

# Swiss Cyber 2022: Public Attack Surface, Crypto Nodes and Threat Protection



**Nicolas Mayencourt**

Keynote | Lausanne, 22. November



# Dreamlab Technologies

## Introduction



### **Nick Mayencourt**

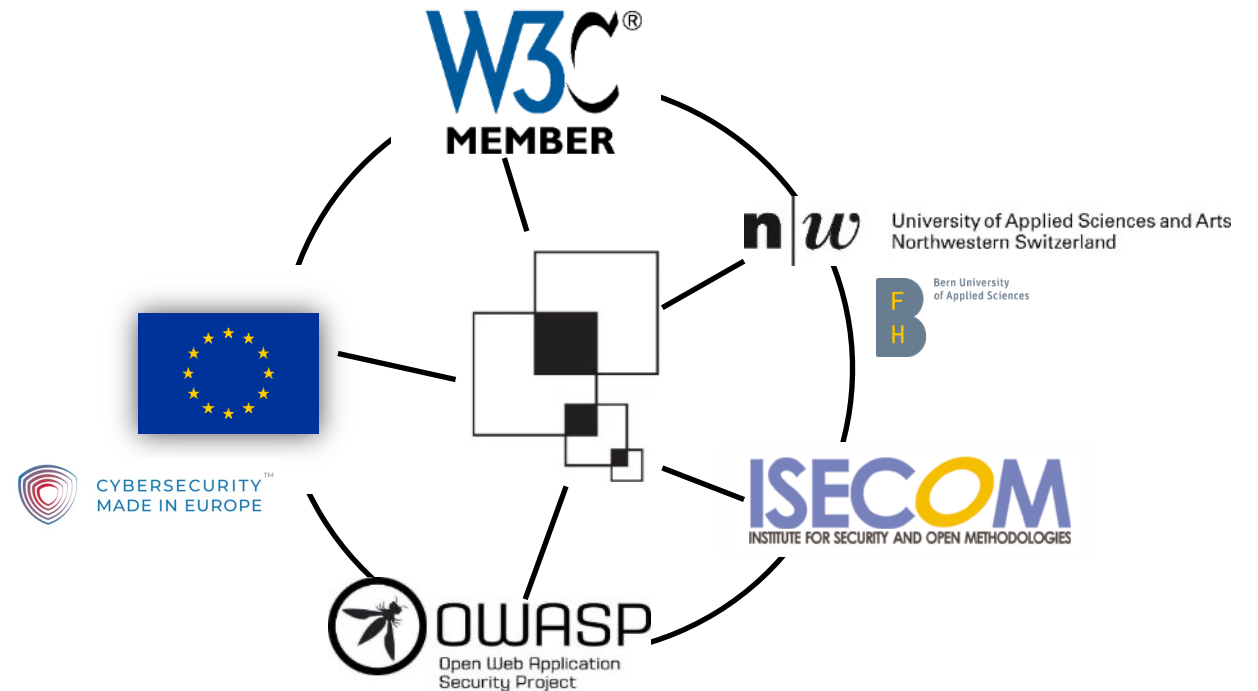
Founder and CEO Dreamlab Technologies,  
Board Member ISECOM and Oneiroi



# Dreamlab Technologies

## Overview

Since 1997	Innovative
3011 Bern	Swiss Made
Cybersecurity	Experienced
Solutions	Professional
Audit	Independent
Consulting	Neutral
Education	Transparent





# Dreamlab Technologies

## Overview

Since 1997

3011 Bern

Cybersecurity

Solutions

Audit

Consulting

Education

Innovative

Swiss Made

Experienced

Professional

Independent

Neutral

Transparent







# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck



# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

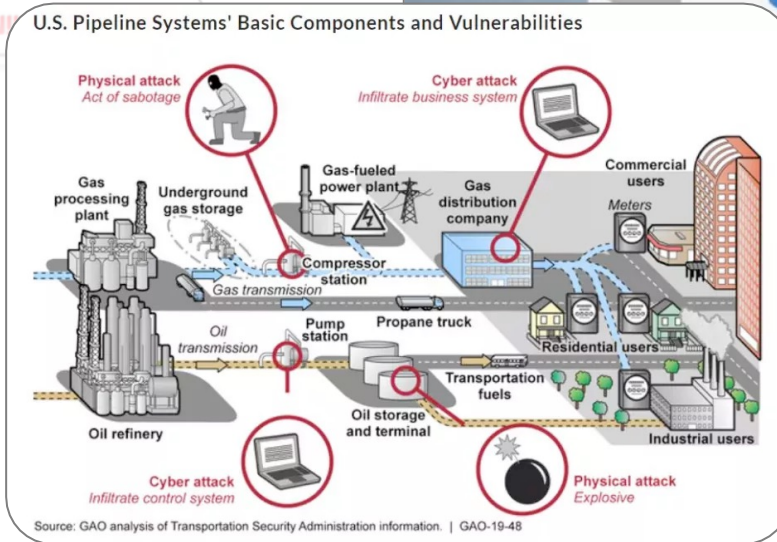
Threat Protection  
Motivation

Conclusion &  
Cybercheck



# Review 2021 (Global)

## Cyberattacks and Leaks which affected Commercial and Individual Spheres

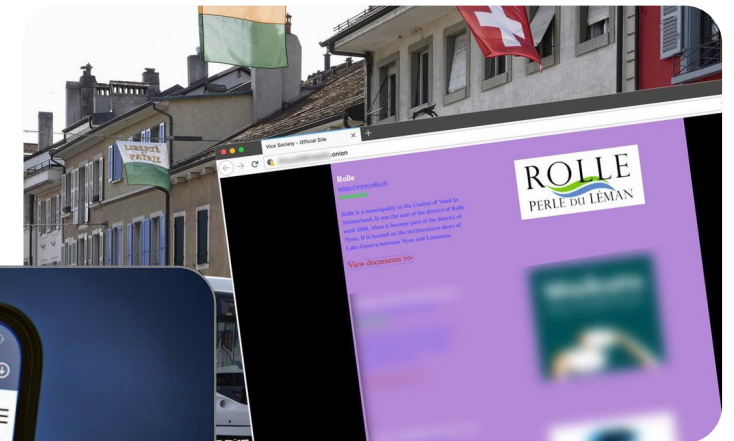
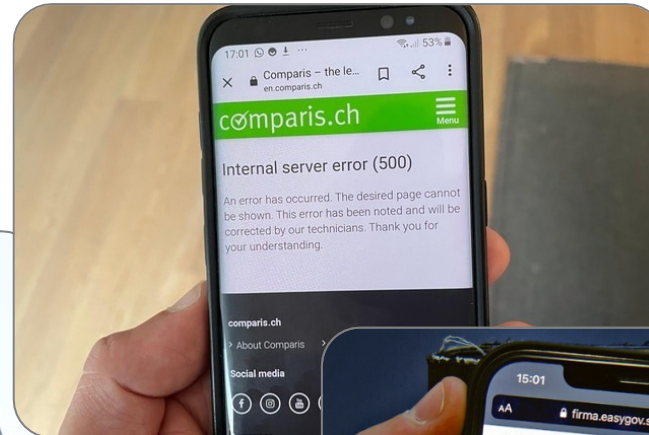






# Review 2021 (Switzerland)

## Cyberattacks and Leaks which affected Commercial and Individual Spheres





# Review 2021 (Switzerland): Physical Burglary vs Cyber Attacks

## Cyberattacks and Leaks which affected Commercial and Individual Spheres





# Country Competitiveness

Country/Economy	Score (0–100)	Rank
Switzerland	66.08	1
Sweden	62.47	2
United States of America	60.56	3
United Kingdom	59.78	4
Netherlands	58.76	5
Denmark	57.53	6
Finland	57.02	7
Singapore	56.61	8
Germany	56.55	9
Republic of Korea	56.11	10
Hong Kong, China	54.24	11
France	53.66	12
Israel	53.55	13
China	53.28	14
Ireland	53.05	15
Japan	52.70	16
Canada	52.26	17
Luxembourg	50.84	18
Austria	50.13	19
Norway	49.29	20
Iceland	49.23	21
Belgium	49.13	22
Australia	48.35	23

## The Global Innovation Index 2020

[https://www.wipo.int/global\\_innovation\\_index/en/2020/](https://www.wipo.int/global_innovation_index/en/2020/)



# Country Competitiveness

Country/Economy	Score (0–100)	Rank
Switzerland	66.08	1
Sweden	62.47	2
United States of America	60.56	3
United Kingdom	59.78	4
Netherlands	58.76	5
Denmark	57.53	6
Finland	57.02	7
Singapore	56.61	8
Germany	56.55	9
Republic of Korea	56.11	10
Hong Kong, China	54.24	11
France	53.66	12
Israel	53.55	13
China	53.28	14
Ireland	53.05	15
Japan	52.70	16
Canada	52.26	17
Luxembourg	50.84	18
Austria	50.13	19
Norway	49.29	20
Iceland	49.23	21
Belgium	49.13	22
Australia	48.35	23

**The Global Innovation Index 2020**

[https://www.wipo.int/global\\_innovation\\_index/en/2020/](https://www.wipo.int/global_innovation_index/en/2020/)

- ✓ Capital / Wealth
- ✓ Innovation
- ✓ Research and Development
- ✓ Precision
- ✓ Quality
- ✓ Independent / Neutral
- ✓ Globally known / recognized



# Country Competitiveness vs. Cybersecurity Commitment

Country/Economy	Score (0–100)	Rank
Switzerland	66.08	1
Sweden	62.47	2
United States of America	60.56	3
United Kingdom	59.78	4
Netherlands	58.76	5
Denmark	57.53	6
Finland	57.02	7
Singapore	56.61	8
Germany	56.55	9
Republic of Korea	56.11	10
Hong Kong, China	54.24	11
France	53.66	12
Israel	53.55	13
China	53.28	14
Ireland	53.05	15
Japan	52.70	16
Canada	52.26	17
Luxembourg	50.84	18
Austria	50.13	19
Norway	49.29	20
Iceland	49.23	21
Belgium	49.13	22
Australia	48.35	23

**The Global Innovation Index 2020**

[https://www.wipo.int/global\\_innovation\\_index/en/2020/](https://www.wipo.int/global_innovation_index/en/2020/)



Country Name	Score	Rank	Country Name	Score	Rank
United States of America**	100	1	Indonesia	94.88	24
United Kingdom	99.54	2	Viet Nam	94.59	25
Saudi Arabia	99.54	2	Sweden	94.55	26
Estonia	99.48	3	Qatar	94.5	27
Korea (Rep. of)	98.52	4	Greece	93.98	28
Singapore	98.52	4	Austria	93.89	29
Spain	98.52	4	Poland	93.86	30
Russian Federation	98.06	5	Kazakhstan	93.15	31
United Arab Emirates	98.06	5	Denmark	92.6	32
Malaysia	98.06	5	China	92.53	33
Lithuania	97.93	6	Croatia	92.53	33
Japan	97.82	7	Slovakia	92.36	34
Canada**	97.67	8	Hungary	91.28	35
France	97.6	9	Israel**	90.93	36
India	97.5	10	Tanzania	90.58	37
Turkey	97.49	11	North Macedonia	89.92	38
Australia	97.47	12	Serbia	89.8	39
Luxembourg	97.41	13	Azerbaijan	89.31	40
Germany	97.41	13	Cyprus	88.82	41
Portugal	97.32	14	Switzerland**	86.97	42
			Ghana	86.69	43

**Global Cybersecurity Index 2020**

<https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020>



# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck



# Dimensions

**LAND**



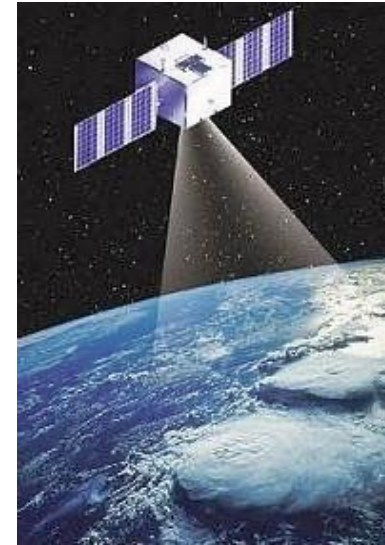
**SEA**



**AIR**



**SPACE**





# Dimensions

**LAND**



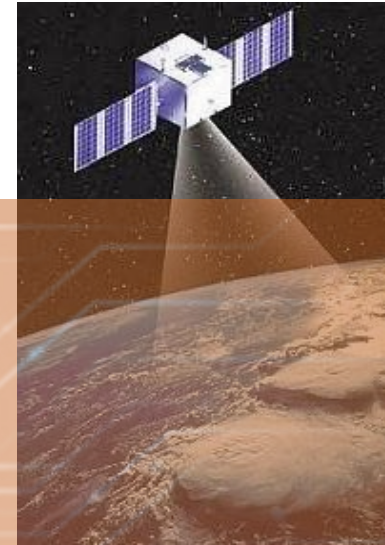
**SEA**



**AIR**



**SPACE**



**CYBER**



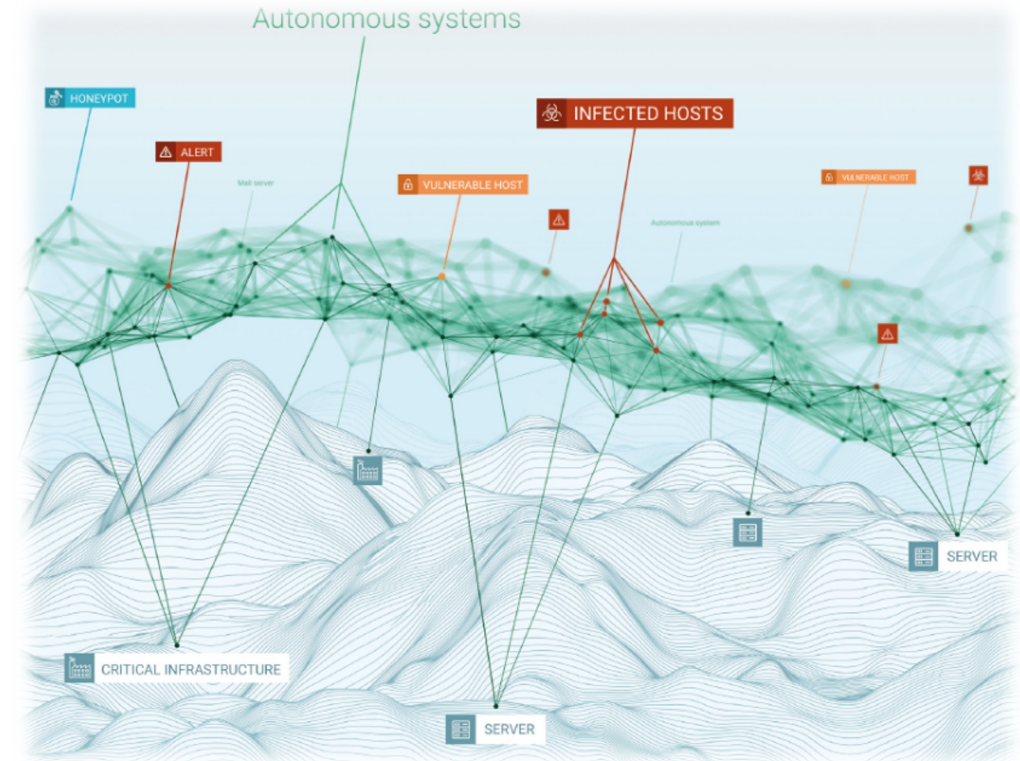


# CyObs

## Introduction

To defend a country, you will need to know its borders:

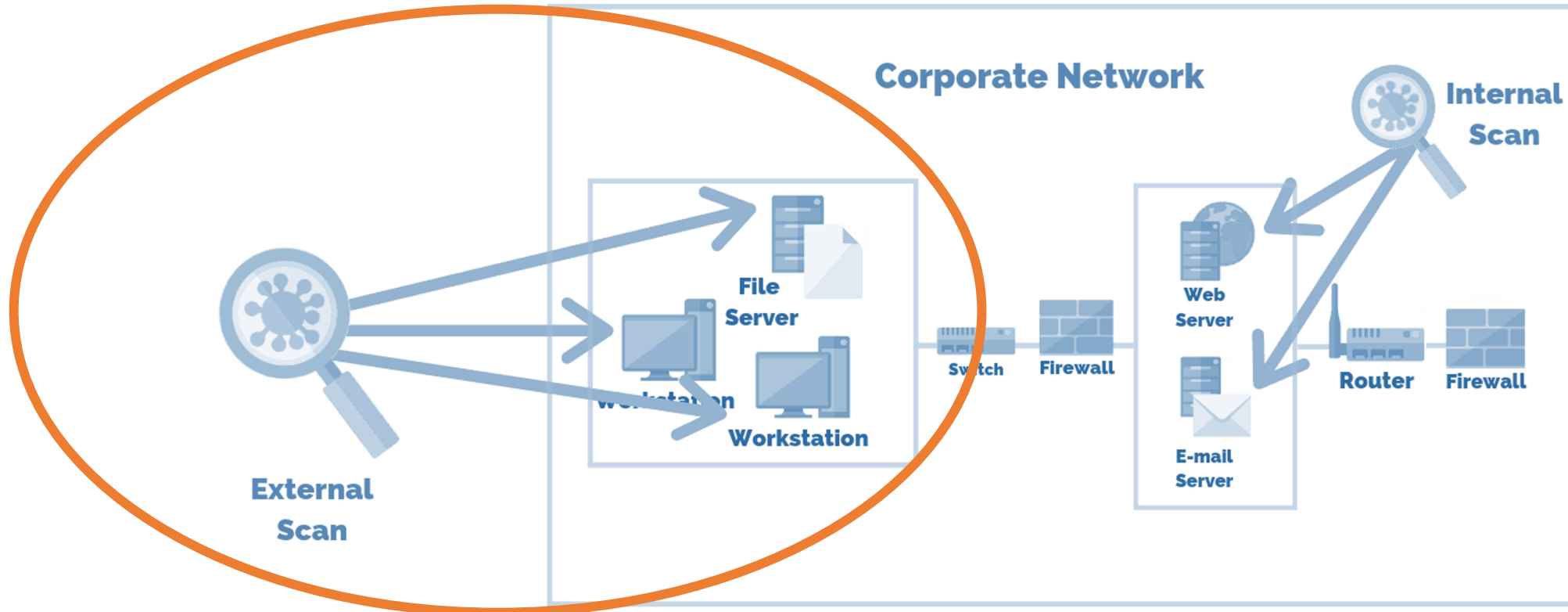
- Land
  - Air
  - Water
  - and **Cyberspace**
- 
- CyObs is the Cyberspace Radar System to map, analyse and visualise the cyberspace of a whole country or a large, global organisation.
  - It identifies all cyber vulnerabilities and the potential attack surface of a country/organisation.
  - CyObs is a starting point for a (national) cyber defence strategy.





# CyObs

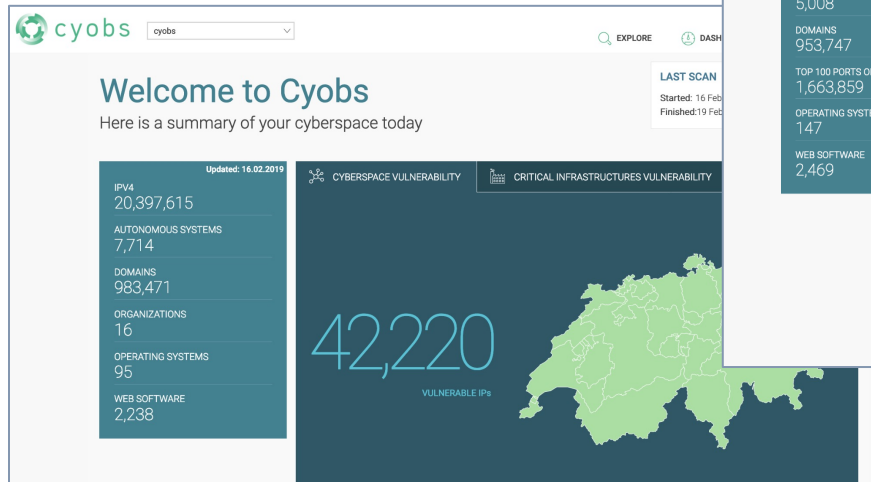
## Introduction



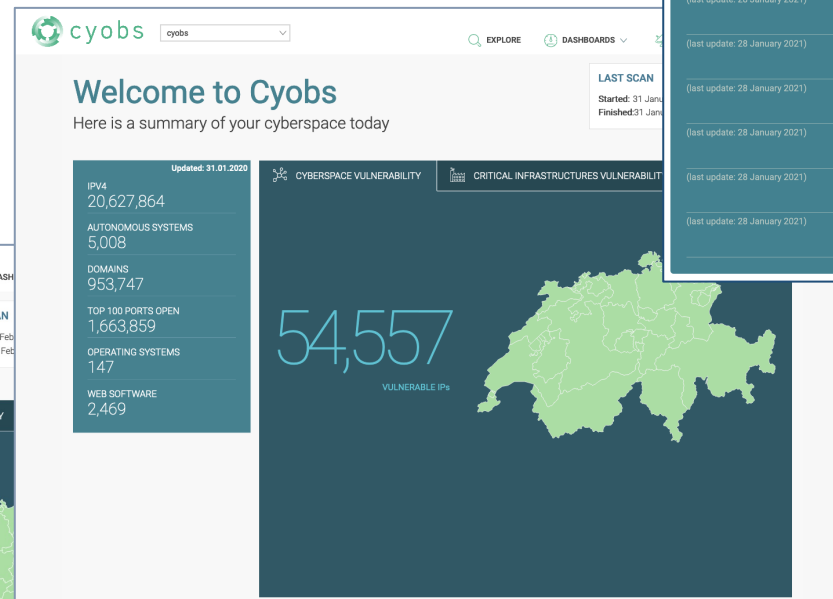


# The Swiss Cyberspace 2019 to 2021

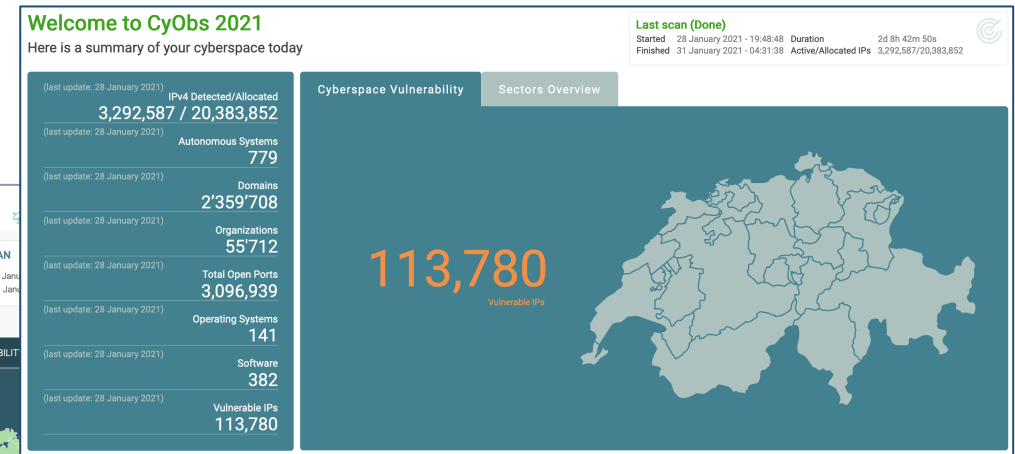
## 2019



## 2020



## 2021

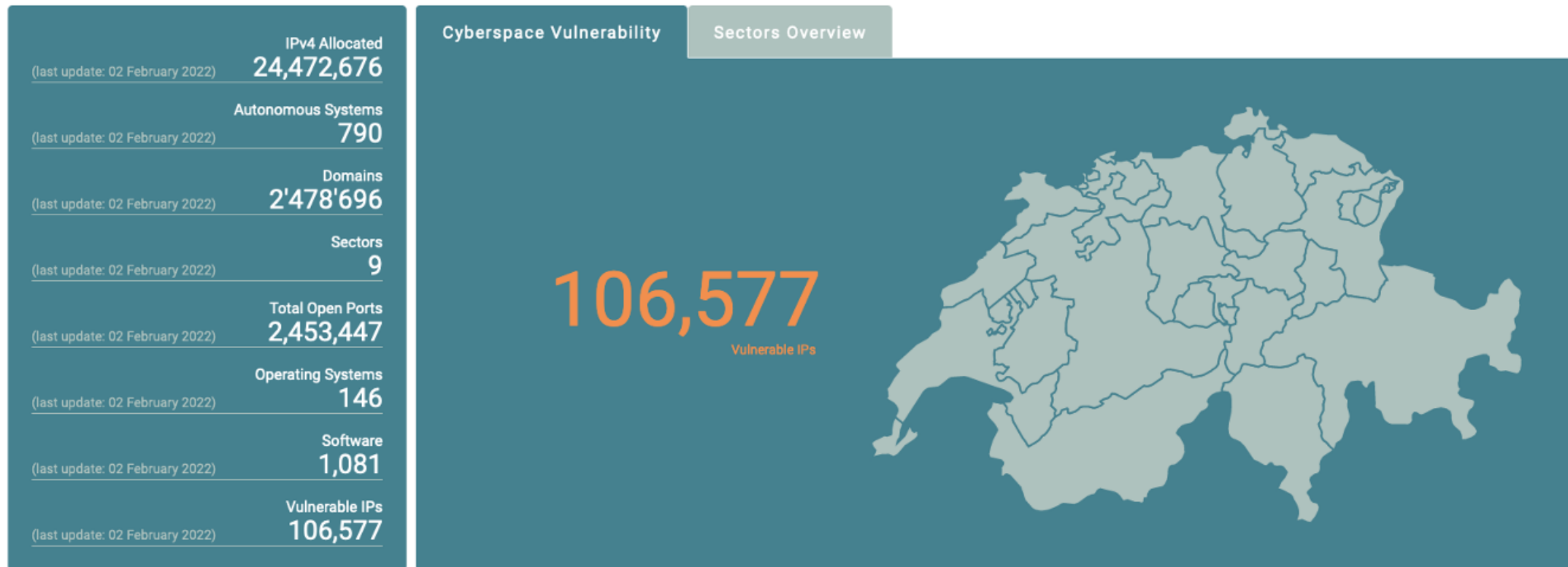




# The Swiss Cyberspace 2022

## Welcome to CyObs

Here is a summary of your cyberspace today





# The Swiss Cyberspace 2022

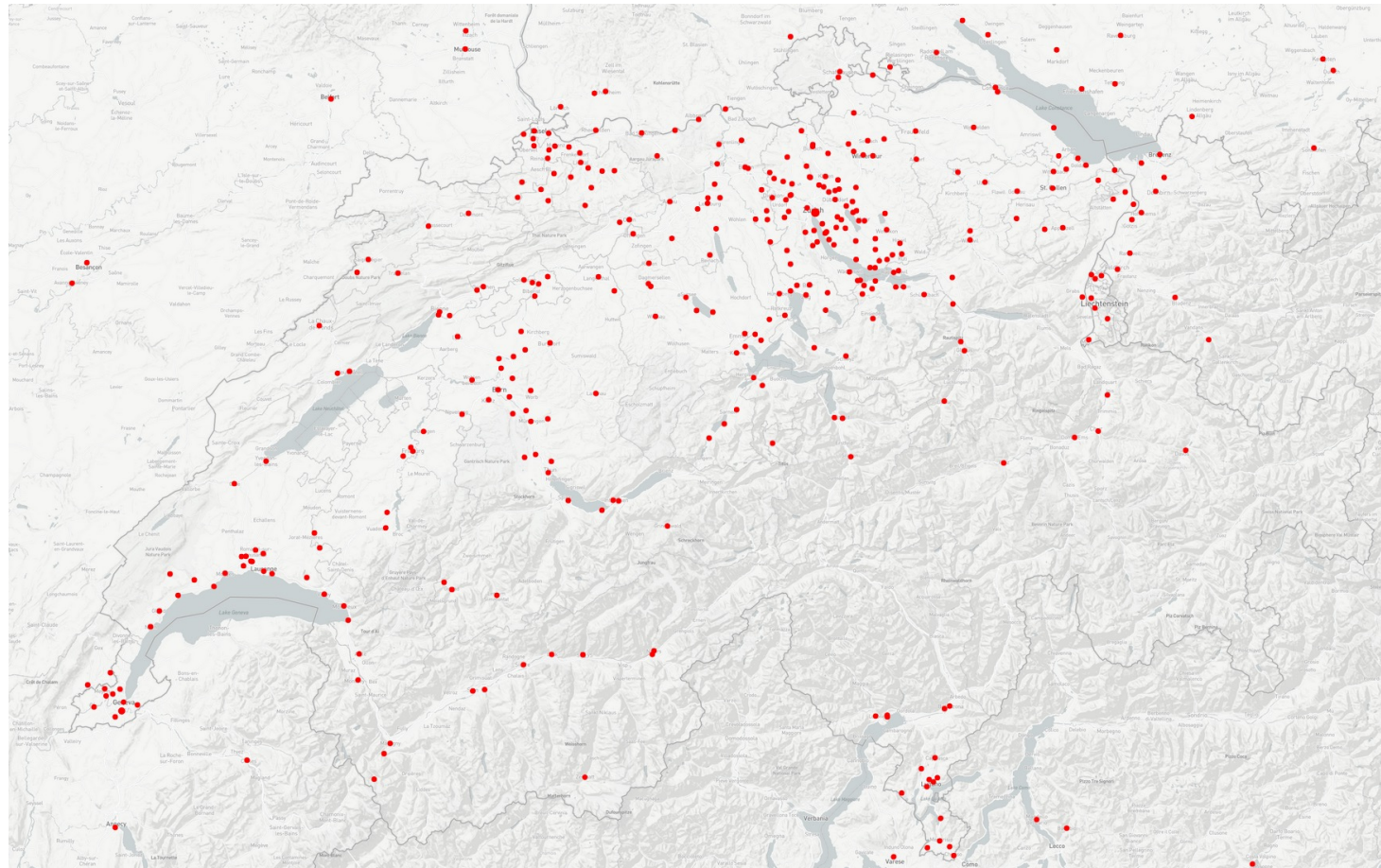
## Overview

Parameter	Results	Description
<b>IPv4 allocated</b>	<b>24,472,676</b>	CH IP range
<b>IPv4 detected/active</b>	<b>2,982,022</b>	ICMP response + port scan activity
<b>Domains</b>	<b>2,478,696</b>	#domains analysed
<b>Domains using DNSSEC</b>	<b>850,884</b>	#domains using DNSSEC
<b>Autonomous Systems</b>	<b>790</b>	Total active AS in CH
<b>Total Open Ports</b>	<b>2'453'447</b>	Cumulative number of open ports
<b>Operating Systems</b>	<b>146</b>	Distinct Operating Systems
<b>Unique Software</b>	<b>1081</b>	Distinct Software
<b>Vulnerable IPs</b>	<b>106,577</b>	Potentially vulnerable IPs

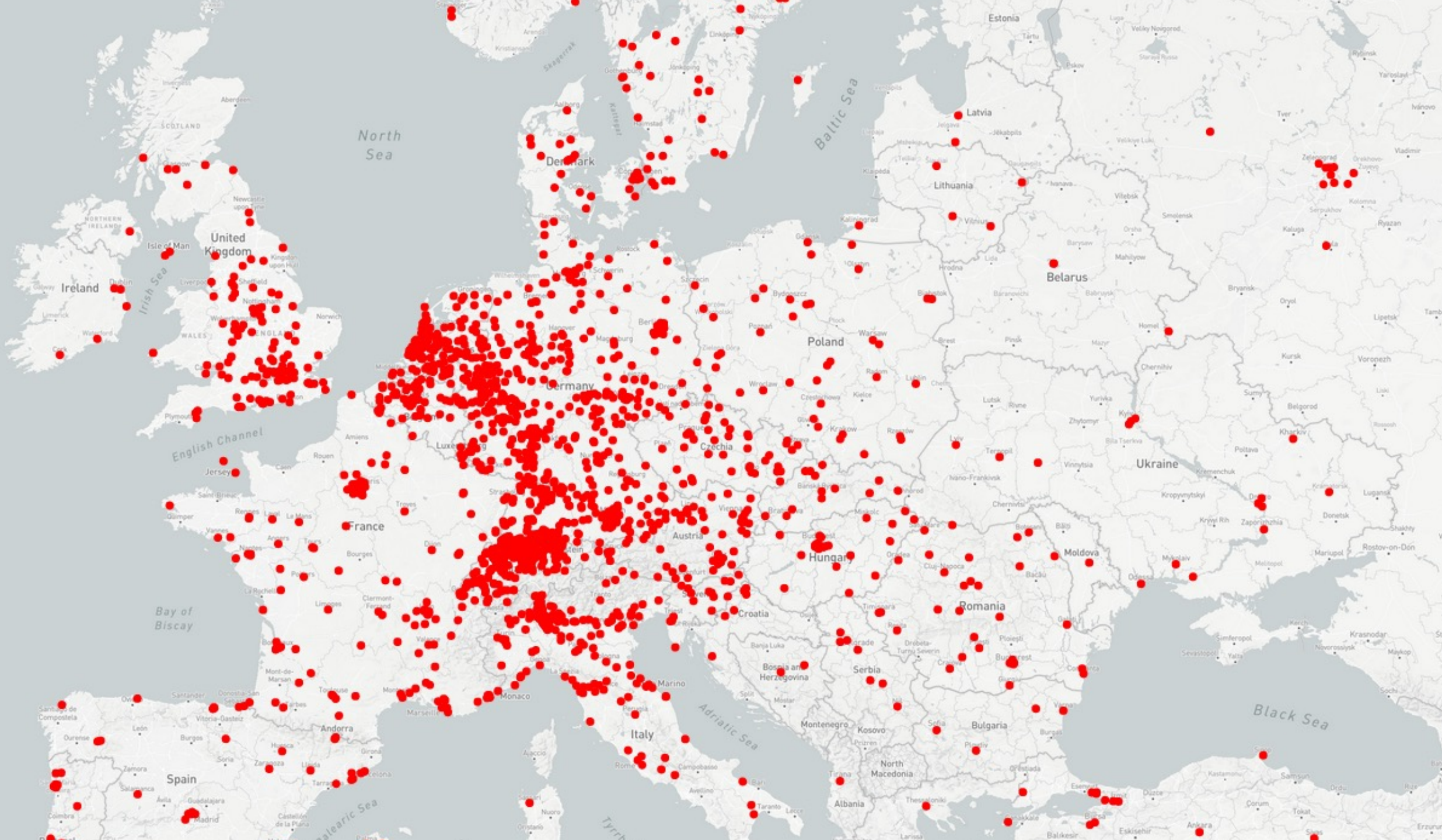


# The Swiss Cyberspace 2022

## .ch DNS Server Distribution



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022



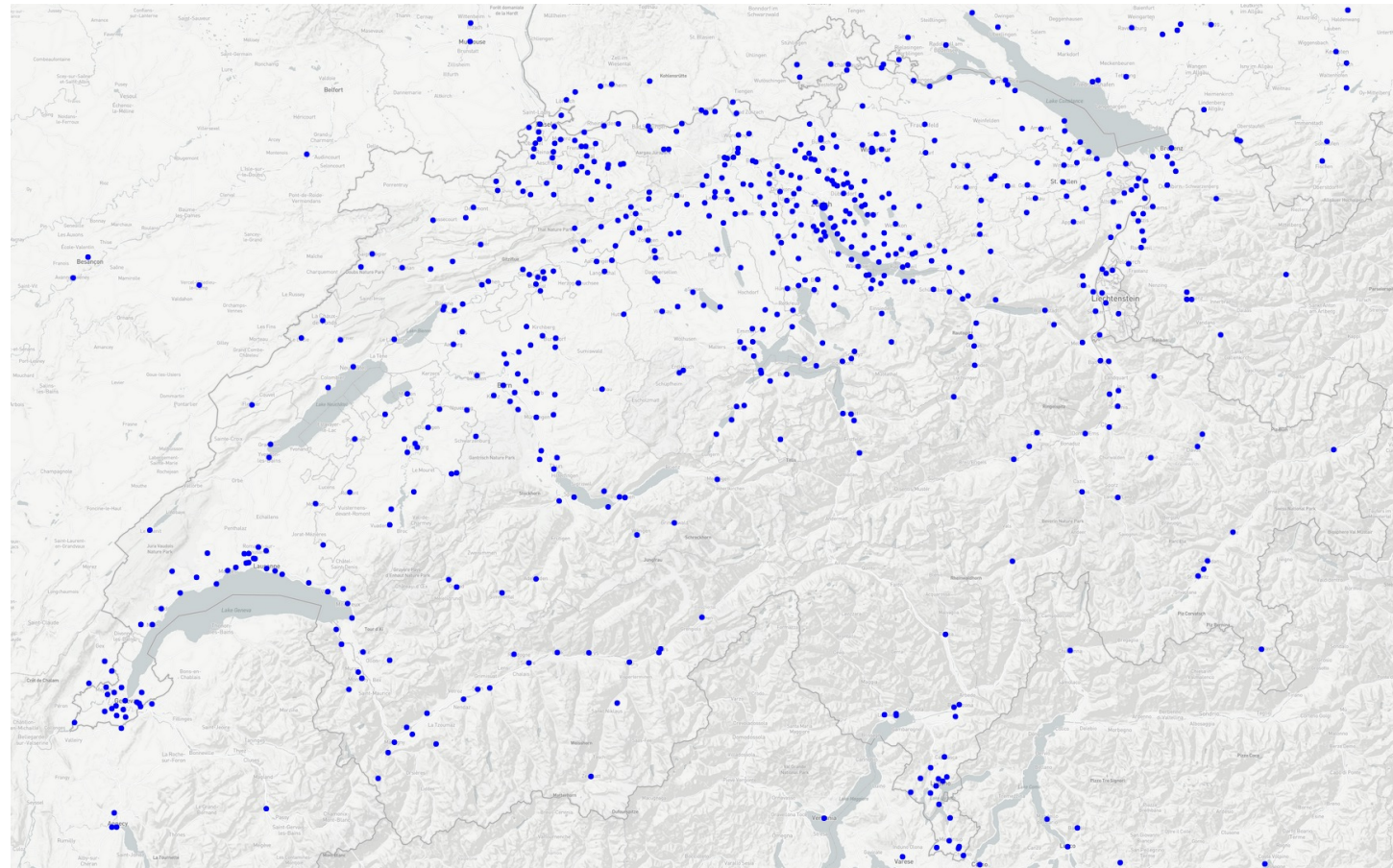




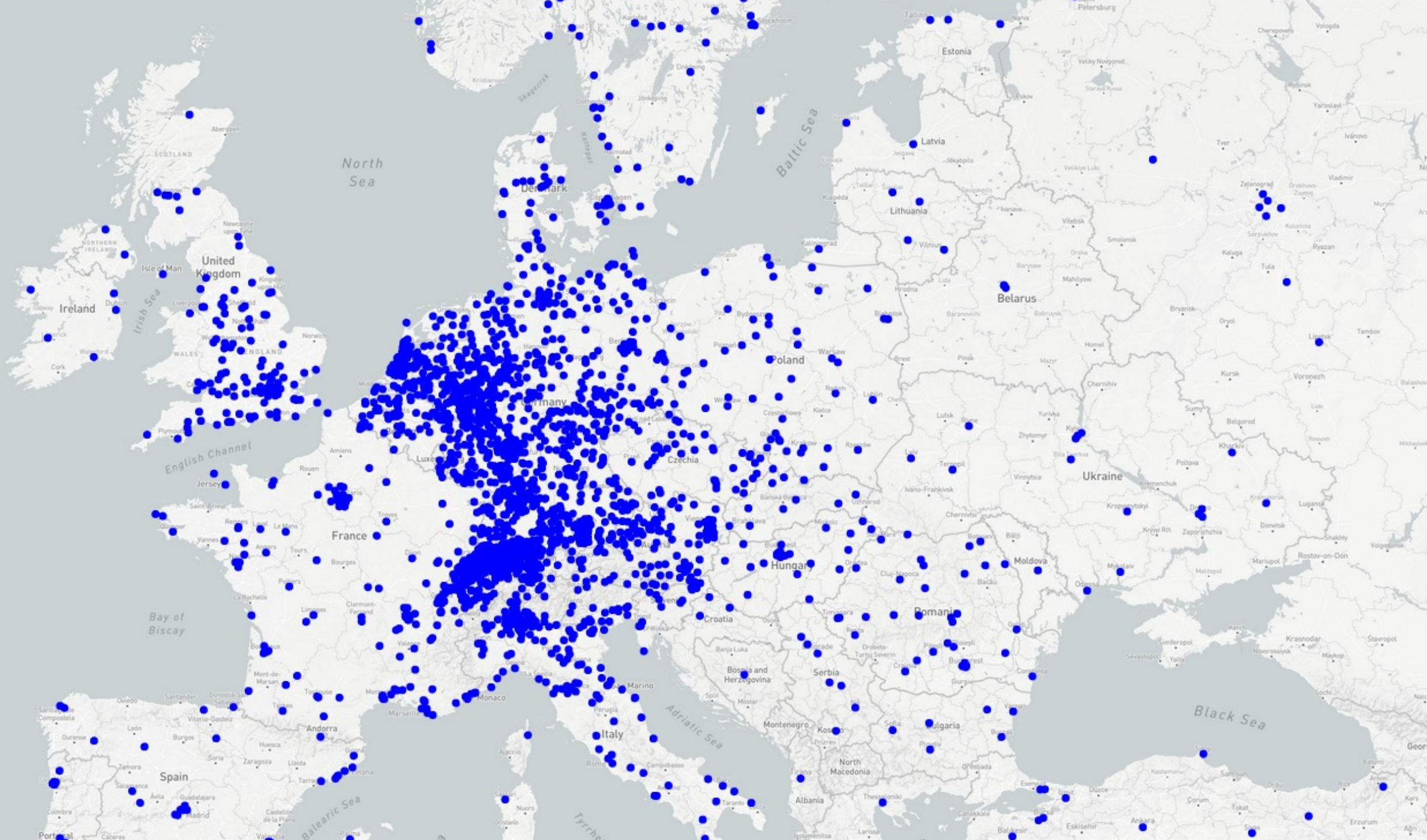


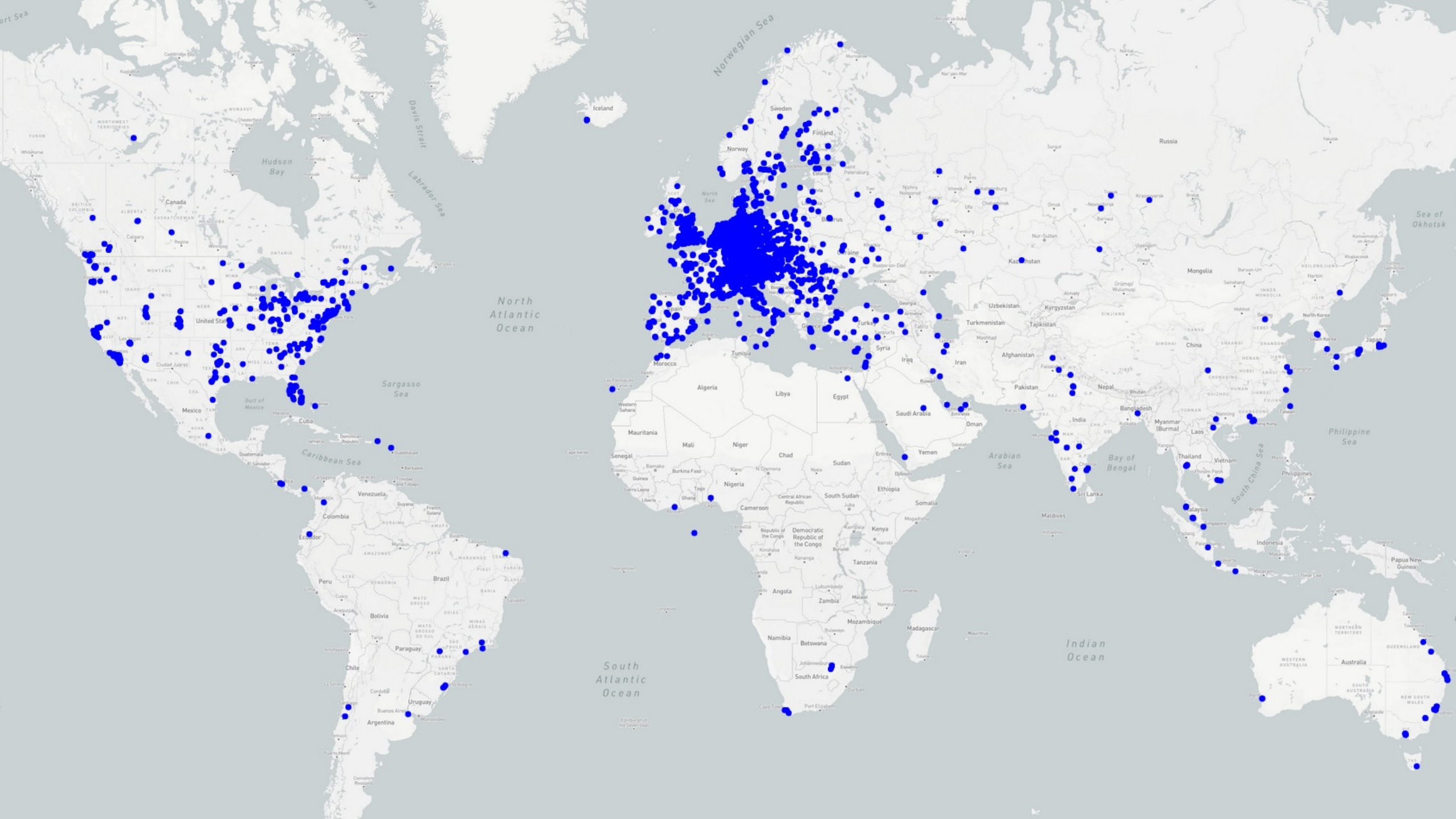
# The Swiss Cyberspace 2022

## .ch Mail Server Distribution



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

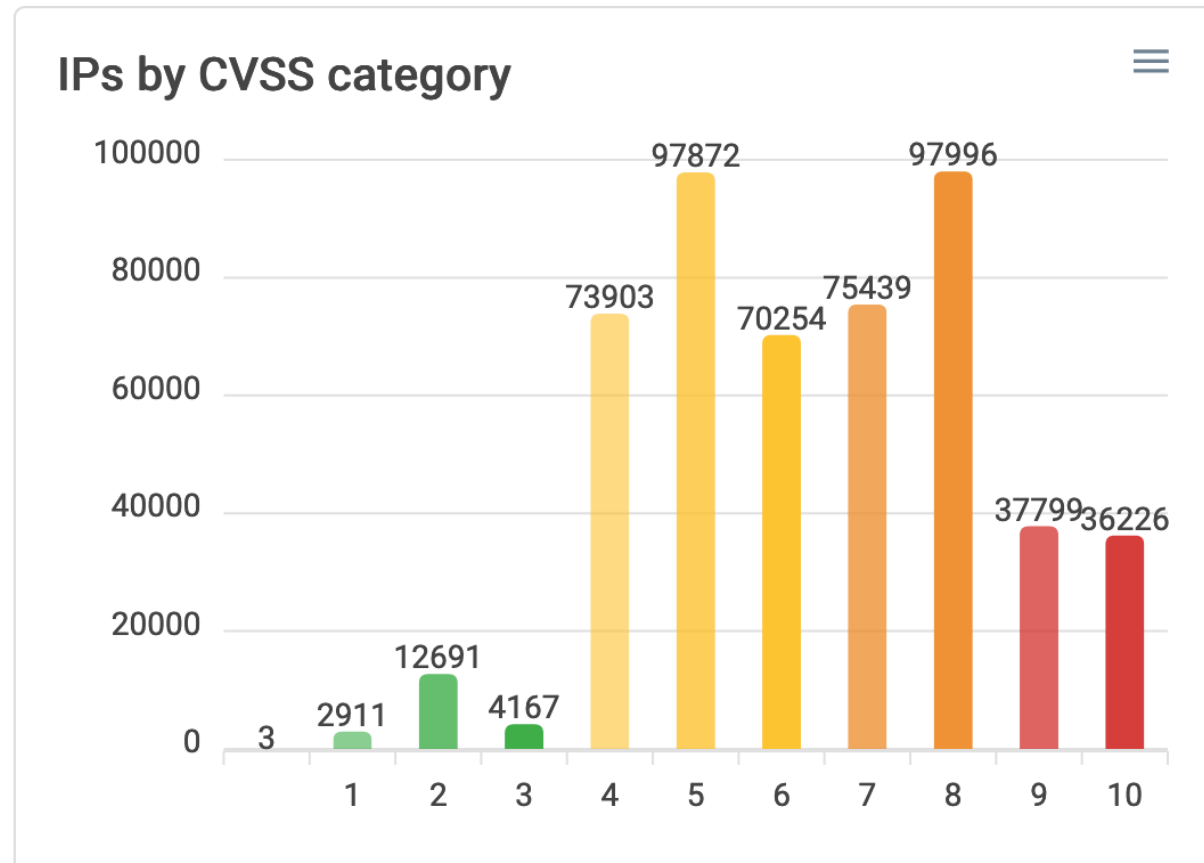






# The Swiss Cyberspace 2022

## Vulnerabilities Overview



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022



# The Swiss Cyberspace 2022

## Bluekeep

**Filters** Save filter

Enter field

Select condition

Enter value

+ Add filter

custom\_plugin.cve equals CVE-2019-0708 🗑️

98 results

⏪ page 1 of 10 ⏩

Results per page 10

**Explore**

📅 02 February 2022 - 📅 02 March 2022 Today

**Highest CVSS Score: 9.8**

**5.145.** Details >

AS: 15600 (QUICKLINE Quickline AG, CH)

Self Signed Certificate Total vuln: 1

**Open ports: 2**

- 443/tcp: ZyXEL ZyWALL http config
- 3389/tcp: Unknown

**Highest CVSS Score: 9.8**

**46.14** Details >

AS: 3303 (SWISSCOM Swisscom Switzerland Ltd, CH)

OS: Linux 2.6.32 (accuracy: 98) Total vuln: 2

**Open ports: 9**

- 21/tcp: Unknown
- 25/tcp: postfix
- 80/tcp: nginx
- 443/tcp: nginx
- 587/tcp: postfix
- 993/tcp: dovecot
- 1723/tcp: Unknown
- 3306/tcp: mysql 5.5.68-mariadb
- 3389/tcp: Unknown

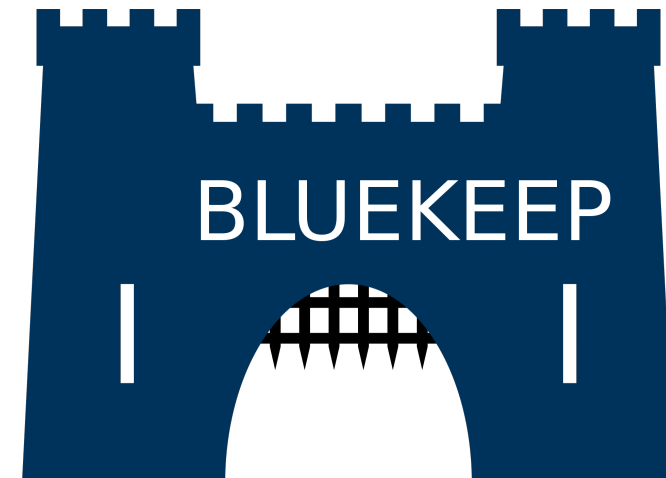
**Highest CVSS Score: 9.8**

**46.14** Details >

AS: 3303 (SWISSCOM Swisscom Switzerland Ltd, CH)

**Open ports: 1**

- 3389/tcp: Unknown



98 hits for Bluekeep (CVE-2019-0708)



# The Swiss Cyberspace 2022

## Log4Shell – Log4j Vulnerability

- CVE-2021-4428
- High-severity (**CVSS 10**) vulnerability
- Affects the core function of [Apache Log4j2](#)
- Discovered in December 2021



**57 IPs vulnerable**  
(as of 21.12.2021)

**11 IPs vulnerable**  
(as of Feb 2022)

Swiss Universities and Government sites amongst affected IPs.





# The Swiss Cyberspace 2022

## More Vulnerabilities requiring Attention



- XML External Entity injection (XXE) vulnerability
- CVE-2019-9670
- CVSS Score **7.5**
- Modification of system files possible
- **15** IPs affected



- Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-34473
- CVSS Score **9.1**
- **Remote Code Execution**
- **84** IPs affected



- Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-26855
- CVSS Score **9.1**
- Part of an attack chain - **Remote Code Execution**
- **73** IPs affected



# The Swiss Cyberspace 2022

## More Vulnerabilities requiring Attention



- Vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA)
- CVE-2020-3452
- CVSS Score **7.5**
- Directory traversal attacks and read sensitive files on a targeted system
- **536** IPs affected



- Webmin Cross-Site Scripting RCE Vulnerability
- CVE-2021-31761
- CVSS Score **9.6 critical**
- **Remote Code Execution**
- **22** IPs affected





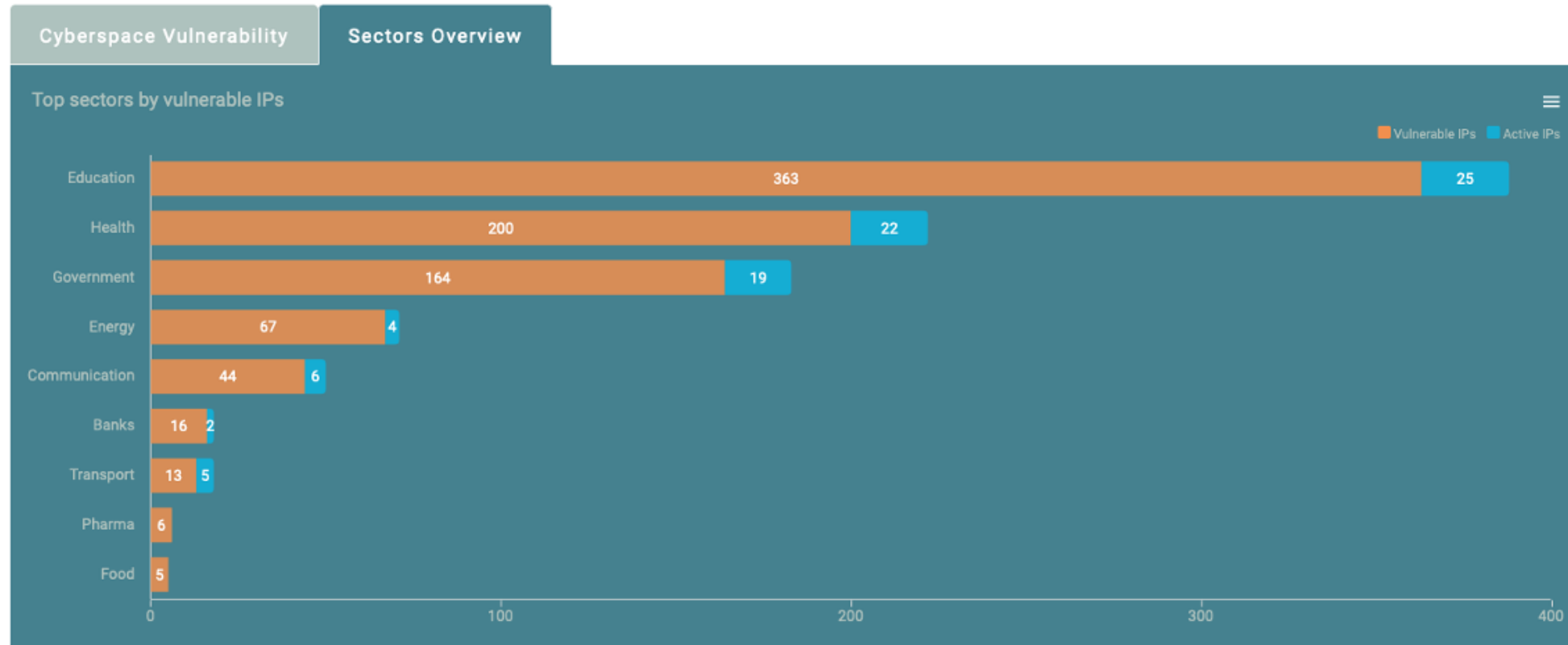
# The Swiss Cyberspace 2022

## Industry/Sector View

### Welcome to CyObs

Here is a summary of your cyberspace today

(last update: 02 February 2022)	IPv4 Allocated <b>24,472,676</b>
(last update: 02 February 2022)	Autonomous Systems <b>790</b>
(last update: 02 February 2022)	Domains <b>2,478,696</b>
(last update: 02 February 2022)	Organizations <b>9</b>
(last update: 02 February 2022)	Total Open Ports <b>2,453,447</b>
(last update: 02 February 2022)	Operating Systems <b>146</b>
(last update: 02 February 2022)	Software <b>1,081</b>
(last update: 02 February 2022)	Vulnerable IPs <b>106,577</b>

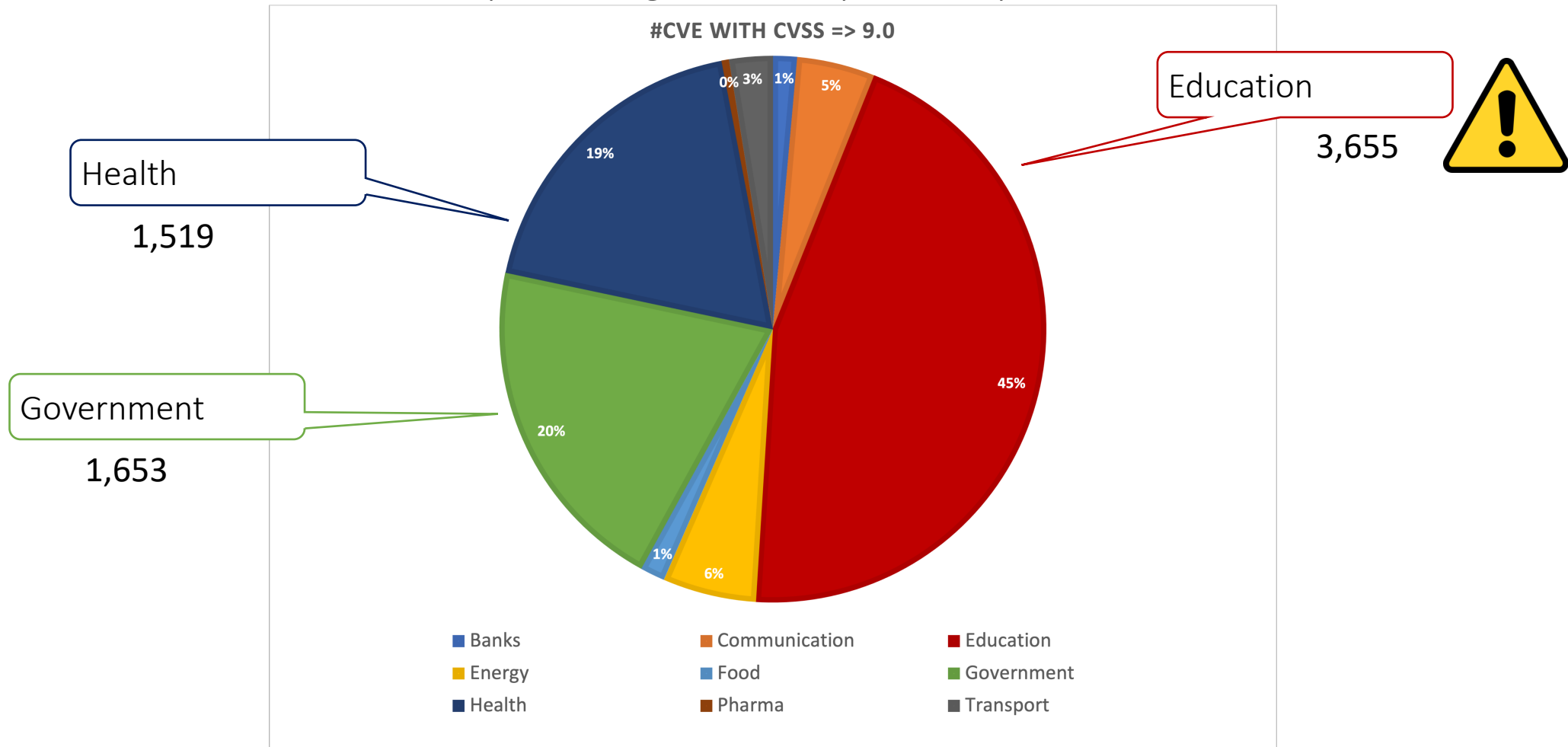


Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022



# The Swiss Cyberspace 2022

## Critical Vulnerabilities (CVSS equal or higher 9.0) by Industry/Sector



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022



# The Swiss Cyberspace 2022

## Vulnerabilities by Industry/Sector – Overview



**Gov** admin.ch  
Cantons  
Municipalities

2,155 domains

9,979



**Energy**  
EVU  
Providers

337 domains

3,324



**Hospitals**  
& Health

288 domains

9,726



**Public Transport**  
Local and SBB

47 domains

1,047



**Banks and Finance**

154 domains

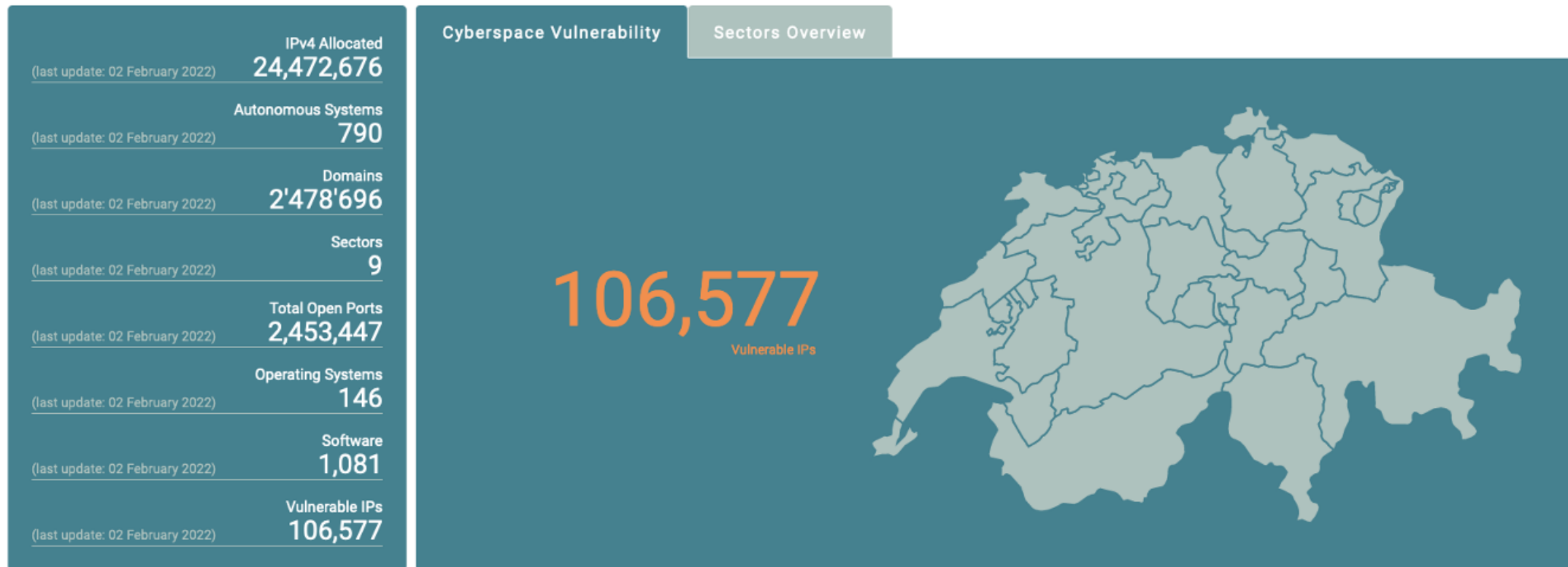
868



# The Swiss Cyberspace 2022

## Welcome to CyObs

Here is a summary of your cyberspace today





# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

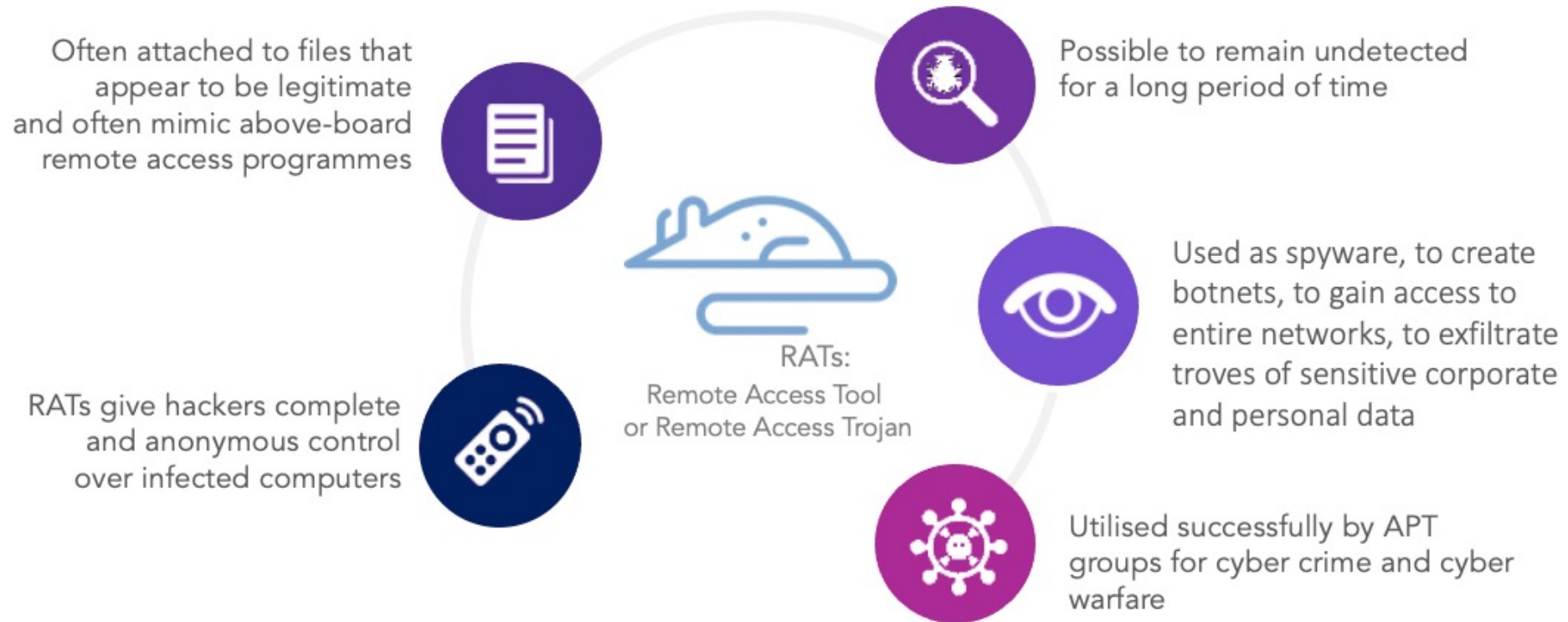
Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck



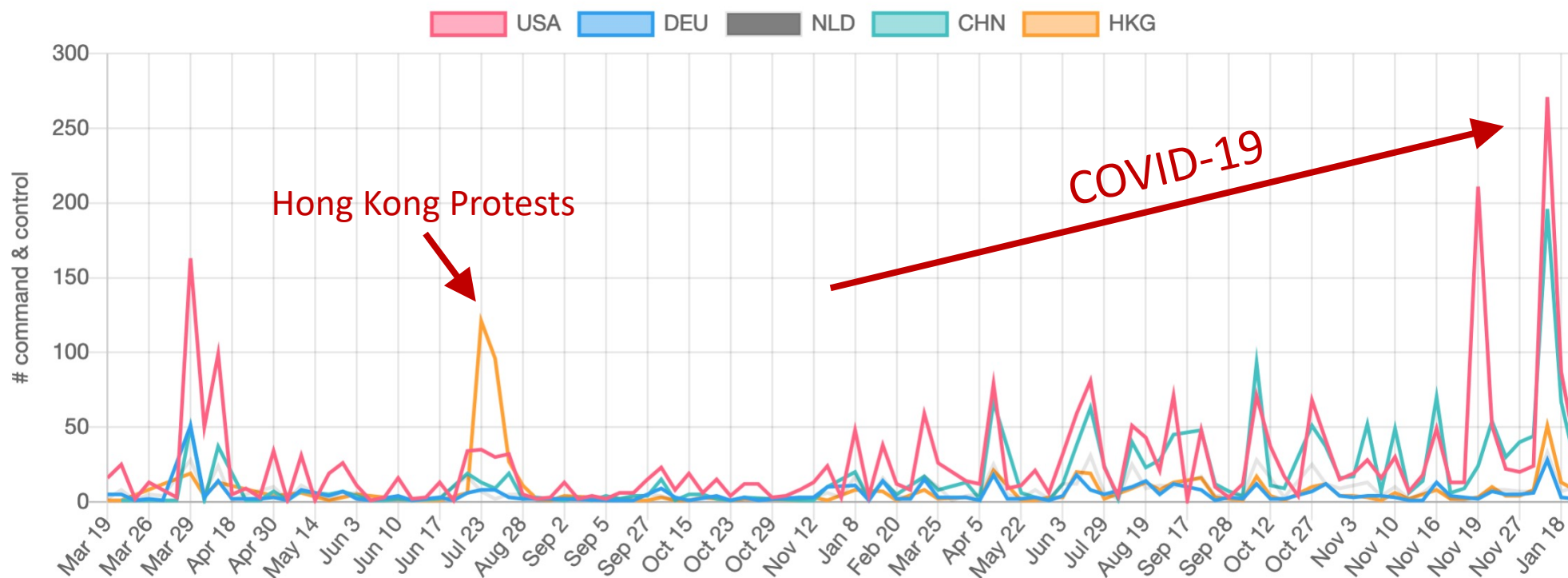
# RATspotting – Comand and Control (C2) Systems





# C2 Server Timeline by Country – Feb 2019 to Jan 2021

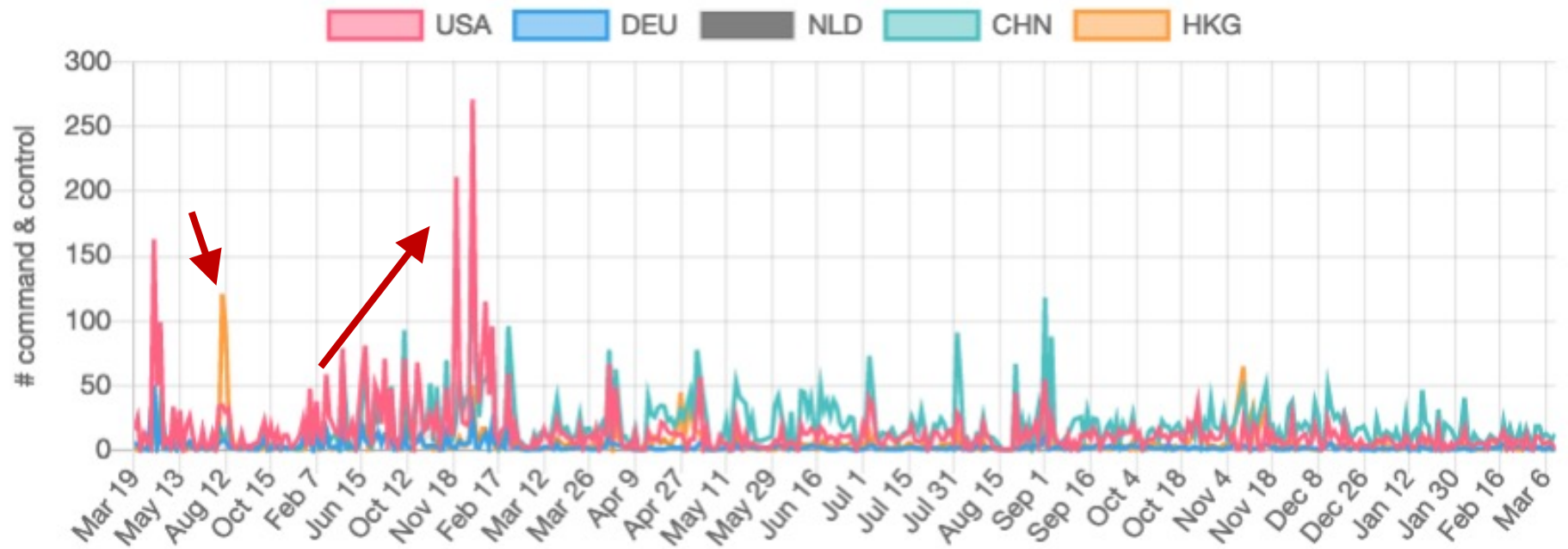
GRAPH **COUNTRY**





# C2 Server Timeline by Country – Feb 2019 to Mar 2022

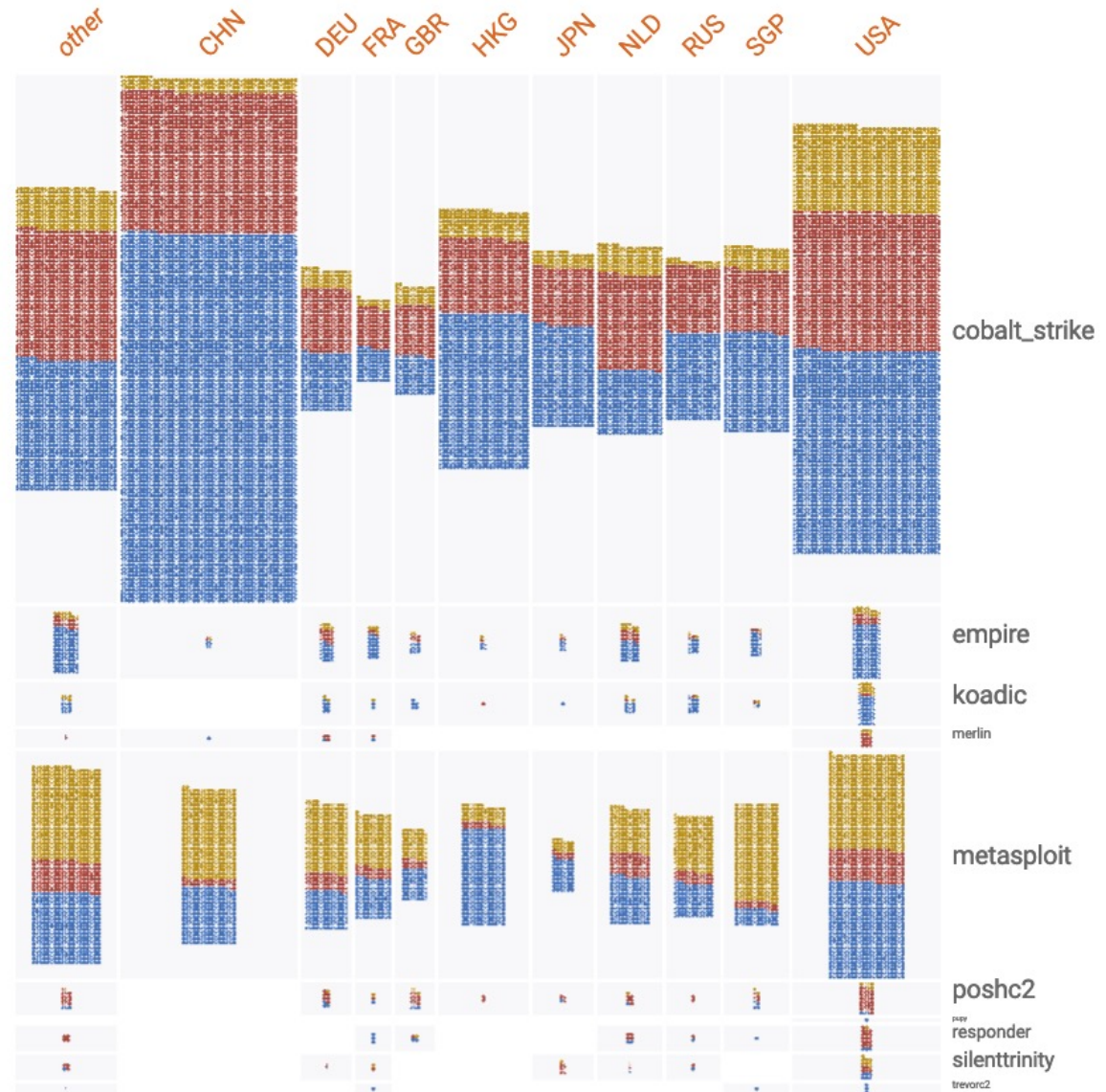
GRAPH **COUNTRY**







# C2 Servers by Country / Malware Type View





# C2 Servers in Switzerland

98 in 03.2022 (vs. 36 in 02.2021)

C2 SERVERS

Copy Excel CSV PDF

Search:

IP	PORT	TYPE	PAYLOAD	COUNTRY	FLAG	CERTIFICATE	FIRST DETECTION	LAST DETECTION	JARM	OTX PULSES
[REDACTED]	443	cobalt_strike		Switzerland	+	None	2022-03-02 06:06	2022-03-07 06:06	[REDACTED]	2
[REDACTED]	3790	metasploit	metasploit/webui	Switzerland	+	localhost	2022-02-16 06:04	2022-03-07 06:07	[REDACTED]	0
[REDACTED]	80	cobalt_strike		Switzerland	+	None	2022-02-14 06:04	2022-02-14 06:04	[REDACTED]	2
[REDACTED]	443	metasploit	multi/meterpreter/reverse_http	Switzerland	+	[REDACTED]	2022-02-13 06:05	2022-02-13 06:05	[REDACTED]	0
[REDACTED]	80	cobalt_strike		Switzerland	+		2022-02-13 06:05	2022-03-07 06:07	[REDACTED]	0
[REDACTED]	443	cobalt_strike		Switzerland	+	None	2022-02-11 06:04	2022-02-11 06:04	[REDACTED]	2
[REDACTED]	3790	metasploit	metasploit/webui	Switzerland	+	localhost	2022-02-06 06:04	2022-02-07 06:04	[REDACTED]	0
[REDACTED]	3790	metasploit	metasploit/webui	Switzerland	+	localhost	2022-02-06 06:04	2022-02-07 06:04	[REDACTED]	0
[REDACTED]	3790	metasploit	metasploit/webui	Switzerland	+	localhost	2022-02-01 06:04	2022-02-07 06:04	[REDACTED]	0
[REDACTED]	80	cobalt_strike		Switzerland	+		2021-12-31 06:11	2022-01-07 06:04	[REDACTED]	2

Showing 1 to 10 of 98 entries (filtered from 26,779 total entries)

IP Port Type Payload  Flag Certificate First Detection Last Detection JARM OTX Pulses

Previous 1 2 3 4 5 ... 10 Next

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022



# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck



# Switzerland and Crypto

**Business**

## Swiss City of Lugano to Make Bitcoin and Tether 'De Facto' Legal Tender

The municipality wants businesses to accept crypto in everyday transactions.

By Stephen Alpher · Mar 3, 2022 at 2:43 p.m. · Updated Mar 3, 2022 at 3:21 p.m.

COMMENTS | May 4, 2021

## Switzerland is a global leader in blockchain adoption

By GlobalData Financial

NEWS

## BBVA Switzerland adds Ethereum to crypto custody

Monday 13 December 2021 15:08 CET | News

[BBVA Switzerland](#), the Swiss division of the Spain-based multinational financial services provider BBVA, has announced the addition of Ethereum (ETH) to its crypto custody and trading service.

[in](#) [twitter](#) [email](#) [facebook](#)



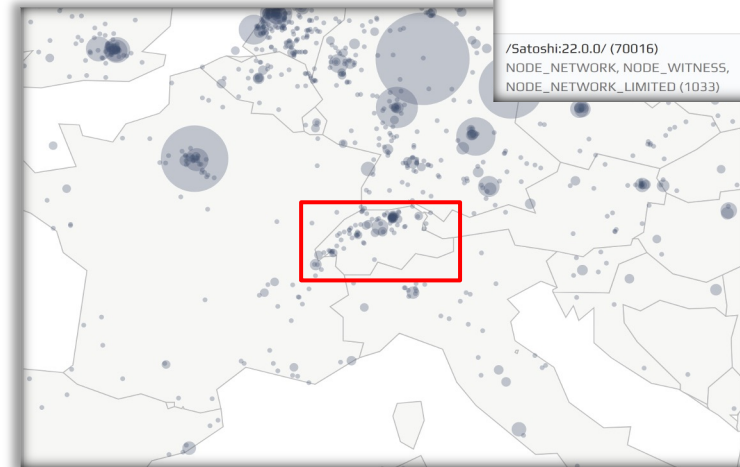
# Swiss Crypto: Bitcoin and Ethereum Overview

Switzerland has **122 Bitcoin nodes**, ranking 11th globally.

- Zurich: 51 nodes
- Geneva: 13 nodes
- Lausanne: 9 nodes

Switzerland has **71 Ethereum nodes**, ranking 15th globally.

- Zurich: 33 nodes
- Basel: 4 nodes
- Lausanne: 3 nodes



Page 1 of 3 (122 nodes/0.80%) NEXT / LAST

USER AGENT	HEIGHT	LOCATION	NETWORK
/Satoshi:0.20.1/ (70015) NODE_NETWORK, NODE_WITNESS, NODE_NETWORK_LIMITED (1033)	725772	Bern, Switzerland Europe/Zurich	Bluewin AS3303
/Satoshi:22.0.0/ (70016) NODE_NETWORK, NODE_BLOOM, NODE_WITNESS, NODE_NETWORK_LIMITED (1037)	725772	Zurich, Switzerland Europe/Zurich	Salt Mobile SA AS15796
/Satoshi:0.20.0/ (70015) NODE_NETWORK, NODE_WITNESS, NODE_NETWORK_LIMITED (1033)	725772	Binningen, Switzerland Europe/Zurich	Sunrise UPC GmbH AS6730
/Satoshi:22.0.0/ (70016) NODE_WITNESS, NODE_NETWORK_LIMITED (1032)	725772	Kilchberg, Switzerland Europe/Zurich	Init7 (Switzerland) Ltd. AS13030
/Satoshi:22.0.0/ (70016) NODE_WITNESS, NODE_NETWORK_LIMITED (1032)	725772	Glattbrugg, Switzerland Europe/Zurich	Init7 (Switzerland) Ltd. AS13030
/Satoshi:22.0.0/ (70016) NODE_NETWORK, NODE_WITNESS, NODE_NETWORK_LIMITED (1033)	725772	Thielle-Wavre, Switzerland Europe/Zurich	Liberty Global B.V. AS6830



# Ethereum Vulnerabilities

Of the 71 Ethereum nodes detected in Switzerland, **24 (33%) have the JSON-RPC interface open on port 8545**. Using the `web3_clientVersion` method, an attacker can obtain the node client, version, platform and compiler:

```
yl@ws17:~$ [redacted] {"jsonrpc":"2.0","method":  
"web3_clientVersion","params":[],"id":67}' http://[redacted]:8545  
{"jsonrpc":"2.0","id":67,"result":"Geth/v1.10.11-stable-7231b3ef/linux-amd64/go1.17.2"}
```

Using the `eth_accounts` method, an attacker can obtain the node accounts addresses:

```
yl@ws17:~$ [redacted] {"jsonrpc":"2.0","method":  
"eth_accounts","params":[],"id":1}' http://[redacted]:8545  
{"jsonrpc":"2.0","id":1,"result":["0xbc82[redacted]"]}
```

Using the `eth_getBalance` method, an attacker can obtain the balance of the node's accounts:

```
yl@ws17:~$ [redacted] {"jsonrpc":"2.0","method":  
"eth_getBalance","params":["0xa51c[redacted]", "latest"],"id":1}' ht  
tp://[redacted]:8545  
{"jsonrpc":"2.0","id":1,"result":"0xecc4"}
```



## Switzerland and Crypto

**Never enable the JSON-RPC interface on an Internet-accessible machine without a firewall policy in place to block the JSON-RPC port (default: 8545).**





# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck





# SME Cyberstudy 2021

**Homeoffice und Cybersicherheit in Schweizer KMU**  
Strategien und Massnahmen in Schweizer KMU mit 4–49 Mitarbeitenden im Umfeld von Corona (COVID-19)  
Marc K. Peter, Andreas Hölzli, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian & Nicole Wettstein

Studie Nr. 2

Die KMU-Transformation und Corona (COVID-19)

la Mobiliare satw digitalswitzerland gfs-zürich n/w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft

**Home office e cyber sicurezza nelle PMI svizzere**  
Strategie e misure adottate dalle PMI svizzere con 4–49 collaboratori nel contesto del coronavirus (COVID-19)  
Marc K. Peter, Andreas Hölzli, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian e Nicole Wettstein

studio n° 2

Trasformazione delle PMI e coronavirus (COVID-19):

la Mobiliare satw digitalswitzerland gfs-zürich n/w

**Télétravail et cybersécurité dans les PME suisses**  
Stratégies et mesures des PME suisses de 4 à 49 collaborateurs dans le contexte du coronavirus (COVID-19)  
Marc K. Peter, Andreas Hölzli, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian et Nicole Wettstein

Étude n° 2

La transformation des PME à l'heure du coronavirus (COVID-19)

la Mobilière satw digitalswitzerland gfs-zürich n/w Fachhochschule Nordwestschweiz Hochschule für Wirtschaft



# Cybersecurity: Managers' Responsibilities

MIS  
QUARTERLY  
EXECUTIVE

*Submission to MIS Quarterly Executive Call for Papers for the December 2022  
Special Issue on «Crisis-Driven Digital Transformation»  
Submitted: 28 February 2022*

## **Managers' Awareness and Protection Behavior to Combat Cyberthreats during the Cybersecurity Pandemic<sup>1</sup>**

**Marc K. Peter**  
FHNW School of Business  
Riggenbachstrasse 16  
4600 Olten, Switzerland  
+41793005560  
[marc.peter@fhnw.ch](mailto:marc.peter@fhnw.ch)

**Tsvetana Spasova**  
FHNW School of Business  
Riggenbachstrasse 16  
4600 Olten, Switzerland  
+41629572958  
[tsvetana.spasova@fhnw.ch](mailto:tsvetana.spasova@fhnw.ch)

**Miriam Christ**  
FHNW School of Business  
Riggenbachstrasse 16  
4600 Olten, Switzerland  
+41629572896  
[miriam.christ@fhnw.ch](mailto:miriam.christ@fhnw.ch)

**Nicolas Mayencourt**  
Dreamlab Technologies  
Monbijoustrasse 36  
3011 Bern, Switzerland  
+41313986666  
[nick@dreamlab.net](mailto:nick@dreamlab.net)

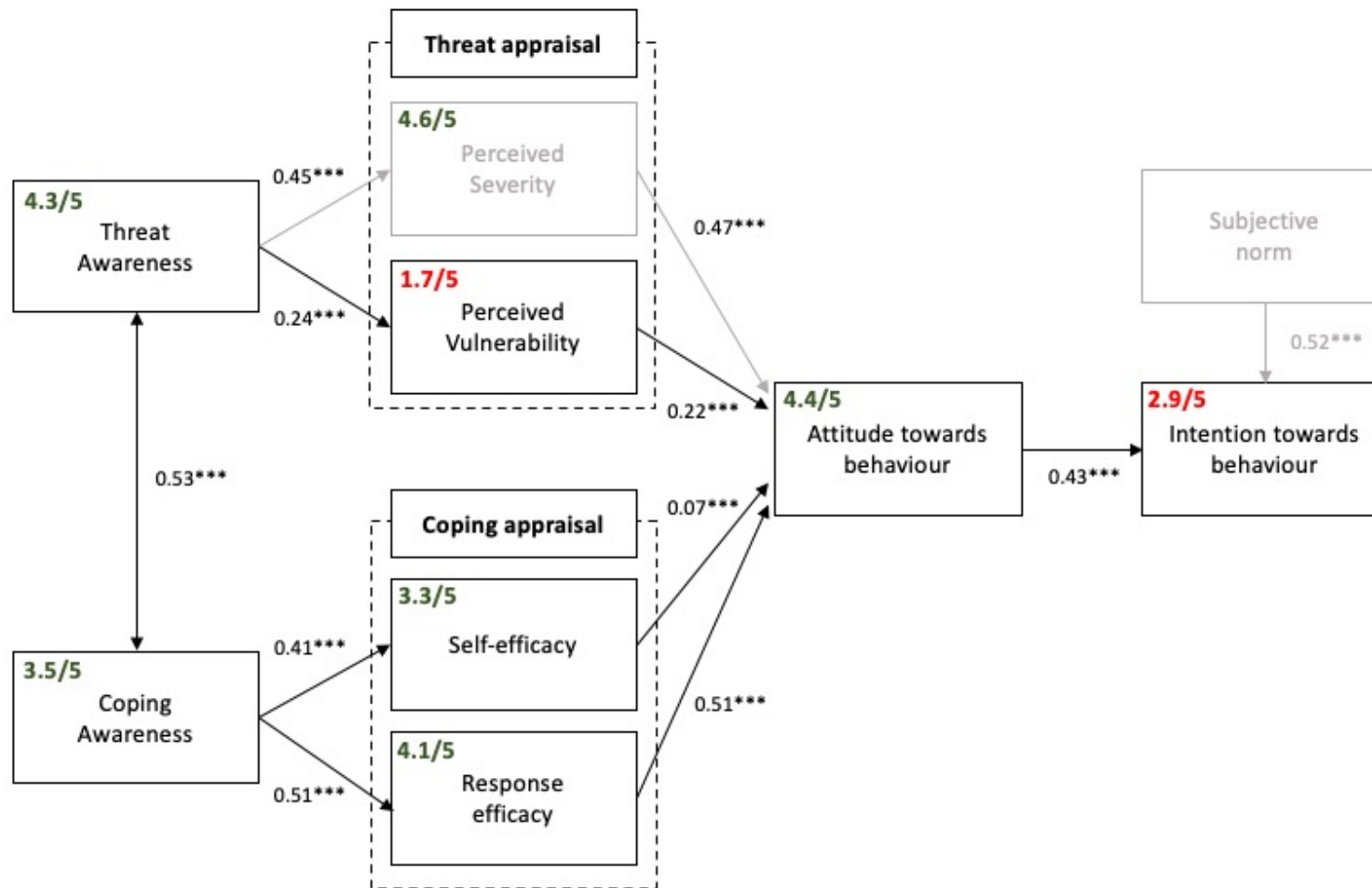
**Johan Lindeque**  
FHNW School of Business  
Riggenbachstrasse 16  
4600 Olten, Switzerland  
+41629572804  
[johan.lindeque@fhnw.ch](mailto:johan.lindeque@fhnw.ch)

**Karin Mändli Lerch**  
Gfs-Zurich  
Riedtlistrasse 9  
8006 Zürich, Switzerland  
+41443604025  
[karin.maendli@gfs-zh.ch](mailto:karin.maendli@gfs-zh.ch)

<sup>1</sup> A previous version of this article was presented as:  
Peter, M. K., Christ, M., Lindeque, J., Spasova, T., & Mändli Lerch, K. 2022. "The Cybersecurity Pandemic: Swiss SME Managers' Cyberthreats and Security Measures Awareness and Protection Motivations in Light of the Covid-19 Crisis". HICSS Hawaii International Conference on System Sciences, 5 January 2022, sponsored by The Society for Information Management and MIS Quarterly Executive.



... and the Challenge is:



Source: Peter, M.K., Christ, M., Lindeque, J., Spasova, T., Mayencourt, N., & Mändli Lerch, K. 2022. "Managers' Awareness and Protection Behavior to Combat Cyberthreats during the Cybersecurity Pandemic". Submission to MIS Quarterly Executive Call for Papers for the December 2022 Special Issue on «Crisis-Driven Digital Transformation», 28 February.



# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck



# Country Competitiveness vs. Cybersecurity Commitment

Country/Economy	Score (0-100)	Rank
Switzerland	66.08	1
Sweden	62.47	2
United States of America	60.56	3
United Kingdom	59.78	4
Netherlands	58.76	5
Denmark	57.53	6
Finland	57.02	7
Singapore	56.61	8
Germany	56.55	9
Republic of Korea	56.11	10
Hong Kong, China	55.72	11
France	53.66	12
Israel	53.55	13
China	52.97	14
Ireland	53.05	15
Spain	52.70	16
Canada	52.26	17
Luxembourg	50.84	18
Austria	50.13	19
Norway	49.29	20
Iceland	49.23	21
Belgium	49.13	22
Australia	48.35	23

The Global Innovation Index 2020

[https://www.wipo.int/global\\_innovation\\_index/en/2020/](https://www.wipo.int/global_innovation_index/en/2020/)

Country Name	Score	Rank	Country Name	Score	Rank
United States of America**	100	1	Indonesia	94.88	24
United Kingdom	99.54	2	Viet Nam	94.59	25
Saudi Arabia	99.54	2	Sweden	94.59	26
Estonia	99.48	3	Qatar	94.59	27
Korea (Rep. of)	98.54	4	Greece	93.86	28
Singapore	98.54	4	Australia	93.86	29
Spain	98.54	4	Poland	93.86	30
Russian Federation	98.06	5	Kazakhstan	93.15	31
United Arab Emirates	98.06	5	Denmark	92.6	32
Malaysia	98.06	5	China	92.53	33
Lithuania	97.93	6	Croatia	92.53	33
Japan	97.82	7	Slovakia	92.36	34
Canada**	97.67	8	Hungary	91.28	35
France	97.6	9	Israel**	90.93	36
India	97.5	10	Tanzania	90.58	37
Turkey	97.49	11	North Macedonia	89.92	38
Australia	97.47	12	Serbia	89.8	39
Luxembourg	97.41	13	Azerbaijan	89.31	40
Germany	97.41	13	Cyprus	88.82	41
Portugal	97.32	14	Switzerland**	86.97	42
Italy	97.28	15	Ghana	86.69	43

Global Cybersecurity Index 2020

<https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020>

HOW DO



WE IMPROVE?



## Recommendations

The Cyber Dimension – Need for a Paradigm Shift

Accountabilities  
of a Digital Society  
(incl. awareness and  
education)

Digital Rights  
and  
Privacy

Cyber Peace  
and  
Product Safety



For Swiss SMEs (and many more)





# cybercheck.dreamlab.net

## Beobachter & Dreamlab Cybercheck

# Beobachter

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

**IT-SICHERHEIT KMU-SELBSTTEST**

### Bericht: Auswertung und Handlungsempfehlungen

Besten Dank für das Ausfüllen des Cybersecurity-Selbsttests am 31.01.2022! Nachfolgend finden Sie Ihre Ergebnisse sowie die Möglichkeit umgehend weitere Schritte einzuleiten, um die IT-Sicherheit Ihres Unternehmens zu stärken.

Die Ergebnisse basieren ausschließlich auf den von Ihnen während des Selbsttests getätigten Angaben. Dreamlab Technologies hat hierzu keine weiteren Analysen durchgeführt. Aufgezeigte Stärken und Schwächen Ihrer IT-Sicherheit sollten in jedem Fall fachmännisch nachgeprüft werden.

**AUSWERTUNG UND ÜBERBLICK**

Im folgenden Diagramm sind die Ergebnisse Ihrer Antworten zusammengefasst. Es zeigt auf, in welchen Bereichen Ihr Unternehmen gut aufgestellt ist und wo allenfalls Nachholbedarf besteht. Dabei gilt: Je weiter hinaus die jeweilige Dimension gefüllt ist, desto besser das Ergebnis.

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

**IN DIESEN BEREICHEN SIE GUT AB:**

- Zugänglichkeit

**IN DIESEN BEREICHEN ETWAS VERBESSERT WERDEN:**

- Kommunikation
- IT-Sicherheit

**IN DIESEN BEREICHEN DEUTLICHE VERBESSERUNGEN NOTWENDIG:**

- Infrastruktur
- Organisation

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

### HANDLUNGSEMPFEHLUNGEN FÜR IHR UNTERNEHMEN

Aufgrund Ihrer Antworten ergeben sich folgende zusätzliche Handlungsempfehlungen.

#### NETZWERKÜBERSICHT

Eine Netzwerkübersicht oder ein Zonenplan ist eine wichtige Grundlage, damit Ihre IT-Infrastruktur ausreichend geschützt ist. Deshalb sollten Sie eine solche Übersicht erstellen bzw. erstellen lassen und aktuell halten.

#### ANTIVIREN

Häufige und regelmäßige Antivirenschans helfen, Schadsoftware zu erkennen und unschädlich zu machen. Es lohnt sich, mindestens wöchentliche Scans durchzuführen – auch der Server.

#### BACK-UP

Einer der Hauptzwecke von Back-ups ist die Wiederherstellung von Daten, zum Beispiel nach einem Befall durch Ransomware. Daher ist die Erstellung regelmäßiger Back-ups essenziell. Entscheidend ist – gerade im Fall einer Ransomware –, dass Back-ups physisch vom Netzwerk getrennt aufbewahrt werden, da sie sonst möglicherweise ebenfalls befallen und somit unbrauchbar gemacht werden.

#### DURCHFÜHRUNG VON SENSIBILISIERUNGSMASSNAHMEN

Mitarbeitende sollen immer wieder über aktuelle Bedrohungen und Entwicklungen informiert und sensibilisiert werden. Je regelmäßiger und professioneller dies geschieht, desto höher die Chance, dass Mitarbeitende im Ernstfall die richtigen Entscheidungen treffen und Schlimmeres verhindern können. Schulen Sie Ihre Mitarbeitenden mindestens einmal jährlich bezüglich IT-Sicherheit und gestalten Sie die Schulungen so, dass sie einen bleibenden Eindruck hinterlassen.

#### IMPLIKATIONEN DER NEUEN EU-DATENSCHUTZGRUNDVERORDNUNG

Am 25. Mai 2018 ist die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Diese sieht bei Verstößen, die zu Datenpannen führen, hohe Strafen vor. Sofern Sie Personendaten von EU-Bürgerinnen verarbeiten, unterstehen Sie automatisch der DSGVO. Obwohl die Durchsetzung in der Schweiz von Fall zu Fall sehr unterschiedlich geschieht, sollten Sie die Auswirkungen der DSGVO auf Ihr Unternehmen und den Handlungsbedarf rechtzeitig abklären. Dies umso mehr, da auch das Schweizer Datenschutzgesetz (DSG), das aktuell überarbeitet wird, sich voraussichtlich stark an die DSGVO anlehnen wird.

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

**OFFENE FRAGEN**

Hier sind alle Fragen aufgeführt, die bei der Bearbeitung ausgelassen oder nicht beantwortet wurden. Es empfiehlt sich, sich bei diesen Fragen nachzugehen und die entsprechenden Informationen einzuholen, falls diese für Ihre IT-Sicherheit relevant sind.

*Gibt es in Ihrem Unternehmen eine Richtlinie zur Verwendung von Dienstleistungen (zum Beispiel Cloud-Dienste wie OneDrive)?*

*Werden E-Mails Ihres Unternehmens verschlüsselt? (Beispiel PGP) Versenden Sie uns Ihre Antworten.*

**Zugänglichkeit**

**Organisation und Verfahren**

**Kommunikation**

**IT-Sicherheit**

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

### VERHALTEN BEI SICHERHEITRELEVANTEN VORKOMMISSEN

Klare Wege und Ansprechpartner sind bei Sicherheitsvorfällen immens wichtig. Stellen Sie sicher, dass Ihre Mitarbeitenden jederzeit im Bild sind, an wen sie sich für IT-Sicherheitsfragen wenden sollen und wie sie dies konkret tun können.

### SCHUTZBEDARFSANALYSE

Damit Sie sich vor Cyberbedrohungen schützen, im Ernstfall reagieren und einen kühlen Kopf bewahren können, müssen Sie wissen, welche Informationen und Systeme geschäftskritisch sind und noch stärker geschützt werden müssen. Identifizieren Sie im Rahmen einer Schutzbedarfsanalyse, ausgehend von Ihren Geschäftsprozessen, die relevanten, besonders kritischen Informationen und Systeme und dokumentieren Sie diese.

### UMGANG MIT IT-SICHERHEITSRISIKEN UND -BEDROHUNGEN

IT-Sicherheitsrisiken sind Geschäftsrisiken. Die Verantwortung für IT-Sicherheit im Unternehmen obliegt somit letztlich dem Management bzw. dem Verwaltungsrat, welcher nach Schweizer Obligationenrecht eine Sorgfaltspflicht wahrzunehmen hat. Integrieren Sie das Thema IT-Sicherheit bzw. die Risiken, die sich aus IT-Sicherheitsbedrohungen ergeben in geeigneter Form in Ihr Gesamt-Risikomanagement und behandeln Sie es gleichwertig wie andere essenzielle Risiken.

### IT-SICHERHEIT ALS INTEGRALER BESTANDTEIL VON PROJEKTEN

IT-Sicherheitsrisiken können zu existenziellen Bedrohungen für Projekte werden. Es reicht weder aus, zu Projektbeginn ein Sicherheitskonzept zu erstellen und dann in der Schublade verschwinden zu lassen, noch am Projektende ein paar Sicherheitsmassnahmen zu definieren, welche nachträglich umgesetzt werden sollen, da zu diesem Zeitpunkt sowieso bereits alle wichtigen Entscheide gefällt wurden und gravierende Mängel nicht mehr behoben werden können.

Wir empfehlen, IT-Sicherheit zu einem integralen Projektbestandteil zu machen, welcher im Projektverlauf genau wie alle anderen Projekt- und Betriebsrisiken laufend bewirtschaftet und behandelt wird.

**DREAMLAB TECHNOLOGIES**  
Nicht glauben. Wissen.

**Beobachter**

### KONTAKTINFORMATIONEN

Für Rückfragen und weitere Auskünfte, kontaktieren Sie bitte Dreamlab Technologies unter 031 398 66 66 oder via E-Mail an [cybercheck@dreamlab.net](mailto:cybercheck@dreamlab.net).

Der kostenlose Selbsttest zur Bestimmung der IT-Sicherheit – mit Handlungsempfehlungen – wurde vom Dreamlab Technologies entwickelt.

Weitere Informationen:  
[www.dreamlab.net](http://www.dreamlab.net)  
[www.it-sicherheit.ch](http://www.it-sicherheit.ch)

**Autoren:**

Jacek Jonczy, Leiter IT-Sicherheitsaudits bei Dreamlab Technologies.  
Nicolas Mayencourt, Gründer und CEO von Dreamlab Technologies.  
Mischa Obrecht, Projektleiter und Berater bei Dreamlab Technologies.  
Marc K. Peter, Berater bei Dreamlab Technologies.





# Agenda

Review 2021

Swiss Public  
Attack Surface  
by CyObs

Command and Control  
(C2) Systems  
by RATspotting

Swiss Crypto  
Nodes

Threat Protection  
Motivation

Conclusion &  
Cybercheck

STOP  
BEING  
NAÏVE



DREAMLAB  
TECHNOLOGIES



# Contact

## Dreamlab Offices

Get in touch with us: [contact@dreamlab.net](mailto:contact@dreamlab.net)  
And follow us at: [twitter.com/DreamlabGlobal](https://twitter.com/DreamlabGlobal)  
[linkedin.com/company/dreamlab-technologies-ag](https://linkedin.com/company/dreamlab-technologies-ag)



### Dreamlab Switzerland

Dreamlab Technologies  
Monbijoustrasse 36  
Switzerland – 3011 Bern

### Dreamlab Spain

Dreamlab Technologies  
Calle Hermosilla 48  
1. Dcha  
Spain – 28001 Madrid

### Dreamlab Chile

Dreamlab Technologies  
Villavicencio 361, Oficina 113  
Chile – 8320154 Santiago de Chile

### Dreamlab Oman

Dreamlab Technologies LLC  
Minarit Al Qurum Building  
2nd floor, Office No. 233  
Postal Code 133  
Al Khuwair, Sultanate of Oman