DREAMLAB
TECHNOLOGIES

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

Nicolas Mayencourt
Keynote | Lausanne, 22. November

Dreamlab Technologies

Introduction

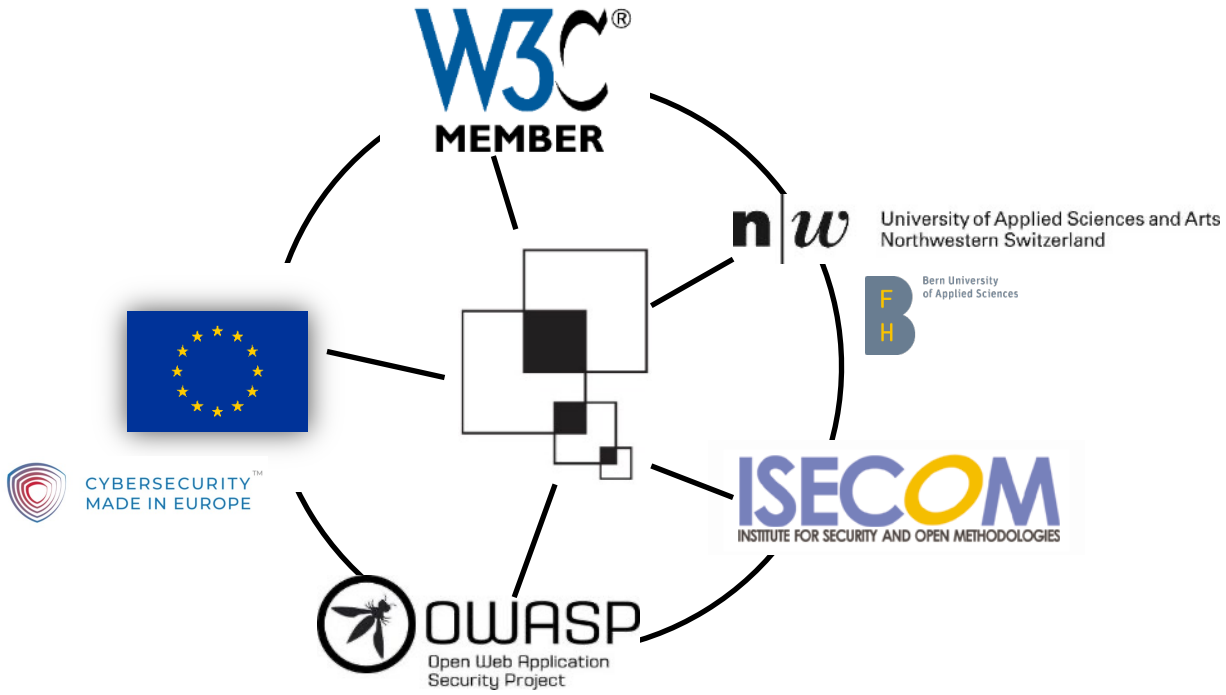
Nick Mayencourt

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

Dreamlab Technologies
Dedication

swiss cyber security DAYS

Dreamlab Technologies

Plattform für Politik & Wirtschaft

Agenda

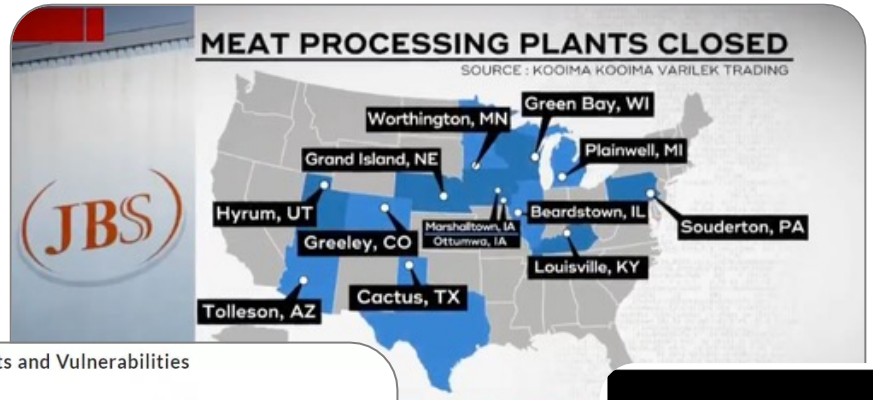
- Review 2021
- Swiss Public Attack Surface by CyObs
- Command and Control (C2) Systems by RATspotting
- Swiss Crypto Nodes
- Threat Protection Motivation
- Conclusion & Cybercheck

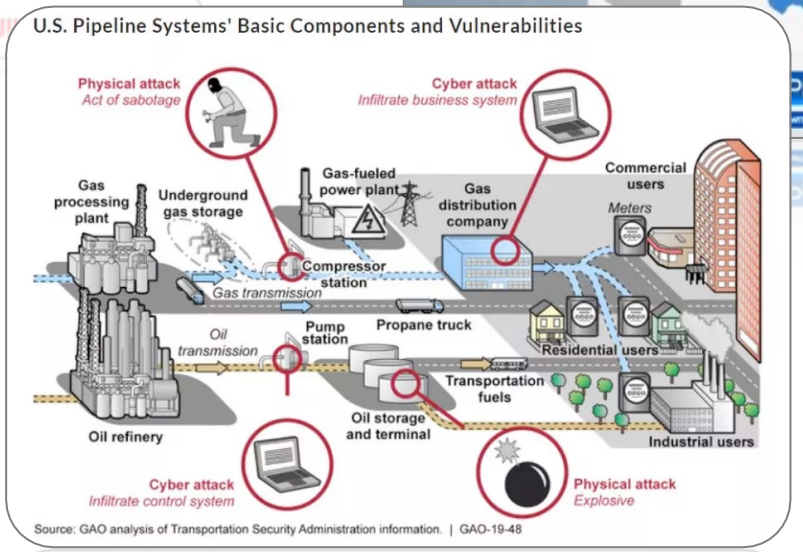
Agenda

- 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

Sources: https://www.netzwoche.ch/news/2022-03-28/bfs-zaehlt-fast-83-digitale-straftaten-pro-tag / BfS (2022): Die Schweiz in 23 Infografiken: Gesellschaft, Wirtschaft, Raum und Umwelt, Neuenburg.

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/

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/

- ✓ 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/

VS

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43

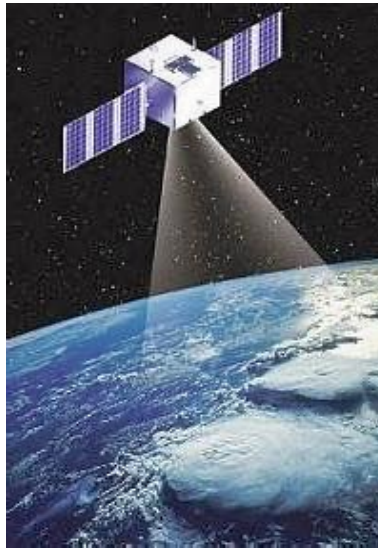
Global Cybersecurity Index 2020

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

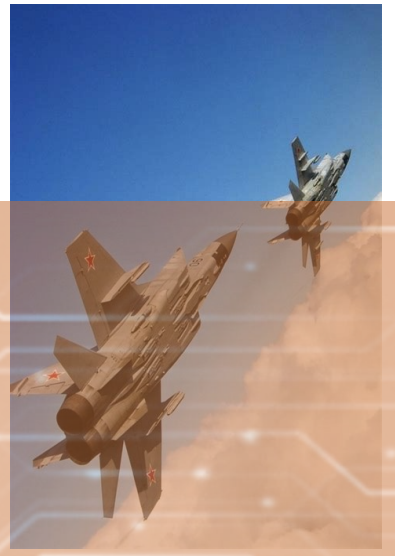
LAND	SEA	AIR	SPACE
			

Dimensions

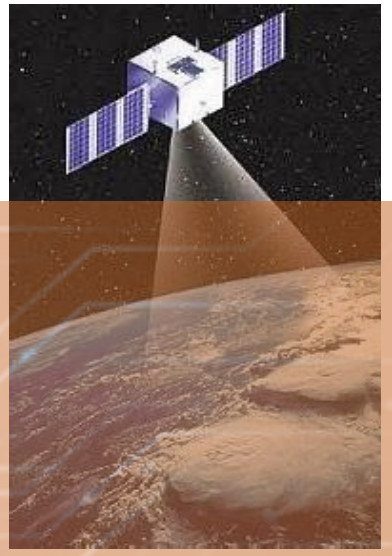
LAND

SEA

AIR



SPACE



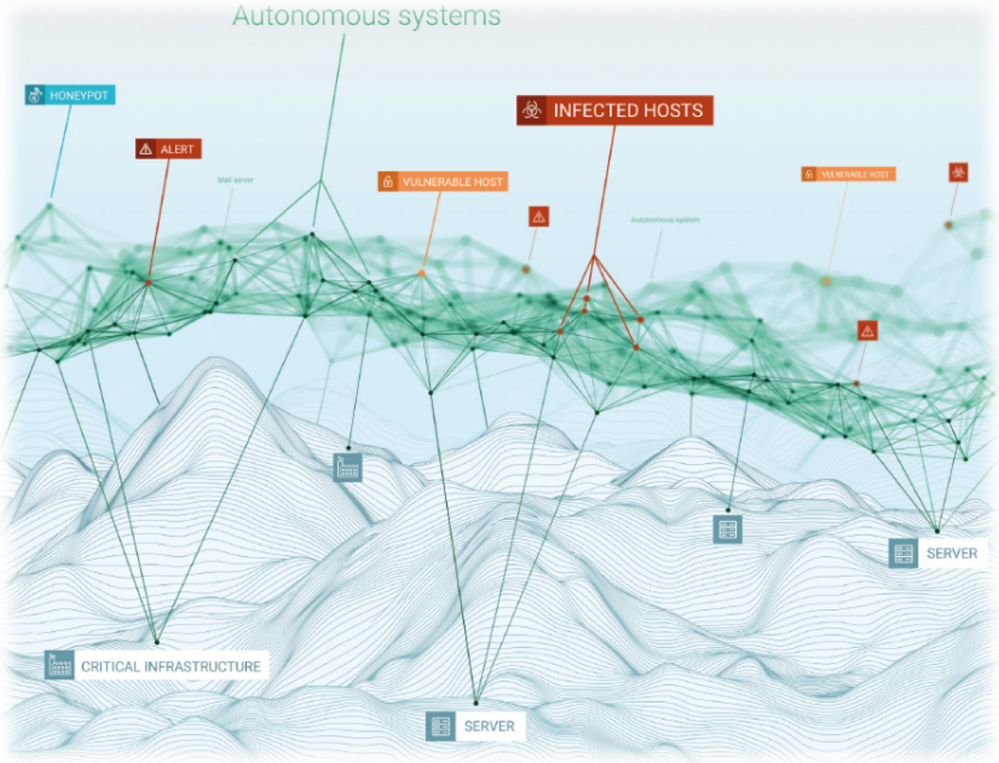
CYBER

CyObs

Introduction

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

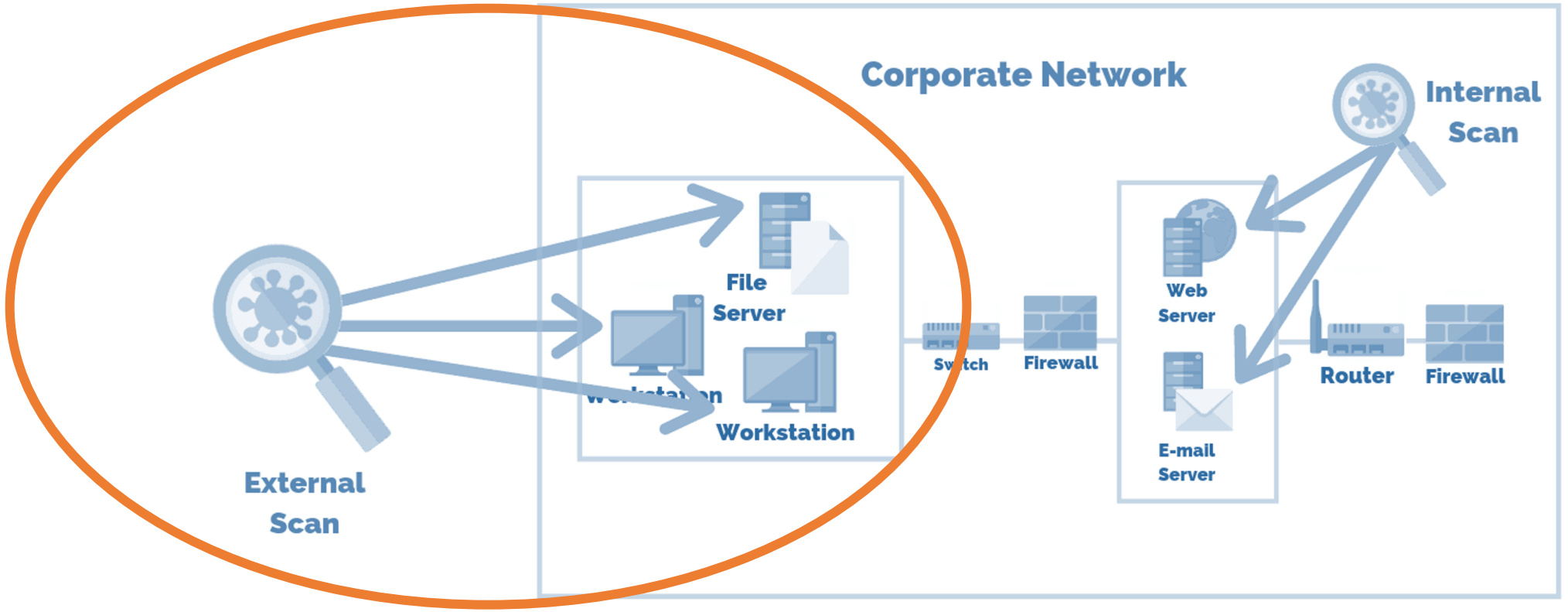
- Land
- Air
- Water
- and **Cyberspace**



- 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

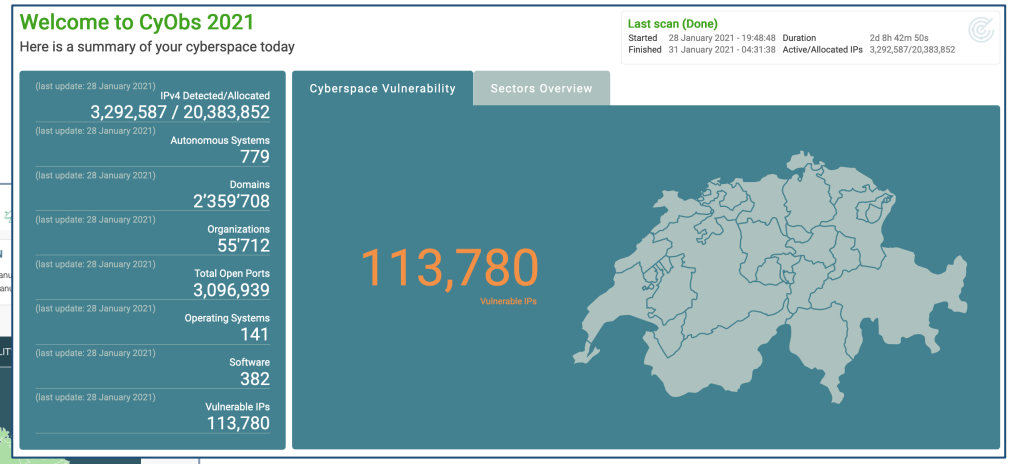
Introduction



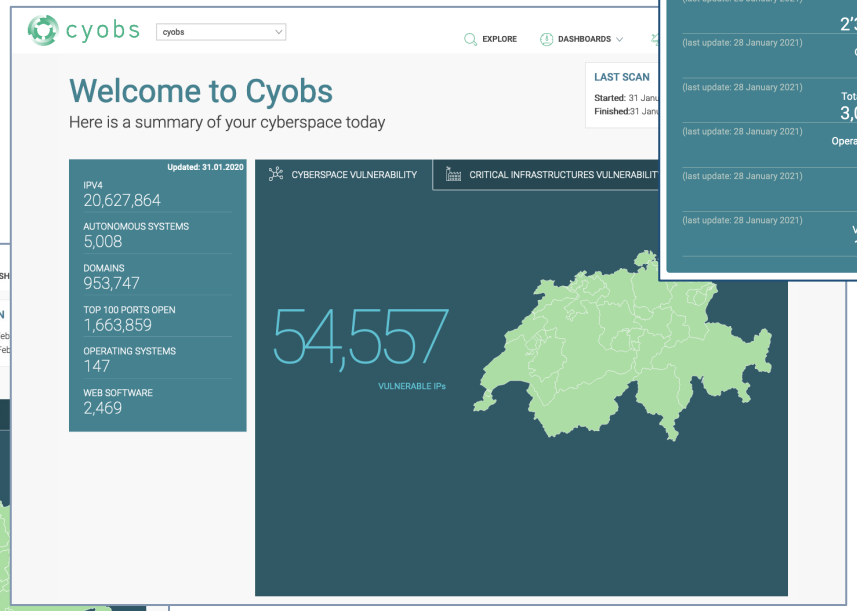
Source: https://purplesec.us/internal-vs-external-vulnerability-scans/

The Swiss Cyberspace 2019 to 2021

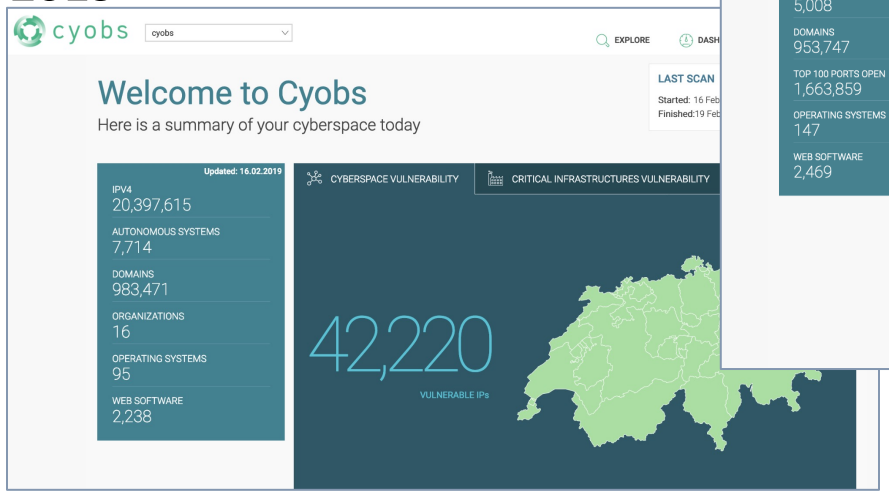
2021



2020



2019



Source: Dreamlab Technologies AG, CyObs & Audit Department, 31 January 2021

The Swiss Cyberspace 2022

Welcome to CyObs

Here is a summary of your cyberspace today

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

Cyberspace Vulnerability | Sectors Overview

106,577
Vulnerable IPs

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

The Swiss Cyberspace 2022

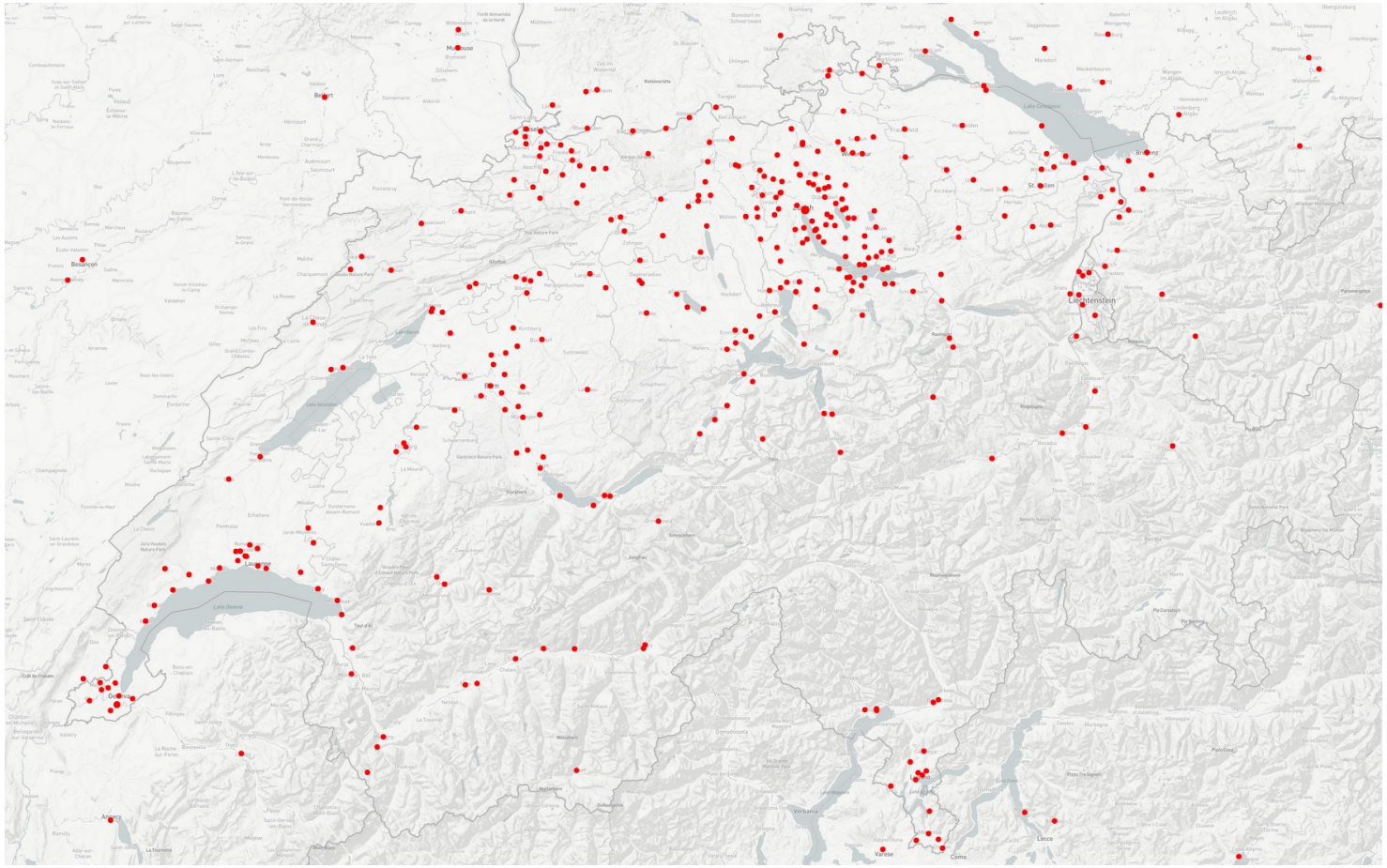
Overview

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

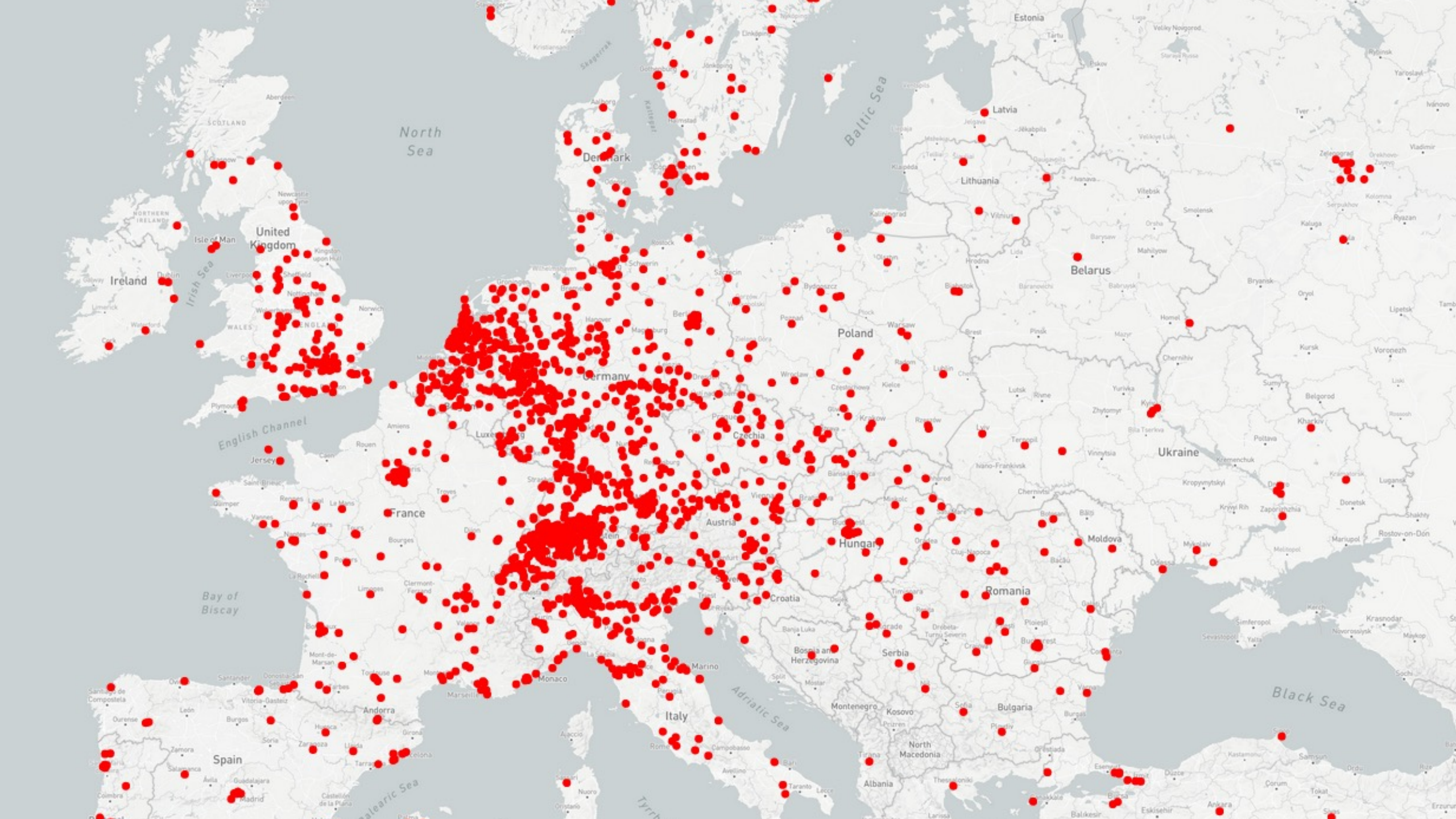
Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

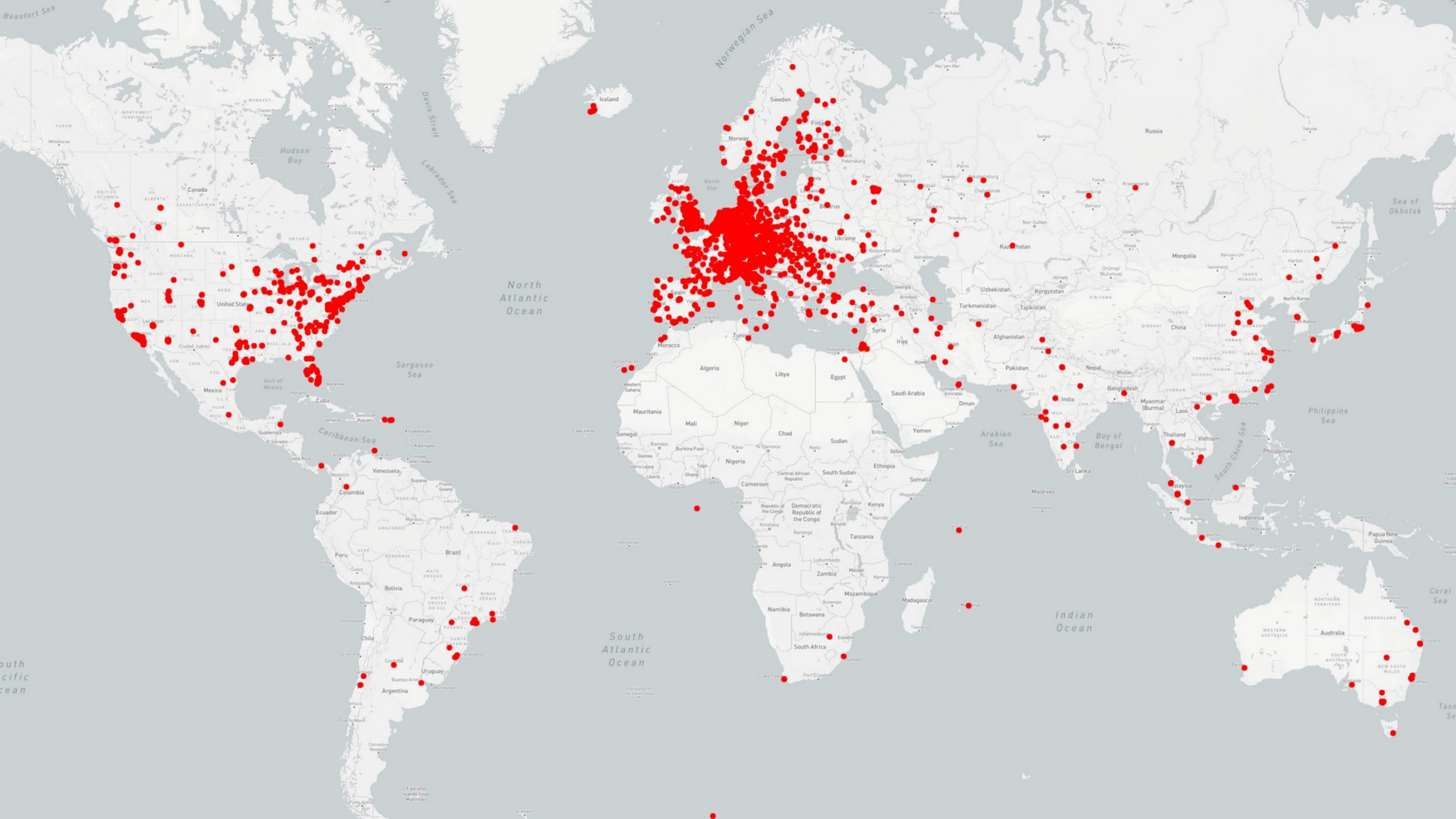
The Swiss Cyberspace 2022

.ch DNS Server Distribution



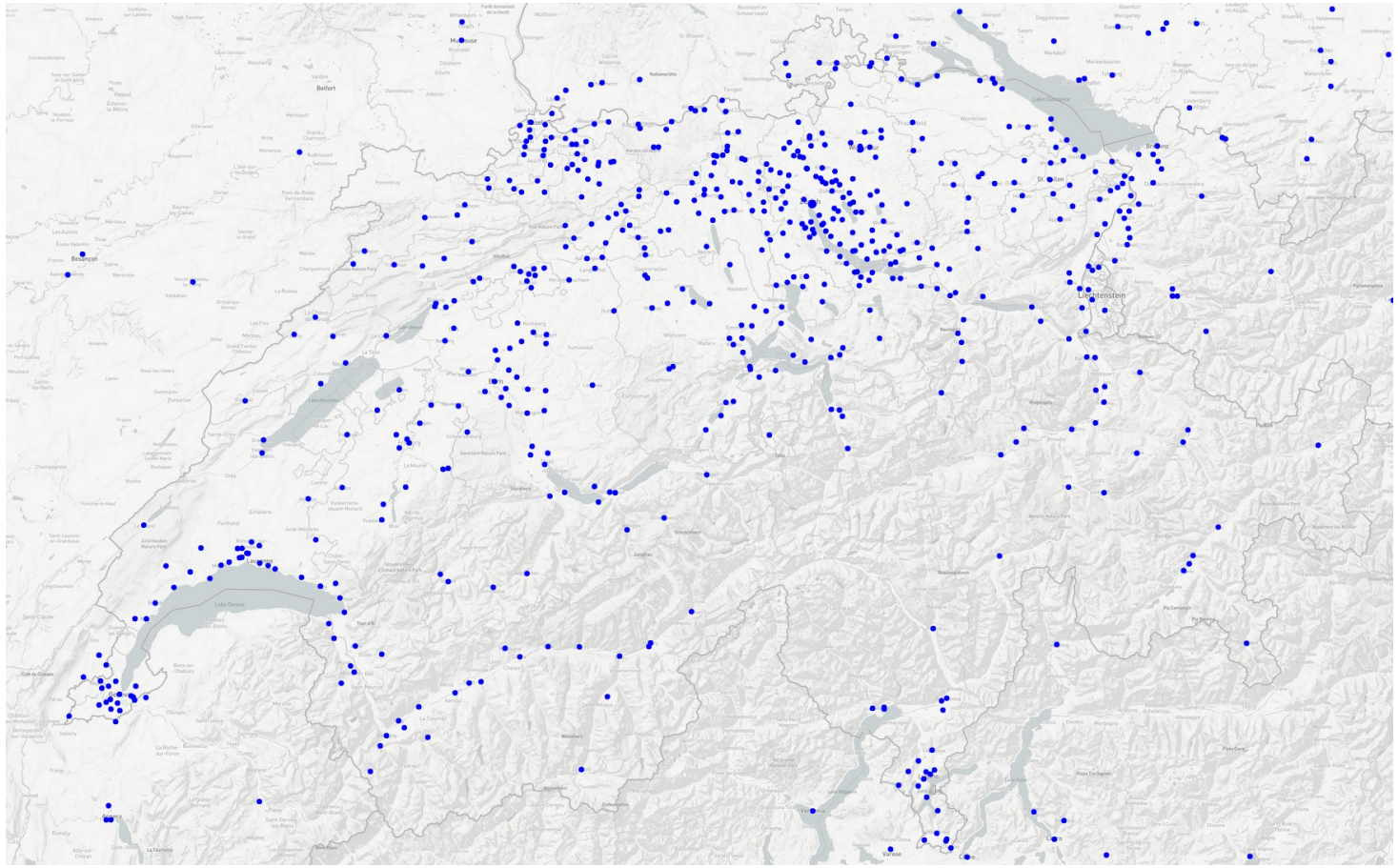
Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022


North Sea
Baltic Sea
Denmark
Estonia
Latvia
Lithuania
Belarus
United Kingdom
Ireland
Isle of Man
Irish Sea
English Channel
Bay of Biscay
Poland
Germany
Czechia
Ukraine
France
Austria
Hungary
Moldova
Romania
Croatia
Serbia
Bosnia and Herzegovina
Montenegro
Kosovo
Bulgaria
North Macedonia
Albania
Italy
Spain
Andorra
Monaco
San Marino
Adriatic Sea
Black Sea

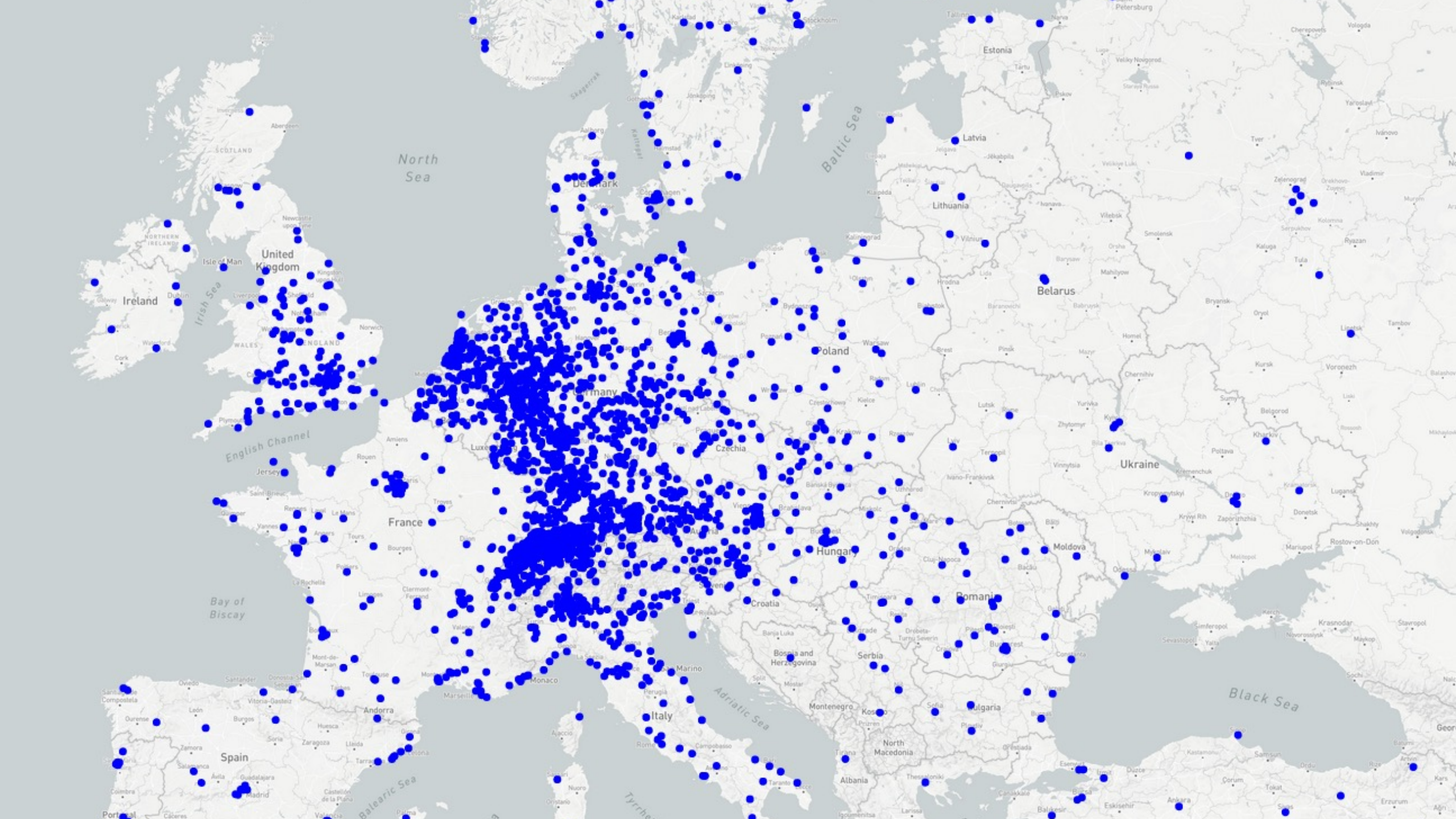

Beaufort Sea
Hudson Bay
Davis Strait
Labrador Sea
Norwegian Sea
Iceland
Sweden
Norway
Finland
Russia
Canada
United States
Mexico
Cuba
Caribbean Sea
Sargasso Sea
North Atlantic Ocean
Gulf of Mexico
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
South Atlantic Ocean
Morocco
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Cameroon
Ethiopia
South Sudan
Somalia
Kenya
Tanzania
Angola
Zambia
Mozambique
Namibia
Botswana
South Africa
Madagascar
Ukraine
Belarus
Kazakhstan
Mongolia
Uzbekistan
Kyrgyzstan
Tajikistan
Turkmenistan
Afghanistan
Pakistan
Iran
Iraq
Syria
Saudi Arabia
Yemen
Oman
India
Nepal
Bangladesh
China
North Korea
South Korea
Japan
Sea of Okhotsk
Philippine Sea
Arabian Sea
Bay of Bengal
South China Sea
Myanmar (Burma)
Laos
Thailand
Vietnam
Malaysia
Indonesia
Philippines
Sri Lanka
Maldives
Indian Ocean
Australia
Papua New Guinea
Coral Sea

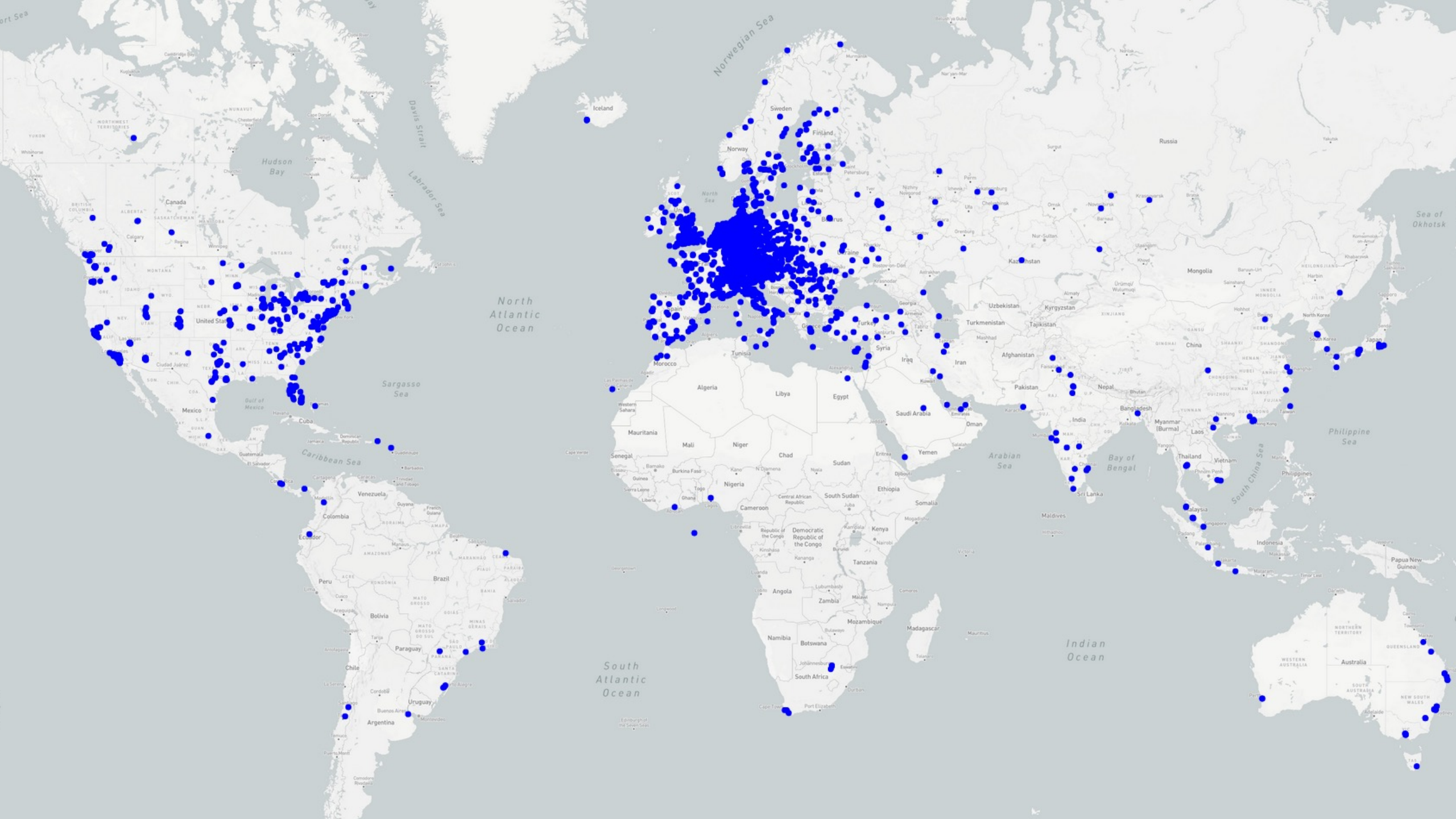
The Swiss Cyberspace 2022

.ch Mail Server Distribution



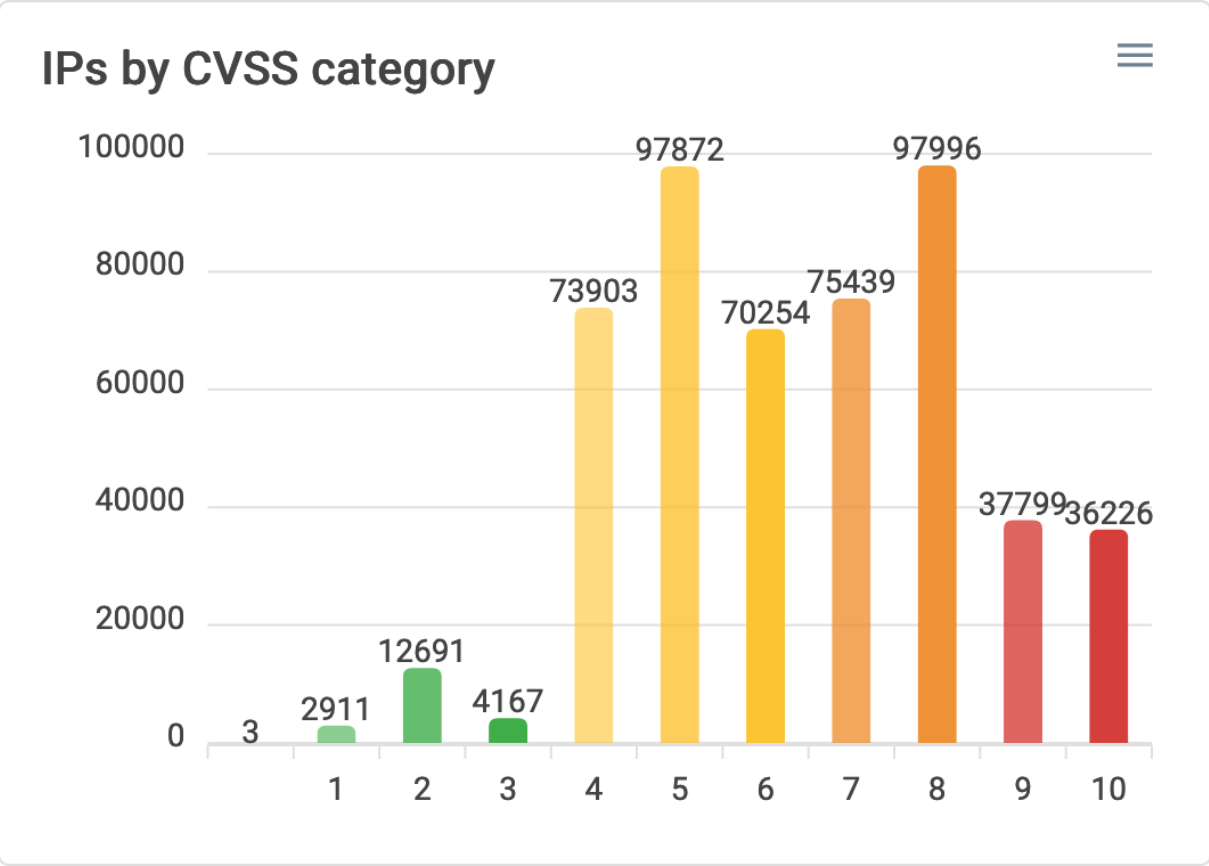
Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022


North Sea
Baltic Sea
Ireland
United Kingdom
Irish Sea
English Channel
Bay of Biscay
France
Spain
Andorra
Monaco
Italy
Adriatic Sea
Balearic Sea
Tyrrhenian Sea
Black Sea
Denmark
Estonia
Latvia
Lithuania
Belarus
Poland
Germany
Czechia
Ukraine
Moldova
Romania
Hungary
Croatia
Bosnia and Herzegovina
Serbia
Montenegro
North Macedonia
Albania
Bulgaria


Norwegian Sea
Iceland
Sweden
Finland
Norway
Russia
Hudson Bay
Davis Strait
Labrador Sea
Canada
North Atlantic Ocean
Sea of Okhotsk
Mongolia
Kazakhstan
Uzbekistan
Kyrgyzstan
Turkmenistan
Tajikistan
Afghanistan
China
North Korea
South Korea
Japan
Sargasso Sea
Gulf of Mexico
Mexico
Cuba
Caribbean Sea
Morocco
Algeria
Tunisia
Libya
Egypt
Syria
Iraq
Iran
Saudi Arabia
Pakistan
India
Nepal
Bangladesh
Myanmar (Burma)
Laos
Thailand
Vietnam
Philippine Sea
Philippines
South China Sea
Arabian Sea
Bay of Bengal
Sri Lanka
Maldives
Malaysia
Indonesia
Papua New Guinea
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Senegal
Ethiopia
Somalia
Yemen
Oman
Cameroon
South Sudan
Kenya
Tanzania
Angola
Zambia
Mozambique
Madagascar
Namibia
Botswana
South Africa
Indian Ocean
South Atlantic Ocean
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
Australia

The Swiss Cyberspace 2022

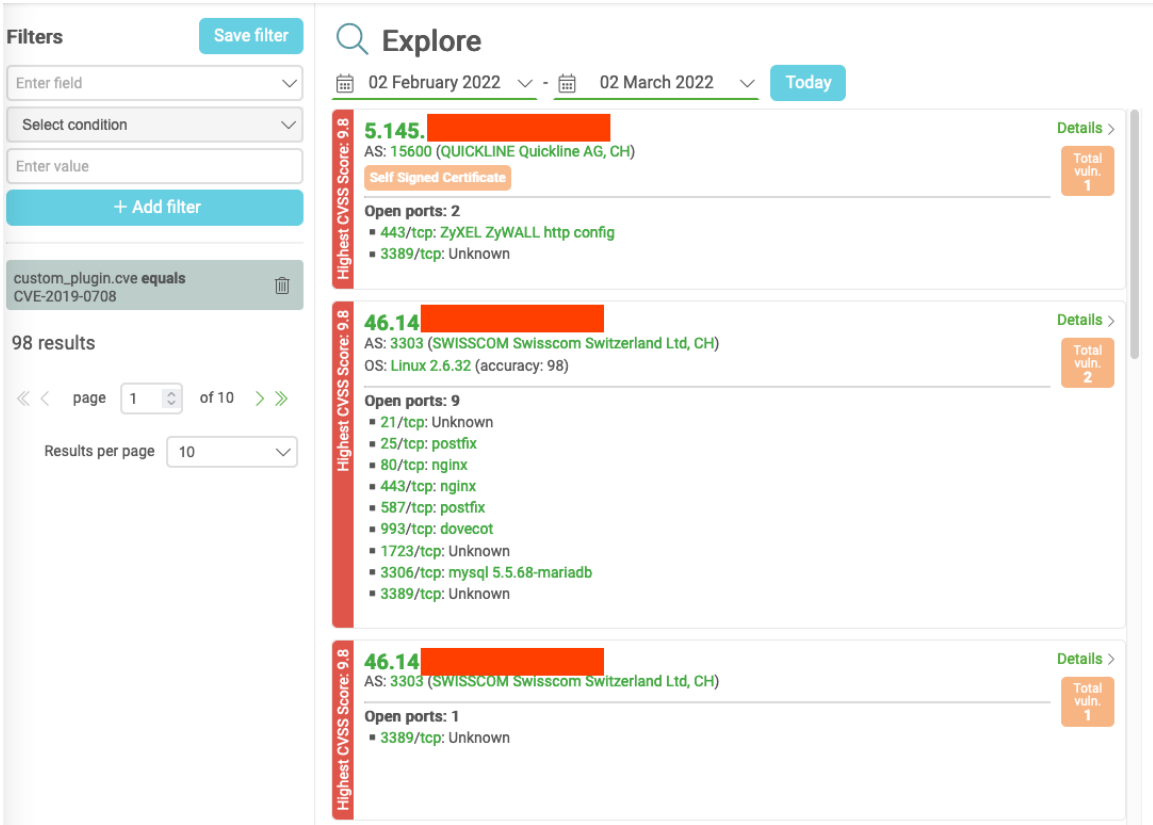
Vulnerabilities Overview

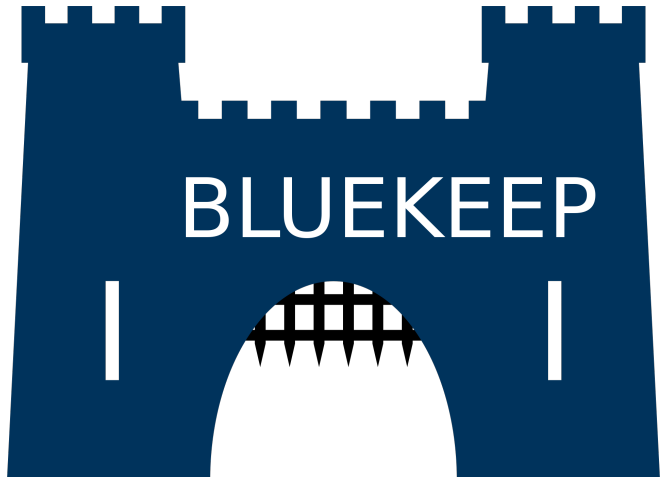


Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

The Swiss Cyberspace 2022

Bluekeep





98 hits for Bluekeep (CVE-2019-0708)

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

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.

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

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

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

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

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

The Swiss Cyberspace 2022

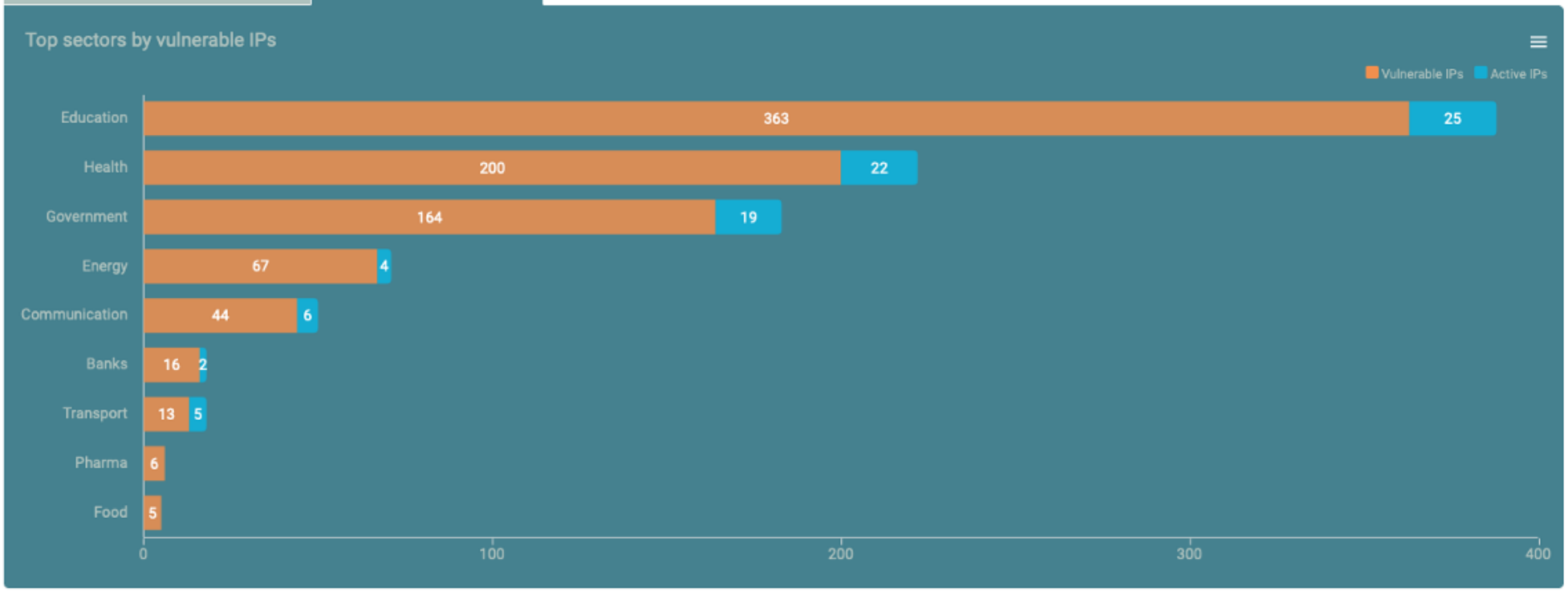
Industry/Sector View

Welcome to CyObs

Here is a summary of your cyberspace today

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

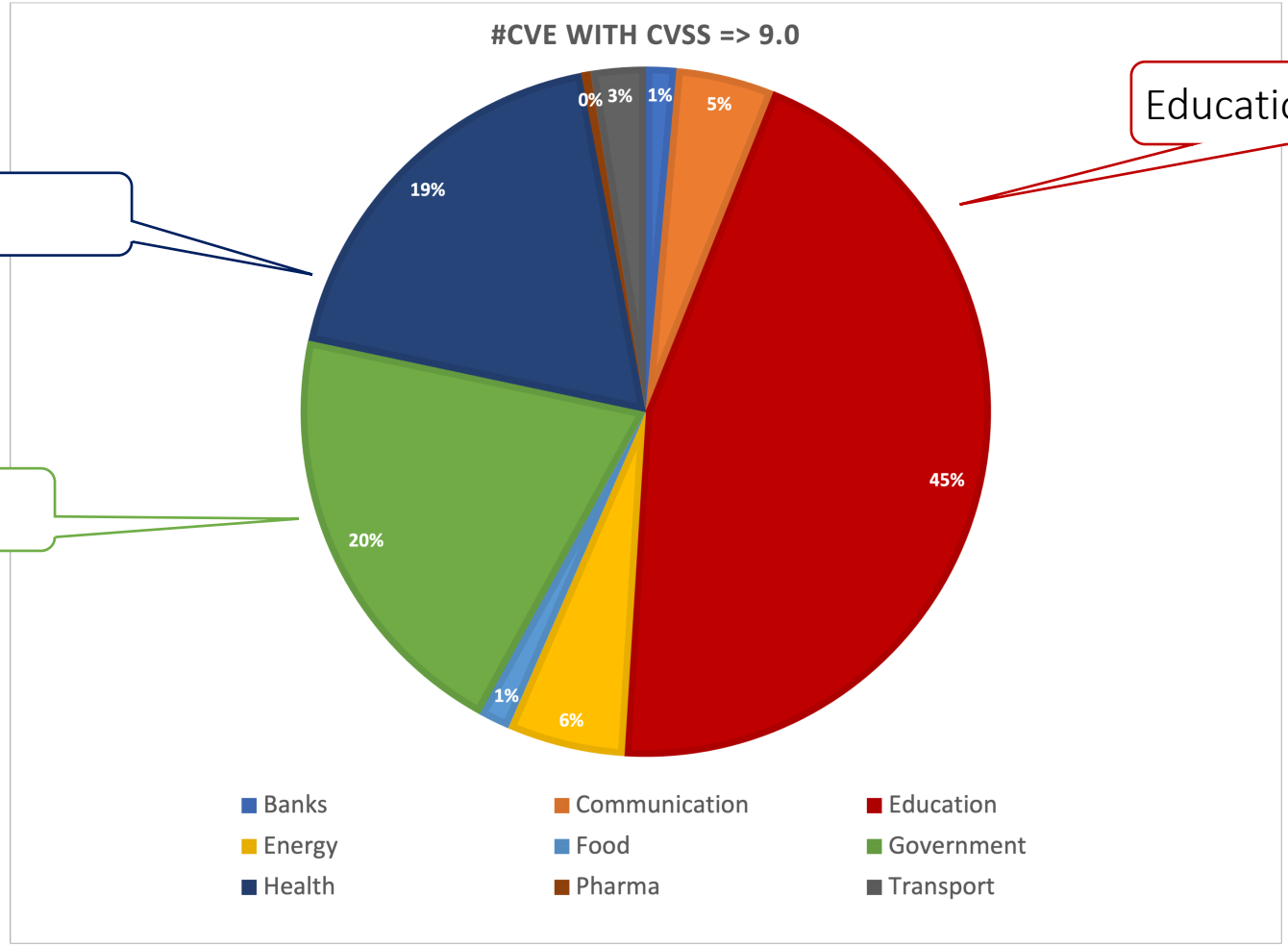
Cyberspace Vulnerability | Sectors Overview



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

Number of CVE matches for all domains per Sector

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

The Swiss Cyberspace 2022

Welcome to CyObs

Here is a summary of your cyberspace today

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

Cyberspace Vulnerability | Sectors Overview

106,577
Vulnerable IPs

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

Agenda

Review 2021

Swiss Public Attack Surface by CyObs

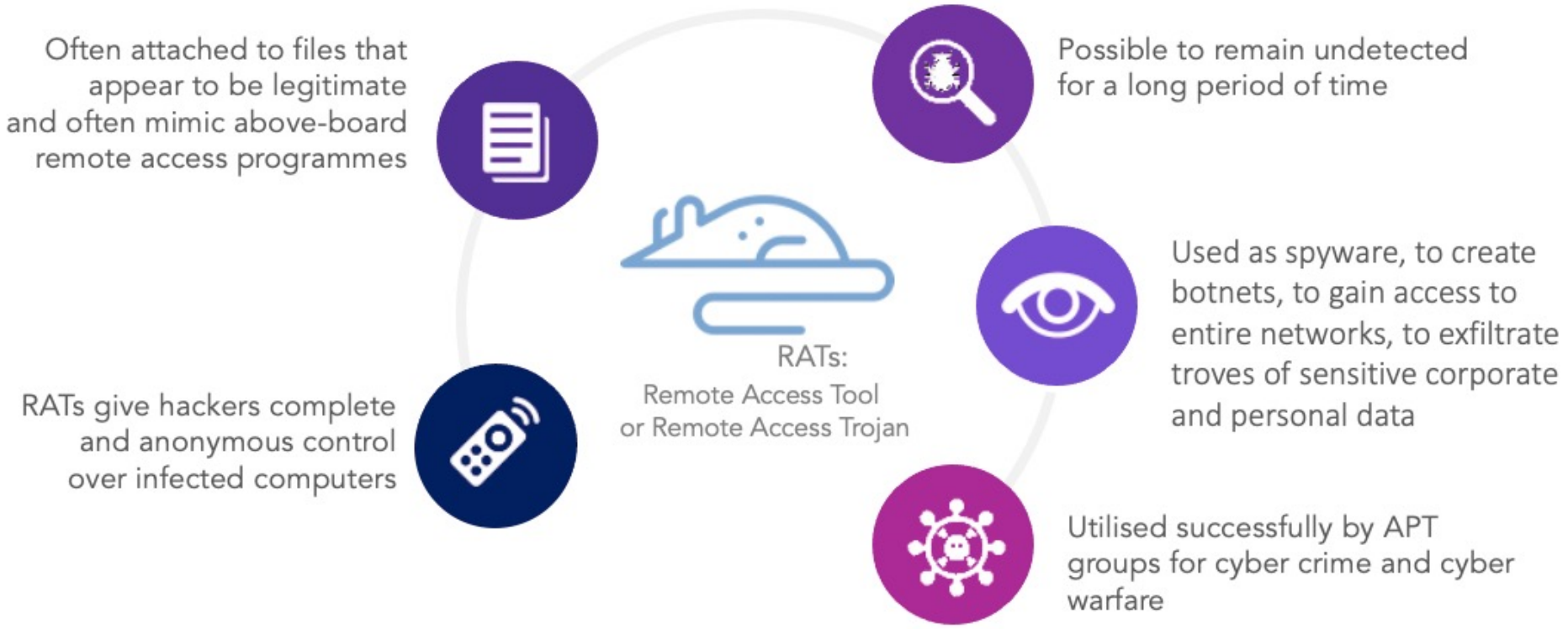
Command and Control (C2) Systems by RATspotting

Swiss Crypto Nodes

Threat Protection Motivation

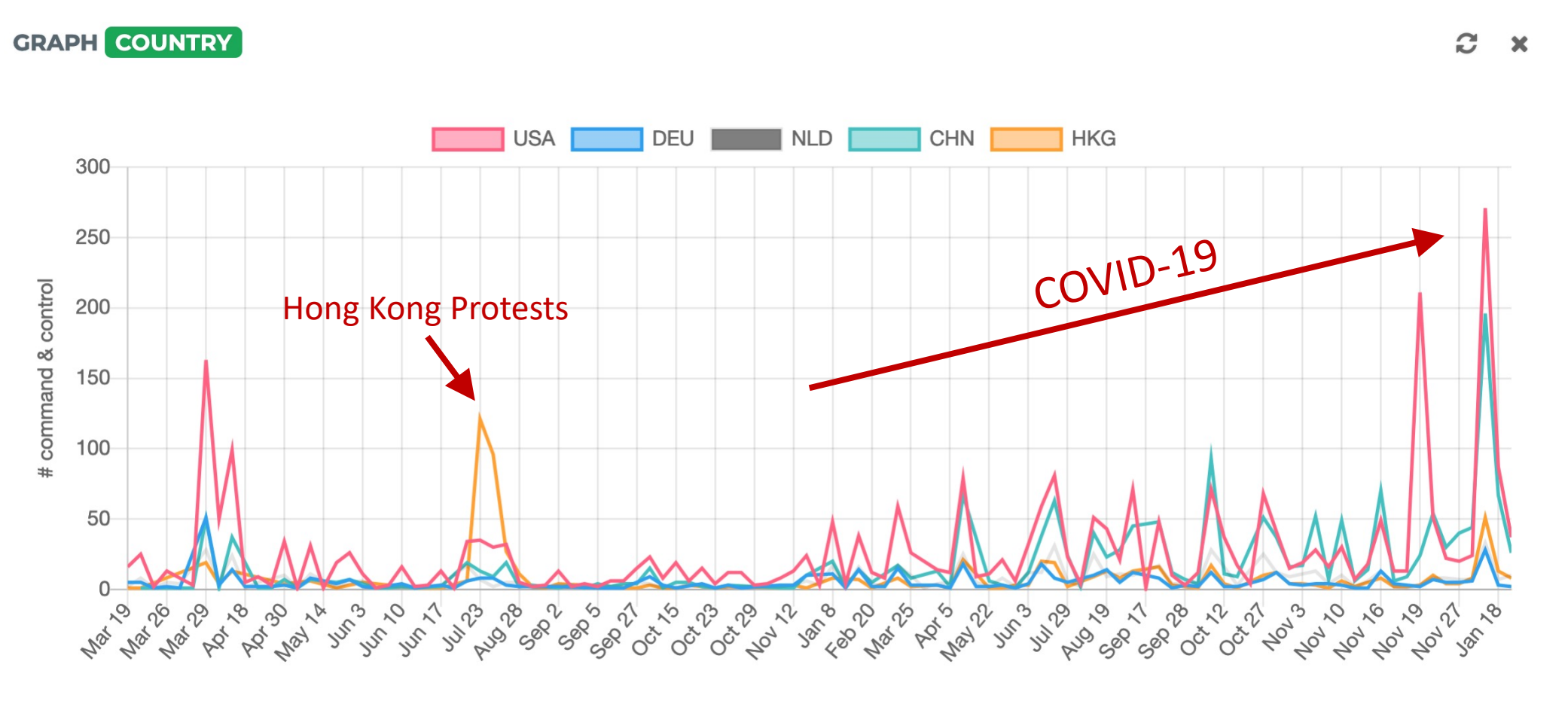
Conclusion & Cybercheck

RATspotting – Comand and Control (C2) Systems



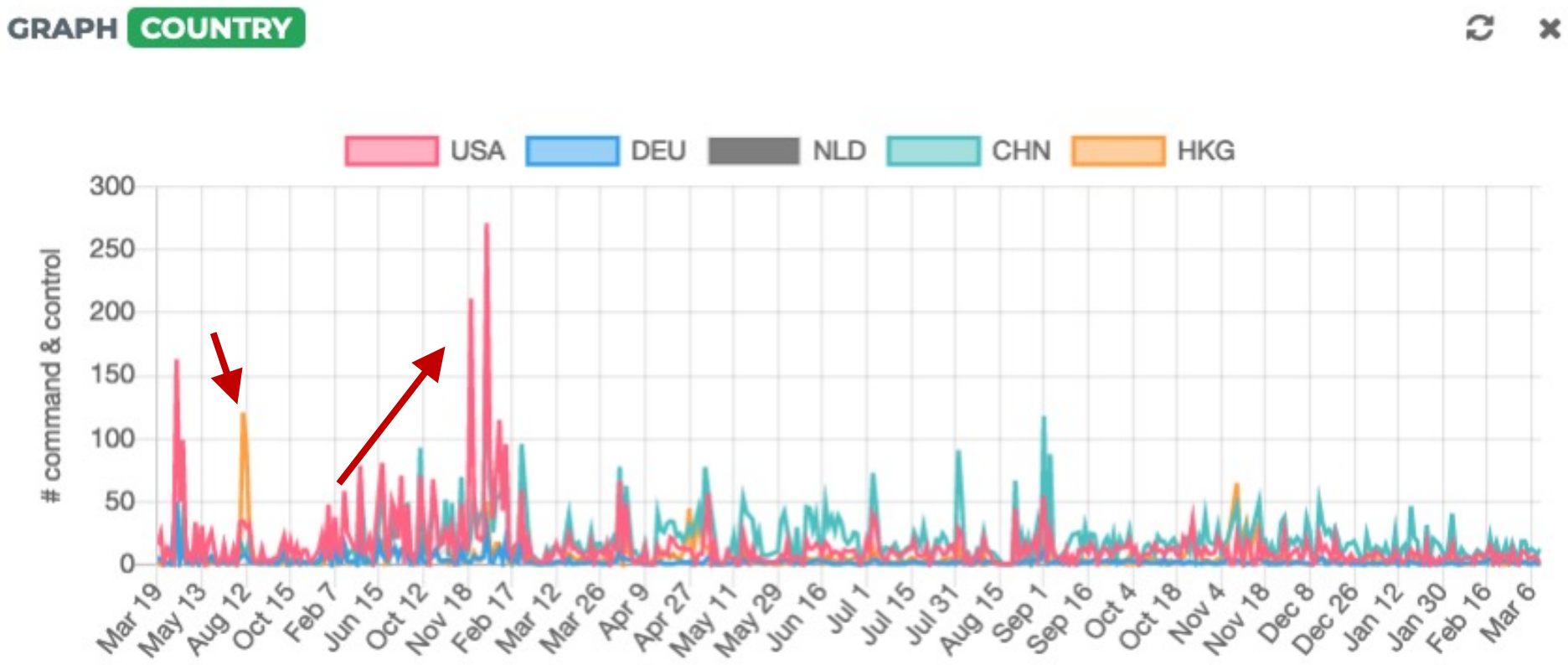
Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

C2 Server Timeline by Country – Feb 2019 to Jan 2021



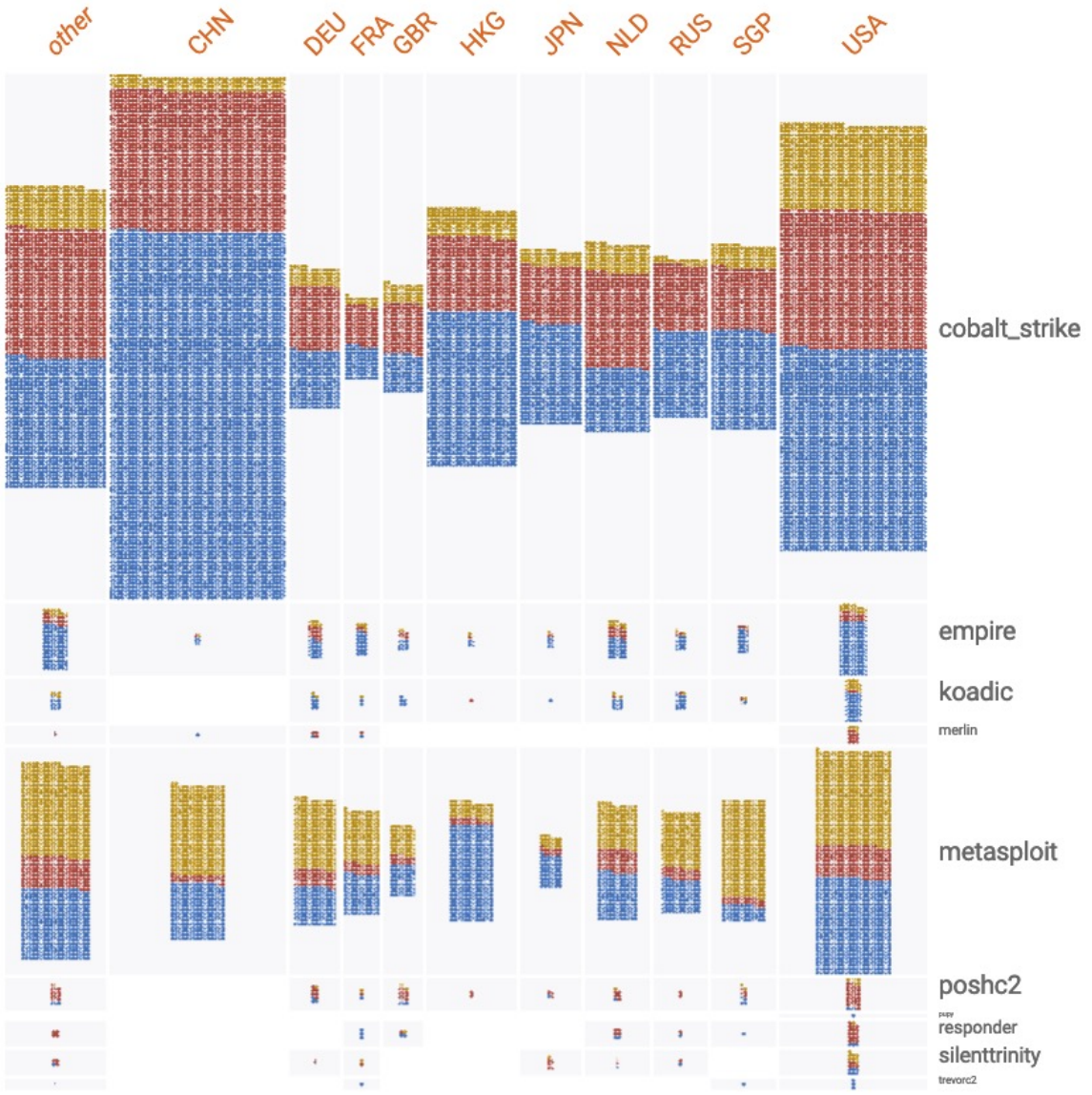
Source: Dreamlab Technologies AG, CyObs & Audit Department, 31 January 2021

C2 Server Timeline by Country – Feb 2019 to Mar 2022



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

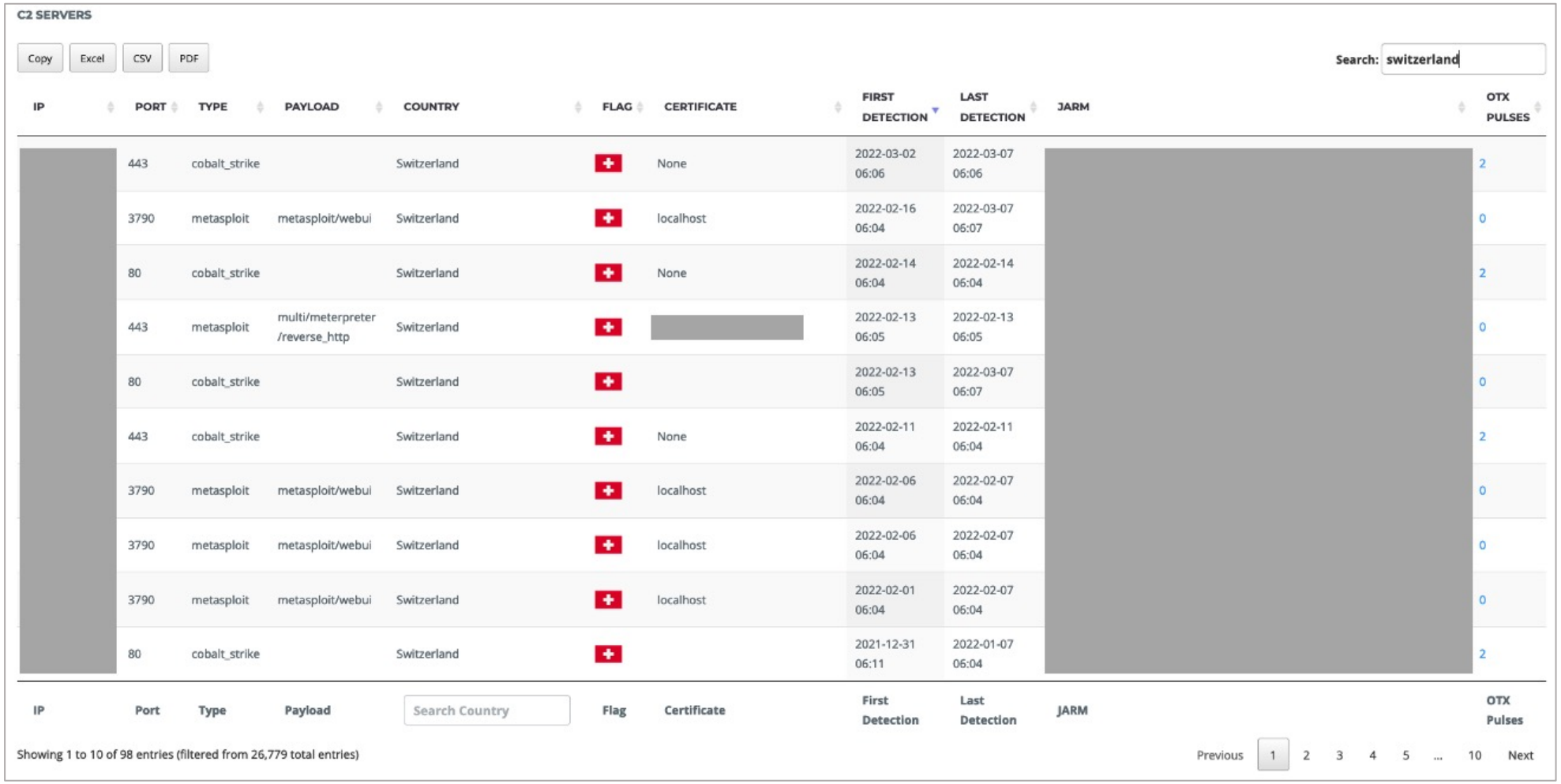
C2 Servers by Country / Malware Type View



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

C2 Servers in Switzerland

98 in 03.2022 (vs. 36 in 02.2021)



C2 SERVERS

Copy | Excel | CSV | PDF

Search: switzerland

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
	3790	metasploit	metasploit/webui	Switzerland		localhost	2022-02-16 06:04	2022-03-07 06:07		0
	80	cobalt_strike		Switzerland		None	2022-02-14 06:04	2022-02-14 06:04		2
	443	metasploit	multi/meterpreter /reverse_http	Switzerland		[redacted]	2022-02-13 06:05	2022-02-13 06:05		0
	80	cobalt_strike		Switzerland			2022-02-13 06:05	2022-03-07 06:07		0
	443	cobalt_strike		Switzerland		None	2022-02-11 06:04	2022-02-11 06:04		2
	3790	metasploit	metasploit/webui	Switzerland		localhost	2022-02-06 06:04	2022-02-07 06:04		0
	3790	metasploit	metasploit/webui	Switzerland		localhost	2022-02-06 06:04	2022-02-07 06:04		0
	3790	metasploit	metasploit/webui	Switzerland		localhost	2022-02-01 06:04	2022-02-07 06:04		0
	80	cobalt_strike		Switzerland			2021-12-31 06:11	2022-01-07 06:04		2

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

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

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

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

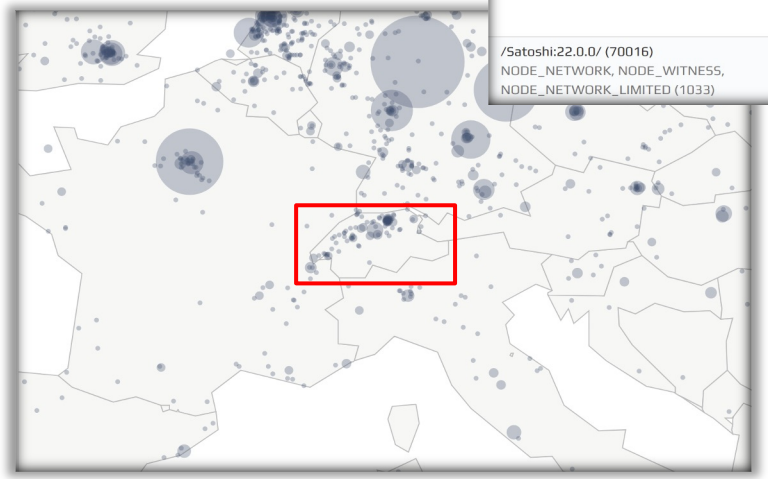
Swiss Crypto: Bitcoin and Ethereum Overview

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

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022 and https://bitnodes.io/

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:

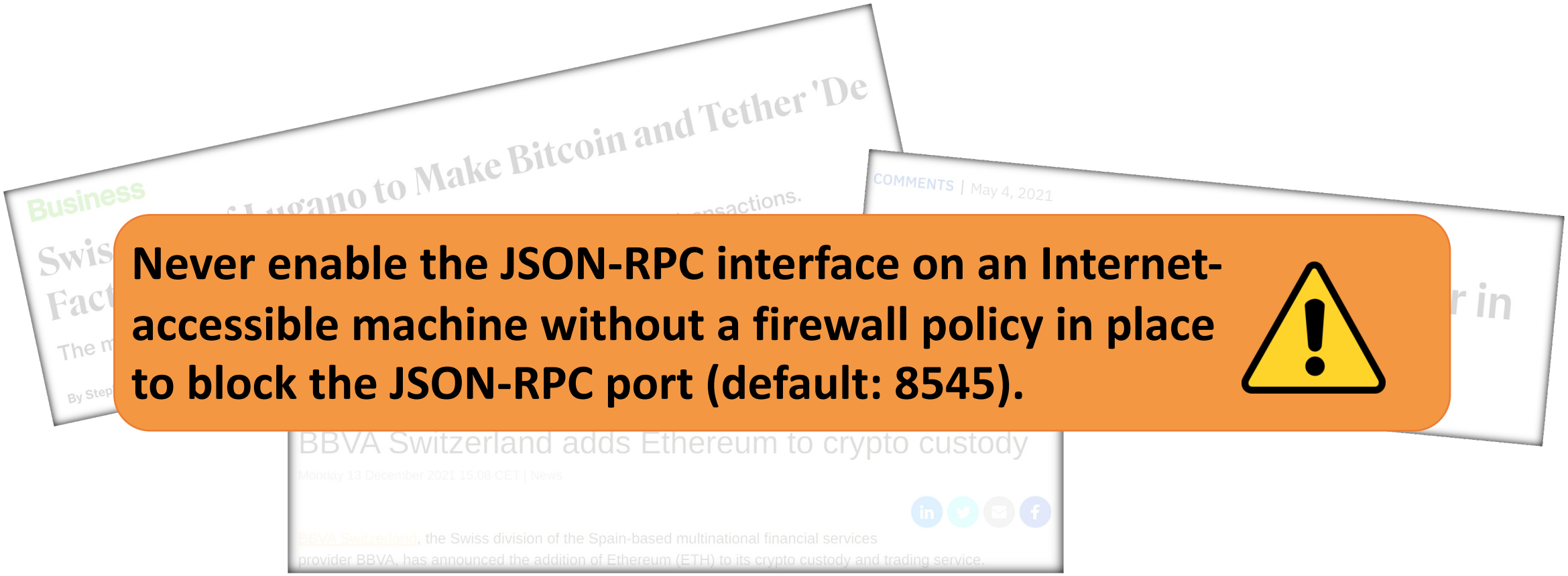
```
yl@ws17:~$ [redacted]{"jsonrpc":"2.0","method":
"eth_accounts","params":[],"id":1}' http://[redacted]:8545
{"jsonrpc":"2.0","id":1,"result":["0xbc82[redacted]"]}
```

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"}
```

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022 and https://bitnodes.io/

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).

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

Agenda

Review 2021

Swiss Public Attack Surface by CyObs

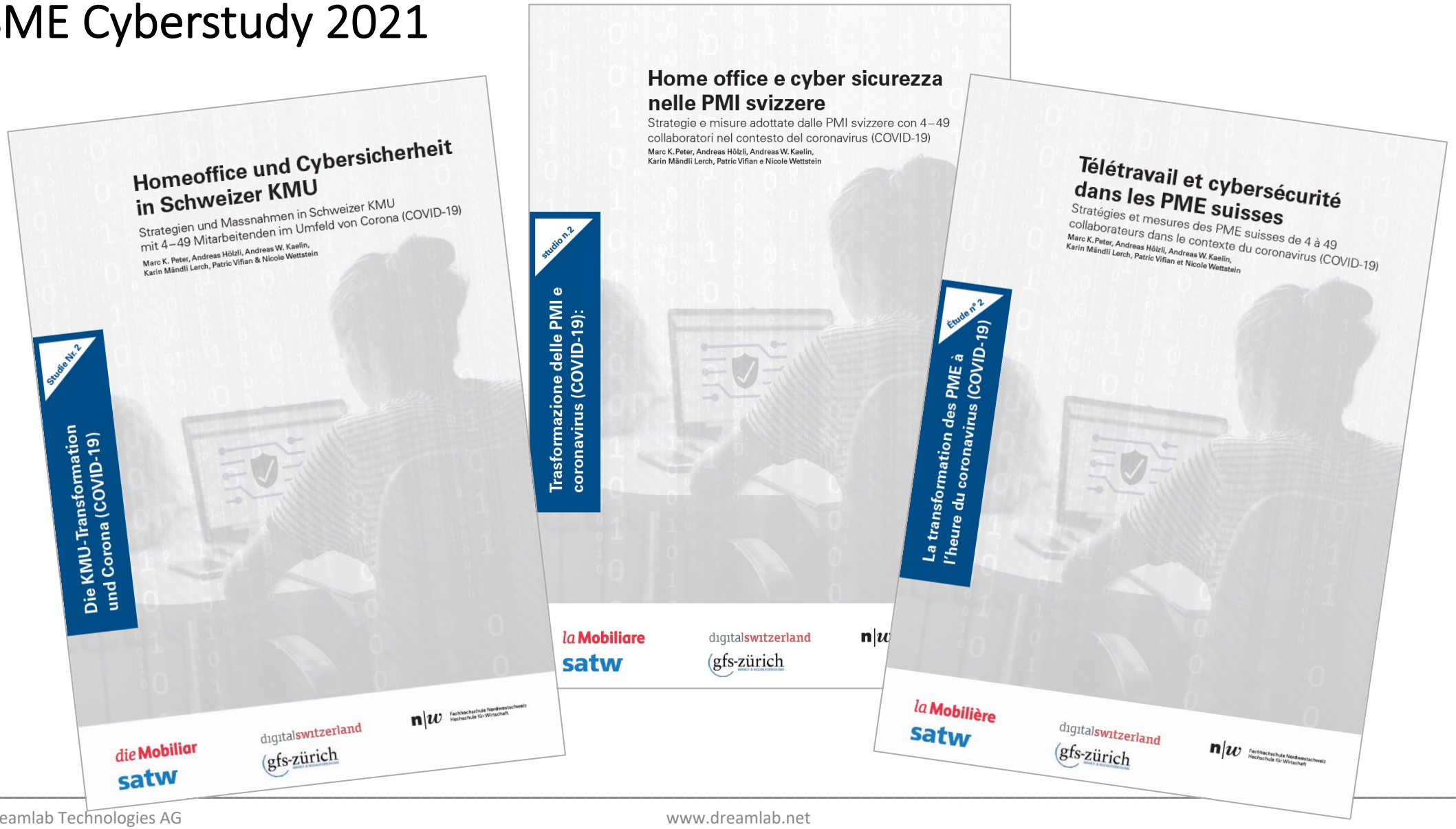
Command and Control (C2) Systems by RATspotting

Swiss Crypto Nodes

Threat Protection Motivation

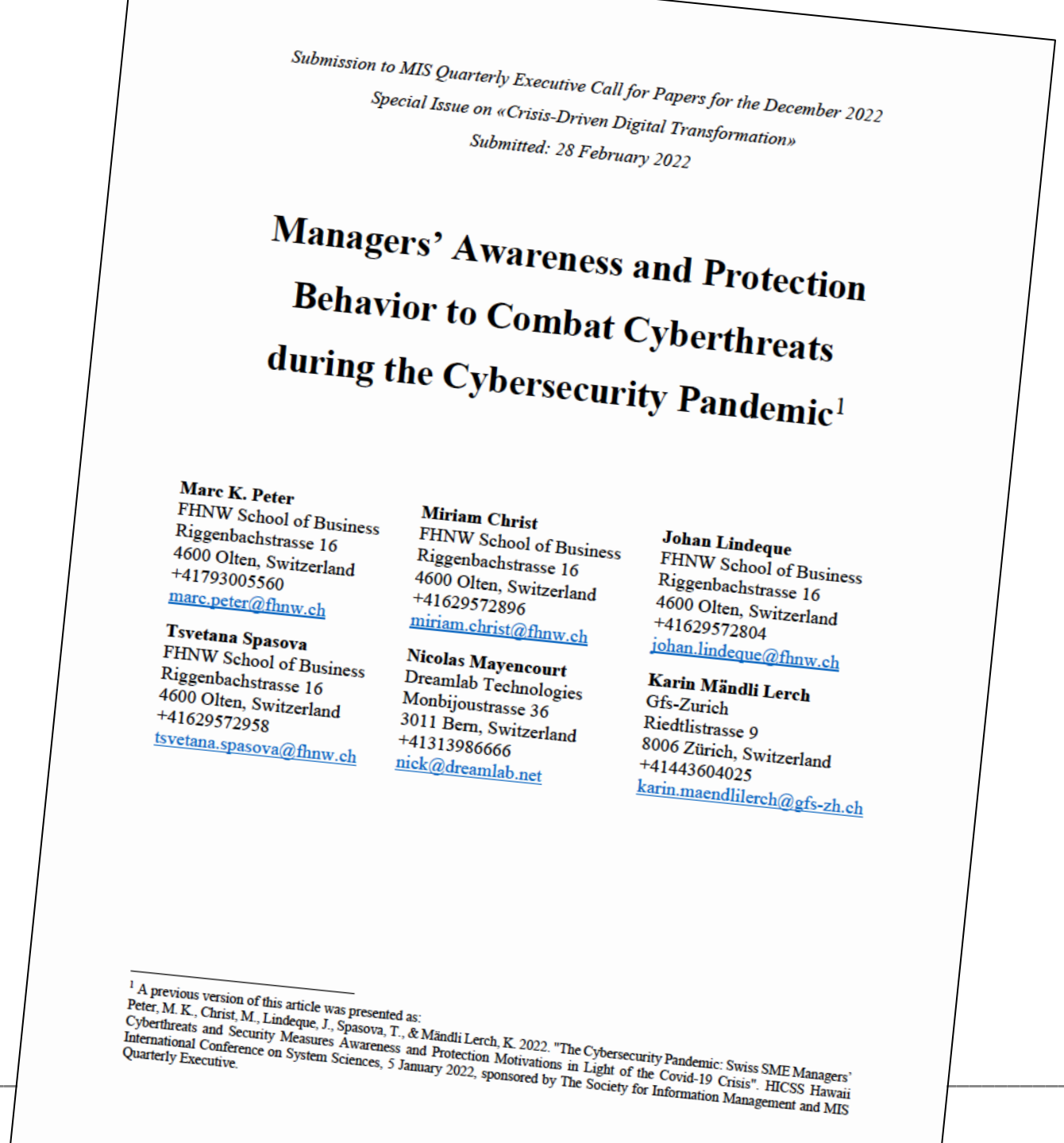
Conclusion & Cybercheck

SME Cyberstudy 2021



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[1]

Marc K. Peter
FHNW School of Business
Riggenbachstrasse 16
4600 Olten, Switzerland
+41793005560
marc.peter@fhnw.ch

Tsvetana Spasova
FHNW School of Business
Riggenbachstrasse 16
4600 Olten, Switzerland
+41629572958
tsvetana.spasova@fhnw.ch

Miriam Christ
FHNW School of Business
Riggenbachstrasse 16
4600 Olten, Switzerland
+41629572896
miriam.christ@fhnw.ch

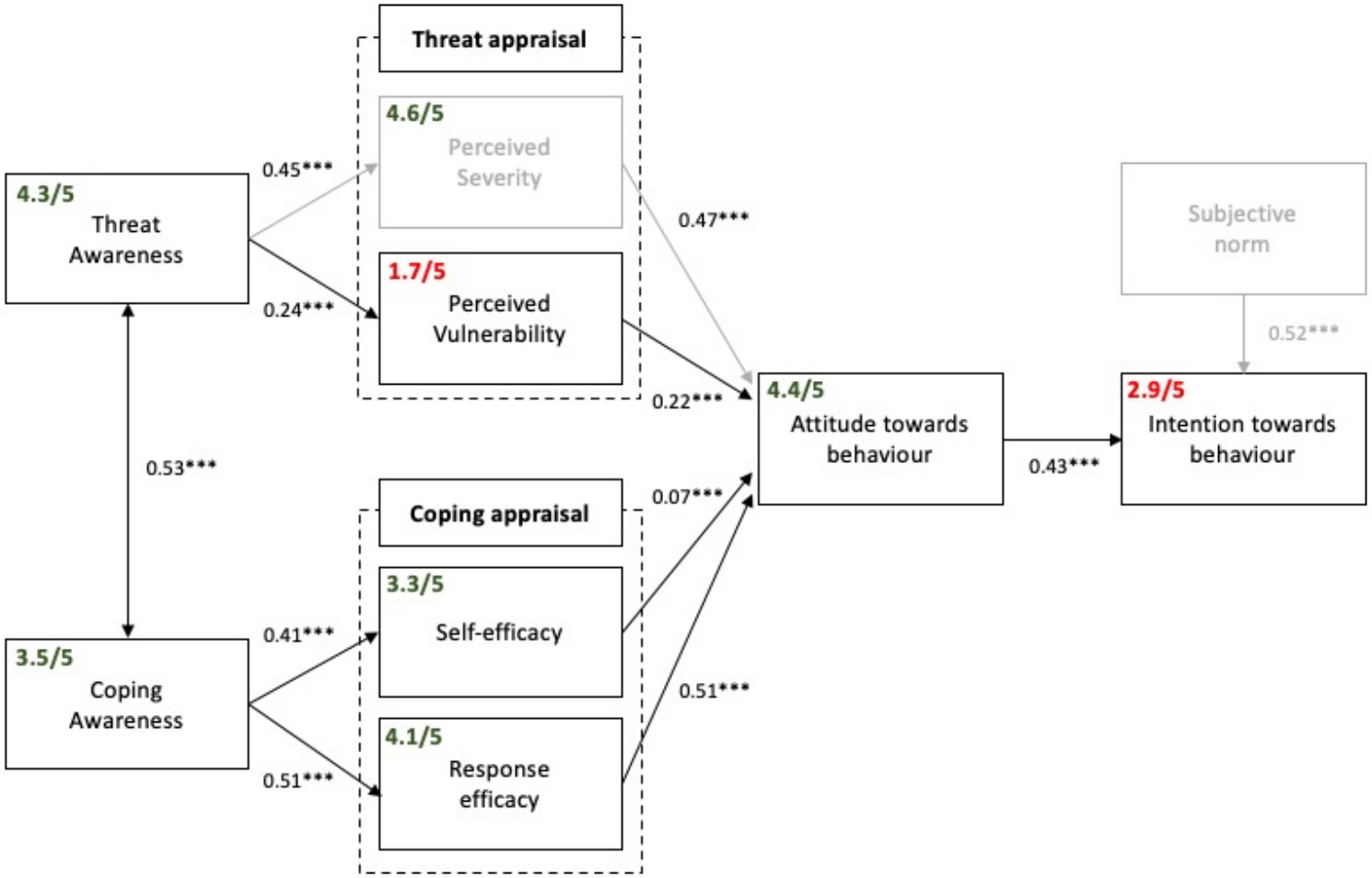
Nicolas Mayencourt
Dreamlab Technologies
Monbijoustrasse 36
3011 Bern, Switzerland
+41313986666
nick@dreamlab.net

Johan Lindeque
FHNW School of Business
Riggenbachstrasse 16
4600 Olten, Switzerland
+41629572804
johan.lindeque@fhnw.ch

Karin Mändli Lerch
Gfs-Zurich
Riedtlistrasse 9
8006 Zürich, Switzerland
+41443604025
karin.maendlilerch@gfs-zh.ch

[1] 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	
Hong Kong, China		11
France	3.66	12
Israel	3.55	
Chi		14
Irela	53.05	15
	52.70	16
Canad	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/

HOW DO WE IMPROVE?

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.	4
Singapore	98.	4
Spain	98.5	4
Russian Federation	3.0	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14

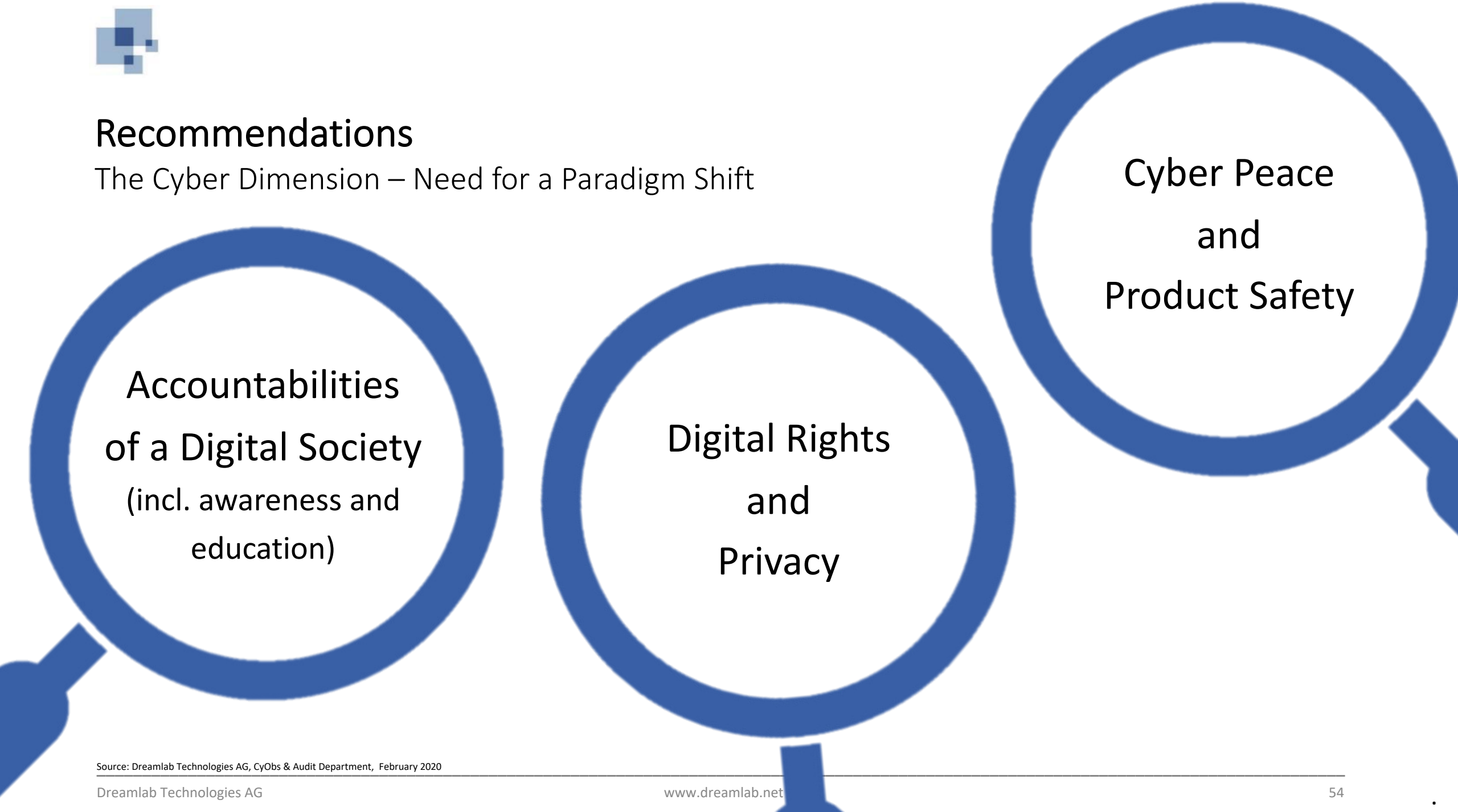
Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	9	26
Qatar	9	27
Gre e	93	28
Aus a	93.	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
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

Recommendations

The Cyber Dimension – Need for a Paradigm Shift



Source: Dreamlab Technologies AG, CyObs & Audit Department, February 2020

For Swiss SMEs (and many more)

cybercheck.dreamlab.net

Beobachter & Dreamlab Cybercheck

Beobachter

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
DREAMLAB
TECHNOLOGIES
BEING
NAÏVE

Contact

Dreamlab Offices

Get in touch with us: contact@dreamlab.net
And follow us at: twitter.com/DreamlabGlobal
linkedin.com/company/dreamlab-technologies-ag

Dreamlab Switzerland

Dreamlab Technologies
Monbijoustrasse 36
Switzerland – 3011 Bern

Dreamlab Chile

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

Dreamlab Spain

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

Dreamlab Oman

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