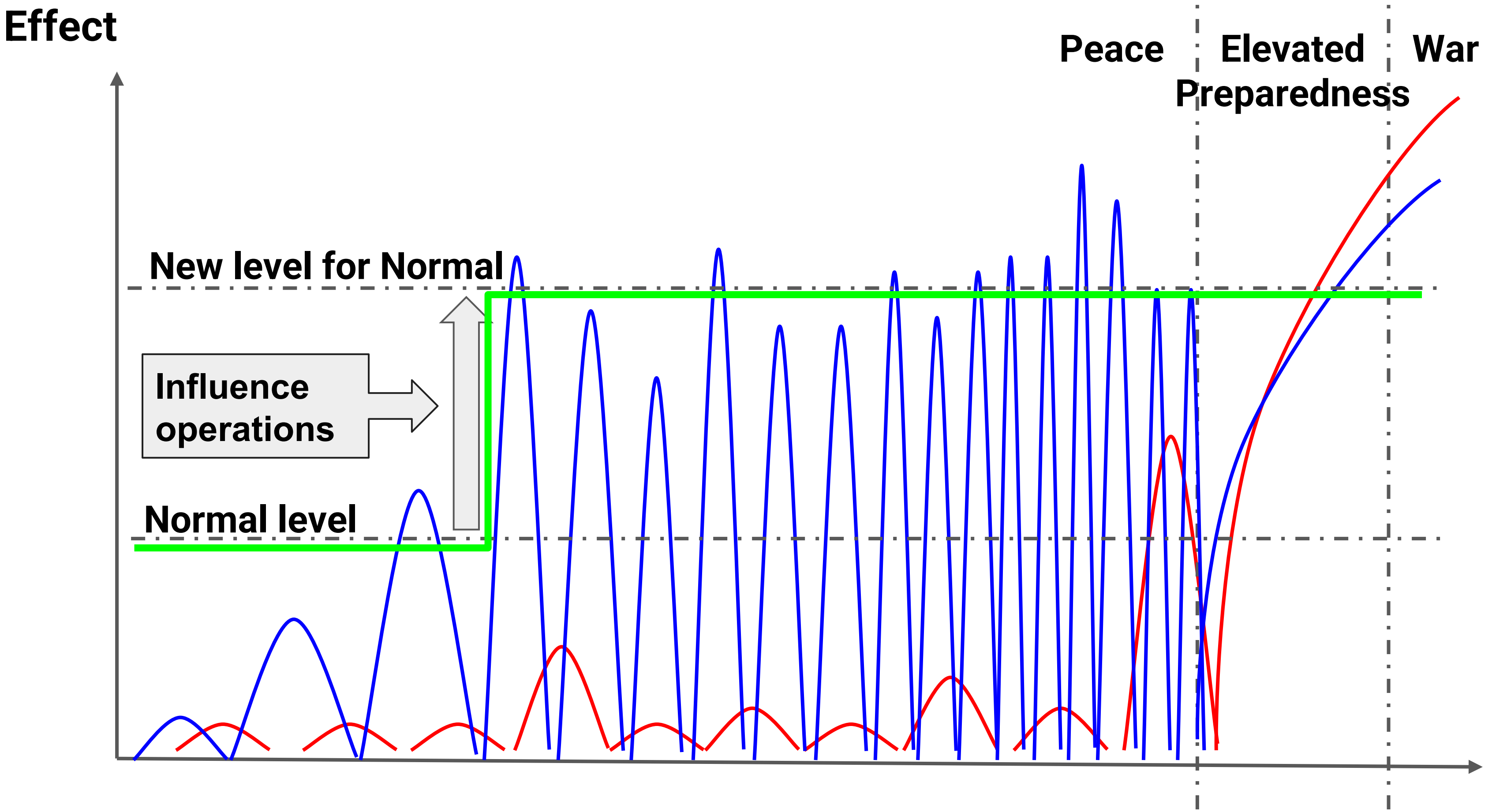

BLL=220 m
h=0-100 R=2000
3357


Effect
Peace
Elevated Preparedness
War
Time
Traditional impact

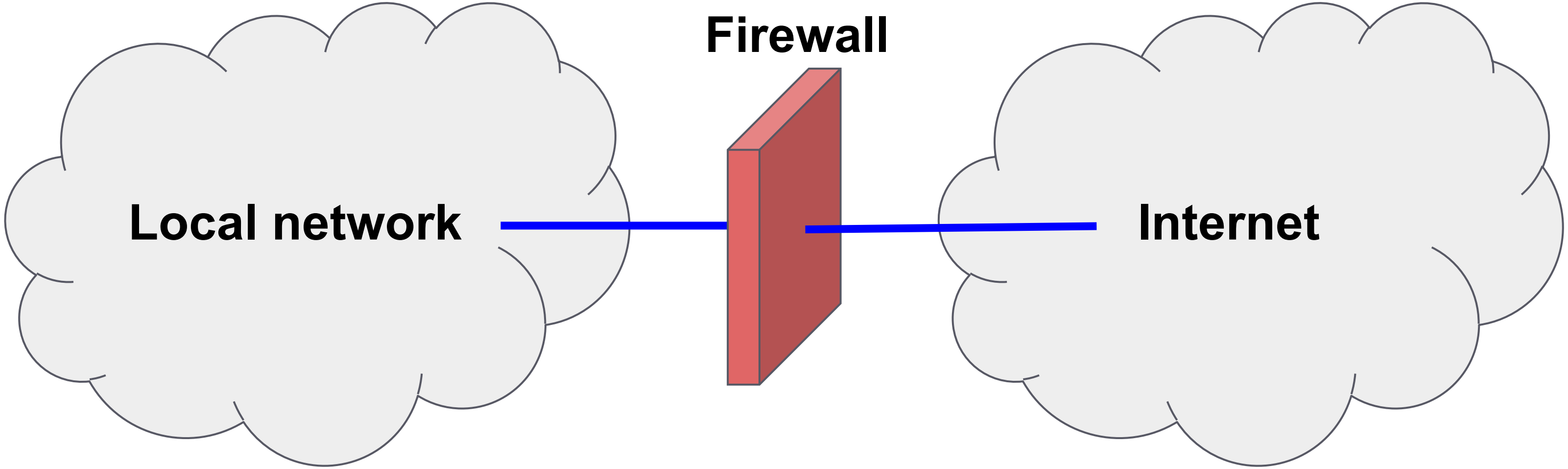

Effect
Peace
Elevated Preparedness
War
IT-Related Impact
Time


Effect
Peace
Elevated
Preparedness
War
Normal level
Time

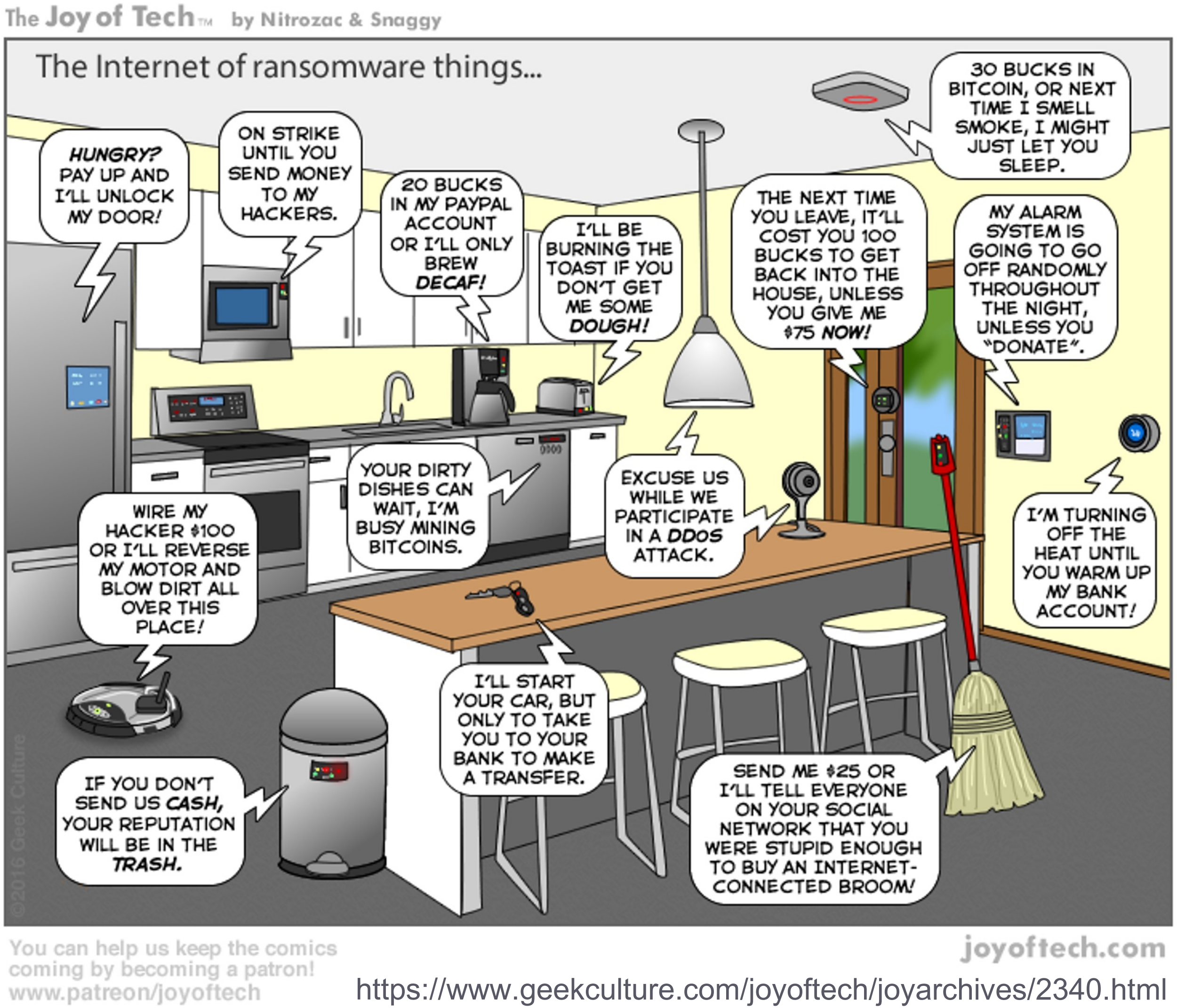

Effect
Peace
Elevated Preparedness
War
New level for Normal
Influence operations
Normal level
Time


Effect
Peace
Elevated Preparedness
War
New level for Normal
Influence operations
Normal level
Time

1993



2023


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

https://www.geekculture.com/joyoftech/joyarchives/2340.html

From pipes to a lasagna

Traditional deployment in ”pipes” implies a tight control throughout the infrastructure

Services

Companies, public sector and others offer services like web, email and apps to companies, citizens and consumers.

Internet Access

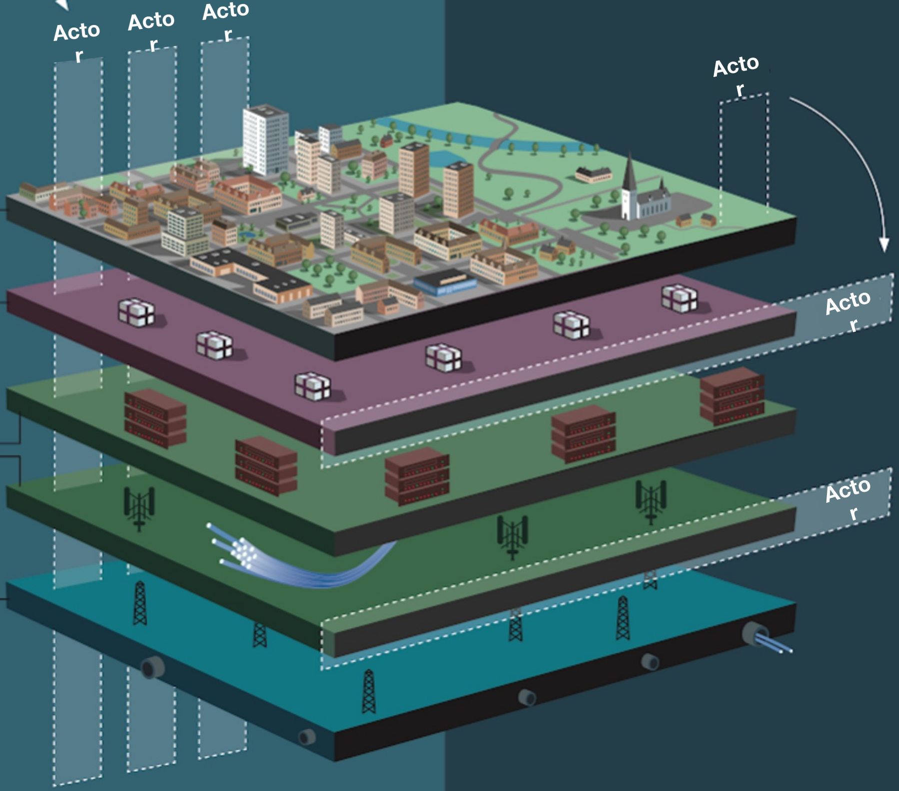
Internet- and mobile operators give companies and consumers access to Internet.

Active infrastructure

Transmission providers ensure transport of data to internet- and mobile operators.

Passive infrastructure

Ducts, fibre, masts etc. Built by municipalities, private companies and others.



A continuous change towards a partial horizontal division of roles implies requirement for different control mechanisms throughout the architecture, between layers.

Pros:

- Simpler management of control
- Increased ability to innovate
- Standardization leads to replaceability of products and services

Cons:

- ”Markets” on different layers that do not work as efficient as possible
- Lack of control and planning
- Low skills regarding procurement
- Non-optimal risk management for the society as a whole

Swedish Government Security Strategy - 2017

Nationell säkerhetsstrategi

Regeringskansliet
Statsrådsberedningen

- To cater for residents' safety, security and health
- To secure availability and functionality of important functions in the society
- To maintain fundamental values: democracy, rule of law, human rights and freedoms
- To under all circumstances defend Sweden's freedom, security and right to self-determination

Threats against these

- Military threats
- Information- and cyber security, digital risks
- Terrorism and violent extremism
- Organised crime
- Threats to energy supply and distribution
- Threats to logistics and infrastructure
- Threats to health issues

Swedish Government Security Strategy - 2017

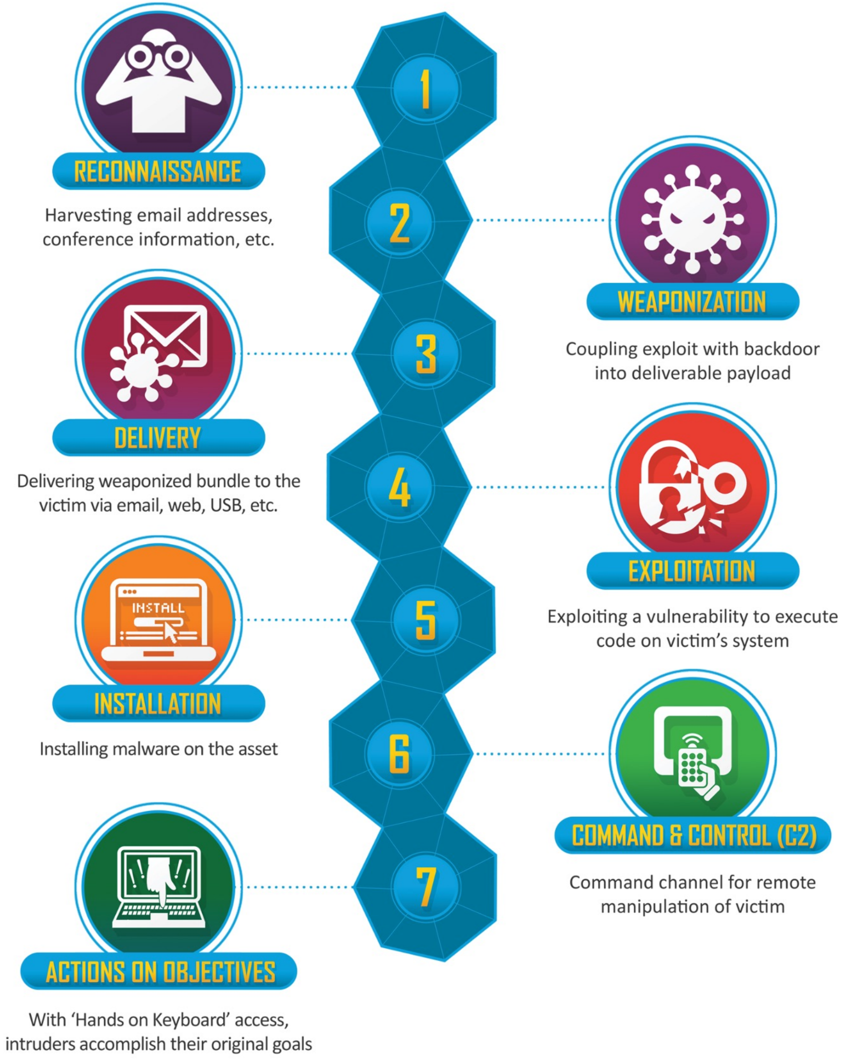
Nationell säkerhetsstrategi

Regeringskansliet
Statsrådsberedningen

- To cater for residents' safety, security and health
- To secure availability and functionality of important functions in the society
- To maintain fundamental values: democracy, rule of law, human rights and freedoms
- To under all circumstances defend Sweden's freedom, security and right to self-determination

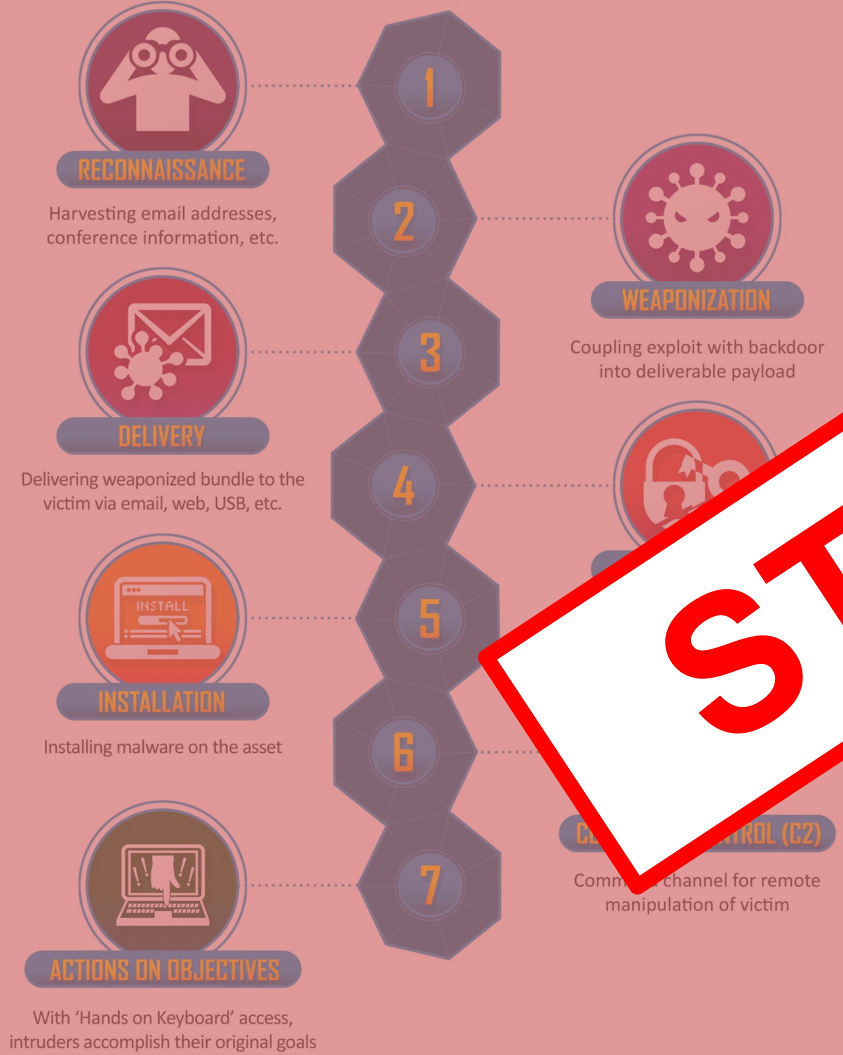
Threats against these

- Military threats
- Information- and cyber security, digital risks
- Terrorism and violent extremism
- Organised crime
- Threats to energy supply and distribution
- Threats to logistics and infrastructure
- Threats to health issues


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Lockheed Martin Cyber Kill Chain

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
5
INSTALL
INSTALLATION
Installing malware on the asset
6
C TROL (C2)
Comm channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

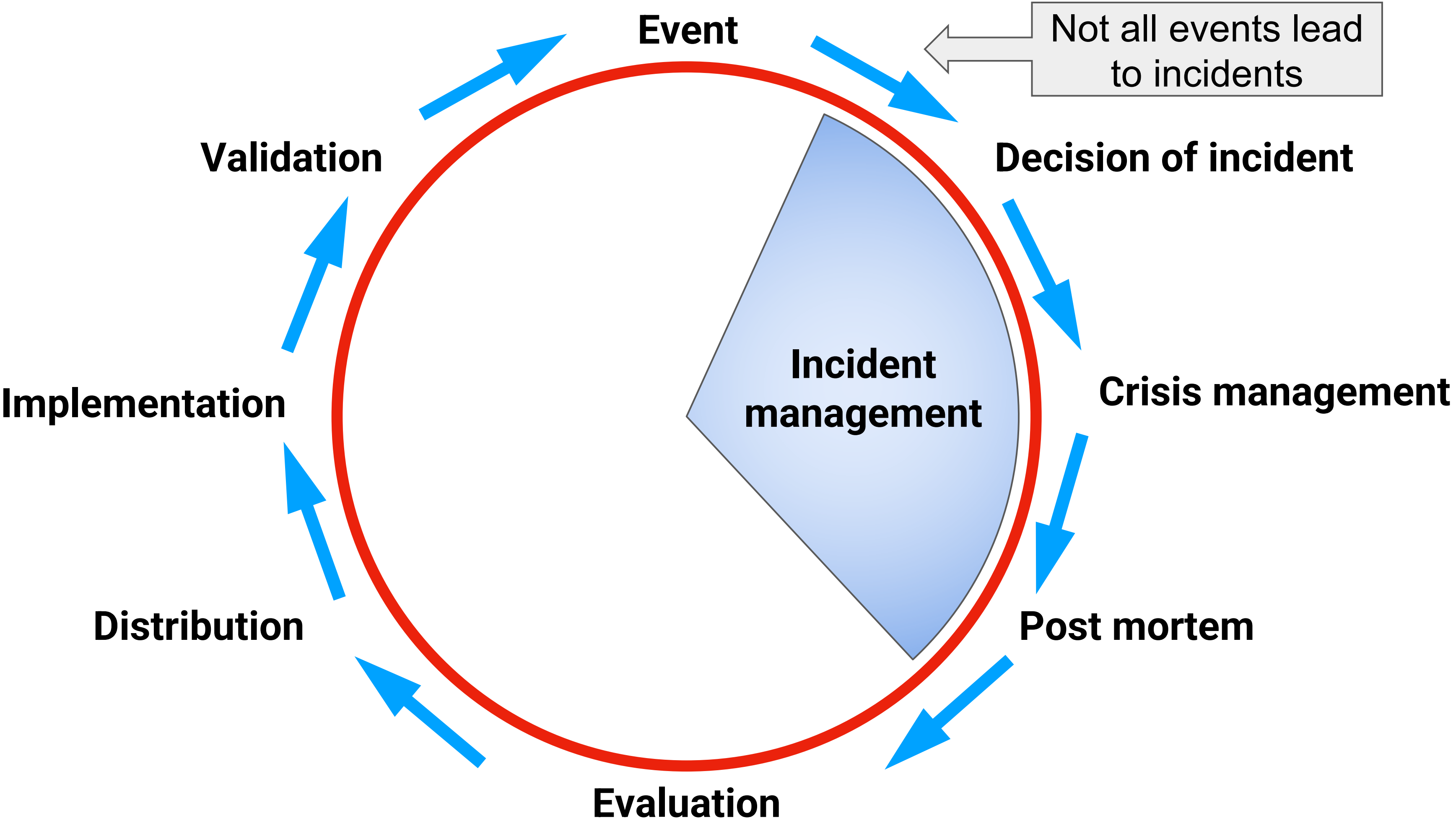
L artin
hain

STOP!

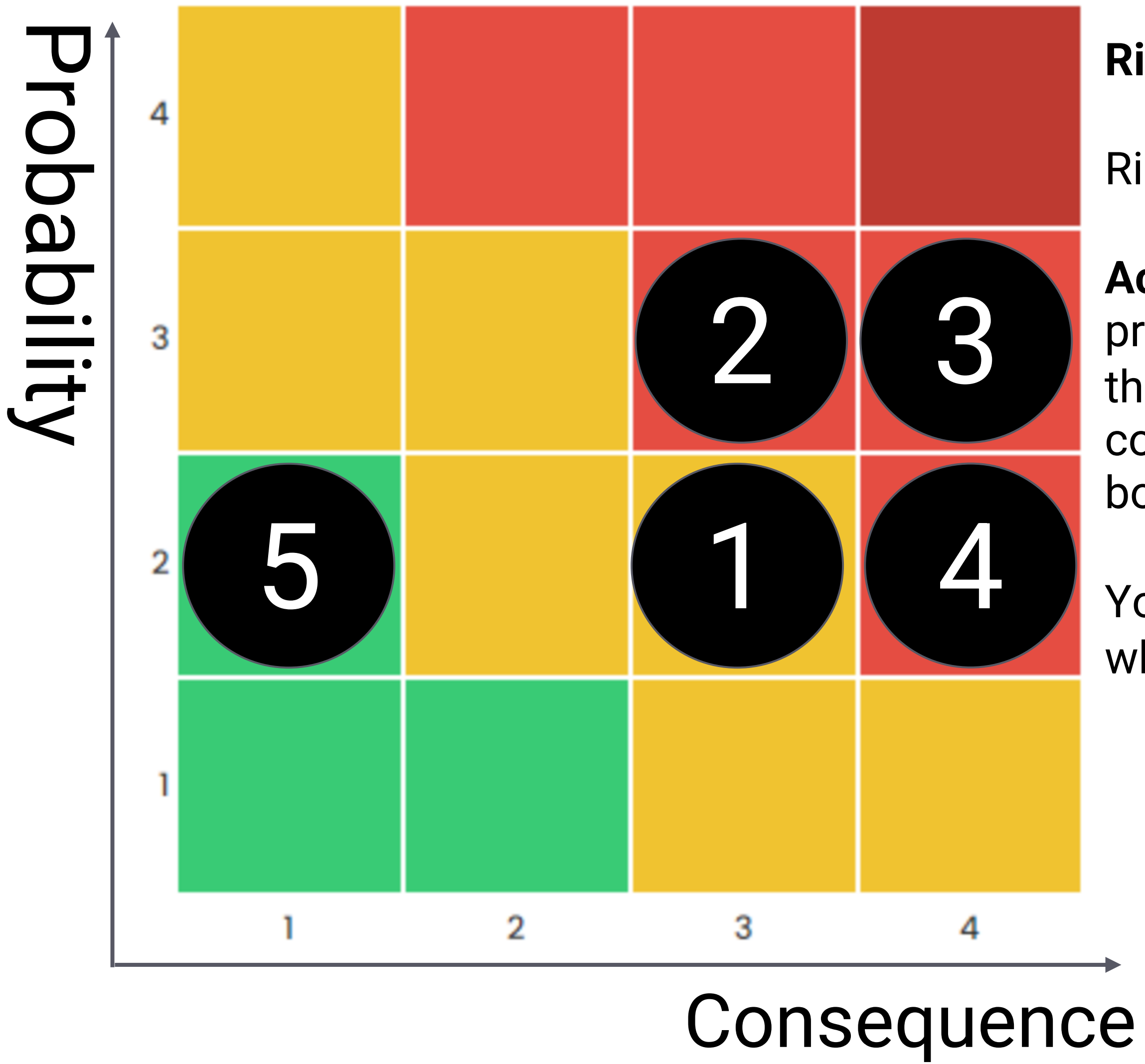
://www.lockheedmartin.com/
-us/capabilities/cyber/cyber-
kill-chain.html

Simpler model, 3 steps:

1. **Intrusion**
   How do I minimize the risk antagonist can gain a foothold?
1. **Horizontal movement**
   How do I minimize the ability for the antagonist to move?
1. **Attack**
   How do I protect what is to be protected?



Not all events lead to incidents

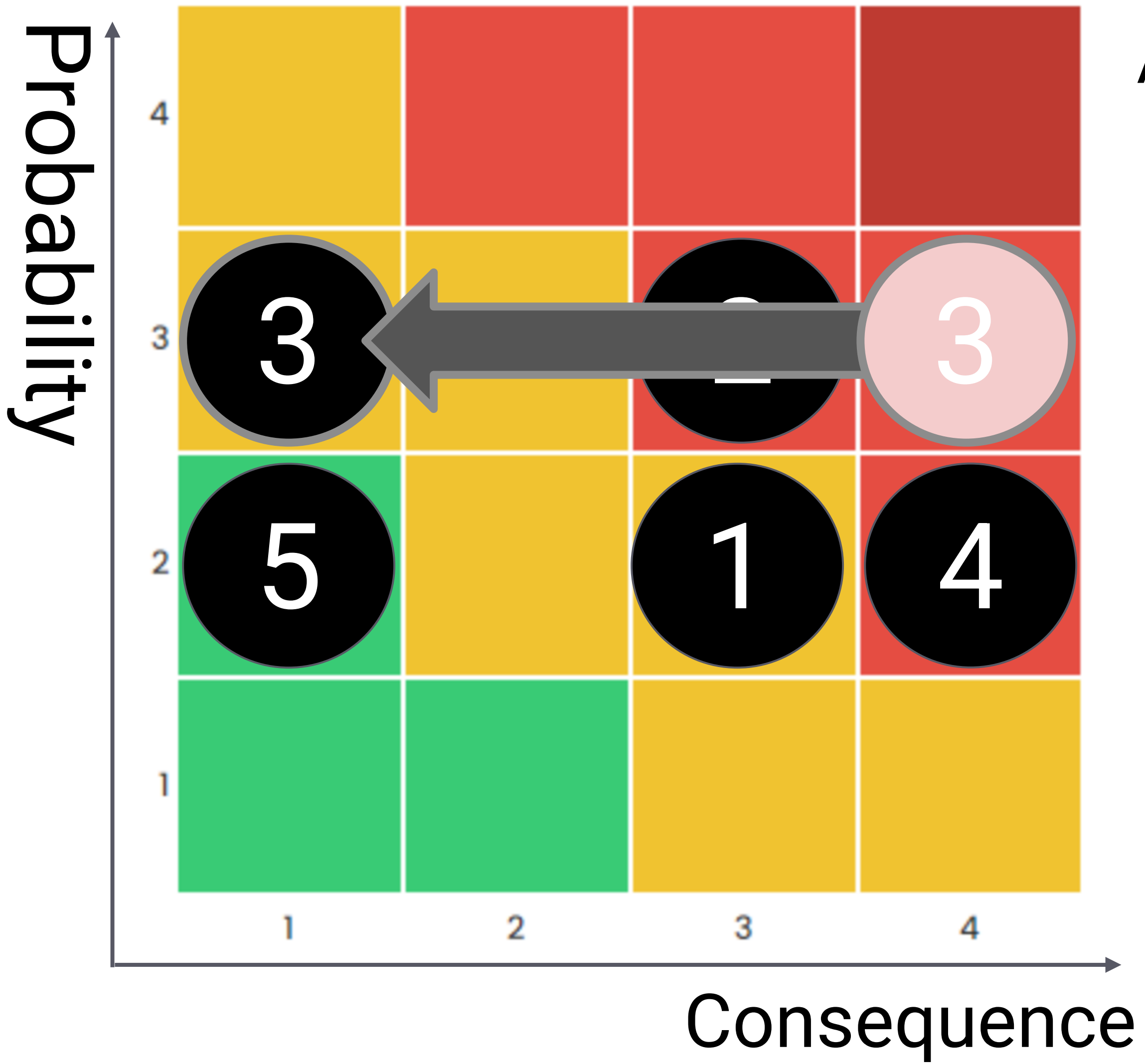


Risk matrix

Risk = (probability x consequence)

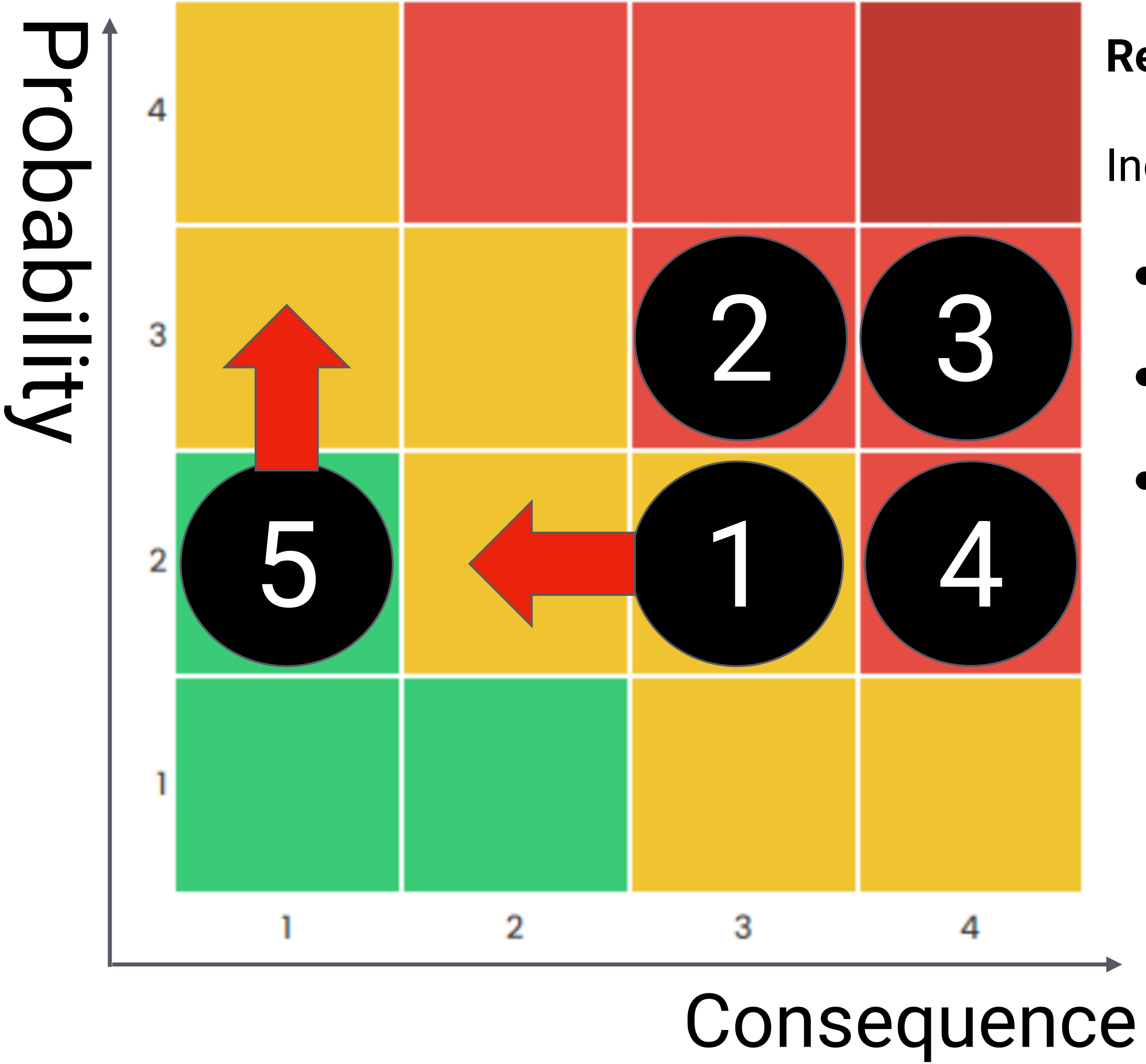
Actions are sought that lower the probability of **events** occurring, or that they lead to negative consequences if they do occur, or both.

You can accept a certain risk, which I call risk appetite.



Actions:

- **Do A**
    - Limit consequence if event 3 happens
- Do B
- Do C
- Do D
- Do nothing



Repeated reports

Indicate for each possible event:

- If the consequence have increased or decreased
- If the probability have increased or decreased
- If it is no longer on the radar (removed), or if it is a new possible event (added)

Control, leadership and obedience

- A well-functioning **pre-planned** coordination leads to a **reduced** need for coordination when handling incidents
- More robust communication is achieved through an **in advance** planned **and practiced** coordination between actors
- **This applies to everyone** who conducts or affects total defense activities
- In addition, there is a need for effect **much earlier** than has traditionally been the case, **before** tools, such as legislation, at elevated preparedness are possible to use

Recommendations

1. **Do a risk assessment, a scenario analysis**

   What events can hit us, and what happens when they do?

1. **Develop plans, and deploy (some) mitigation strategies**

   How can we ensure we are never surprised?

1. **Use cloud architecture**

   Be prepared to move data, compute and storage!

1. **Use a lasagna**

   Separate applications from ip and transport (fiber / mobile)

NET
NOD

netnod.se

Greta Garbos Väg 13, 169 40 Solna, Sweden
info@netnod.se