A Cyber Situation Report on the conventional war in Ukraine

alpha strike labs
by Limes Security

Johannes Klick

CEO | Co-Founder of Alpha Strike Labs

- Internet Scanning Expert, ICS/OT Hacker
- Aktiver Reservist: Kdo. Cyber- und Informationsraum (CIR), Hauptmann d.R.
- Gefundene Schwachstellen:
  - CVE-2015-2177, DoS of Siemens SIMATIC S7-300
  - CVE-2014-6617, Softing FG-100 PB
  - CVE-2015-6616, Softing FG-100 PB XSS
  - Security Advisory 2015/12/02 (Traeger Industry Comp. GmbH) S7 Firewall
- Veröffentlichungen auf akademischen und angewandten Security Conferences:
  - NATO CCDCOE CyCon 2021, Estonia
  - Chaos Communication Camp 2019, Germany | Blackhat 2015, USA
  - ACM IMC | ACM SIGSAC | IEEE CNS | …

Unsere Services

Identifikation aller externen IP-Adressen, Netzwerk-Topologien, Websites und Schwachstellen

Modularität

Schnelle Anpassung an neue Gegebenheiten

60+ **scanbare** Protokolle

State of the Art Technology

Datenhoheit in Deutschland

historische Daten verfügbar

Wir besitzen Daten über die letzten 2,5 Jahre

On Premise Lösungen

dezentrale Suchmaschine

270+ Mio.

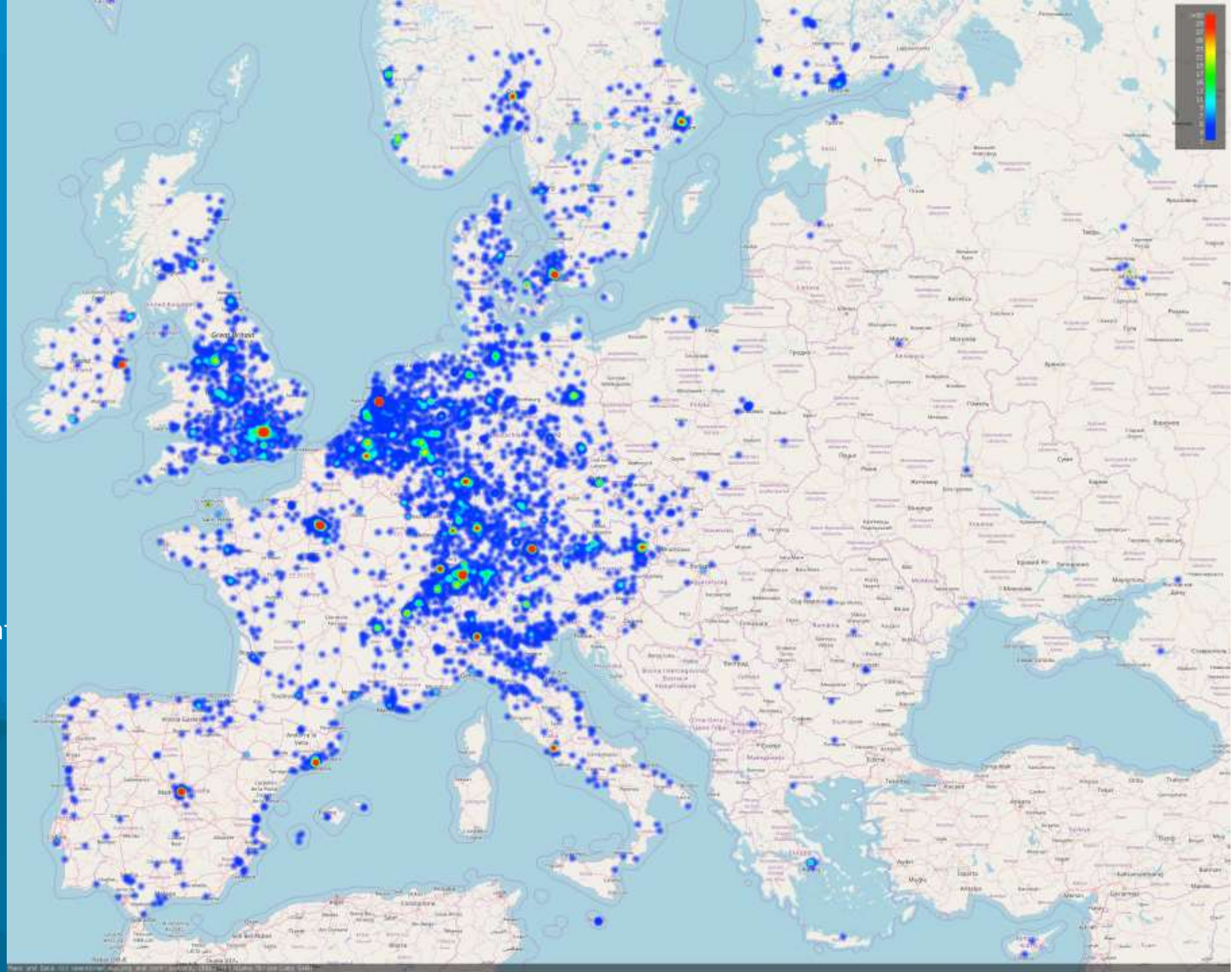
Active Services

Was ist ein Cyber Situation Report?

Verwundbare CITRIX Server

11.01.2020 Europa

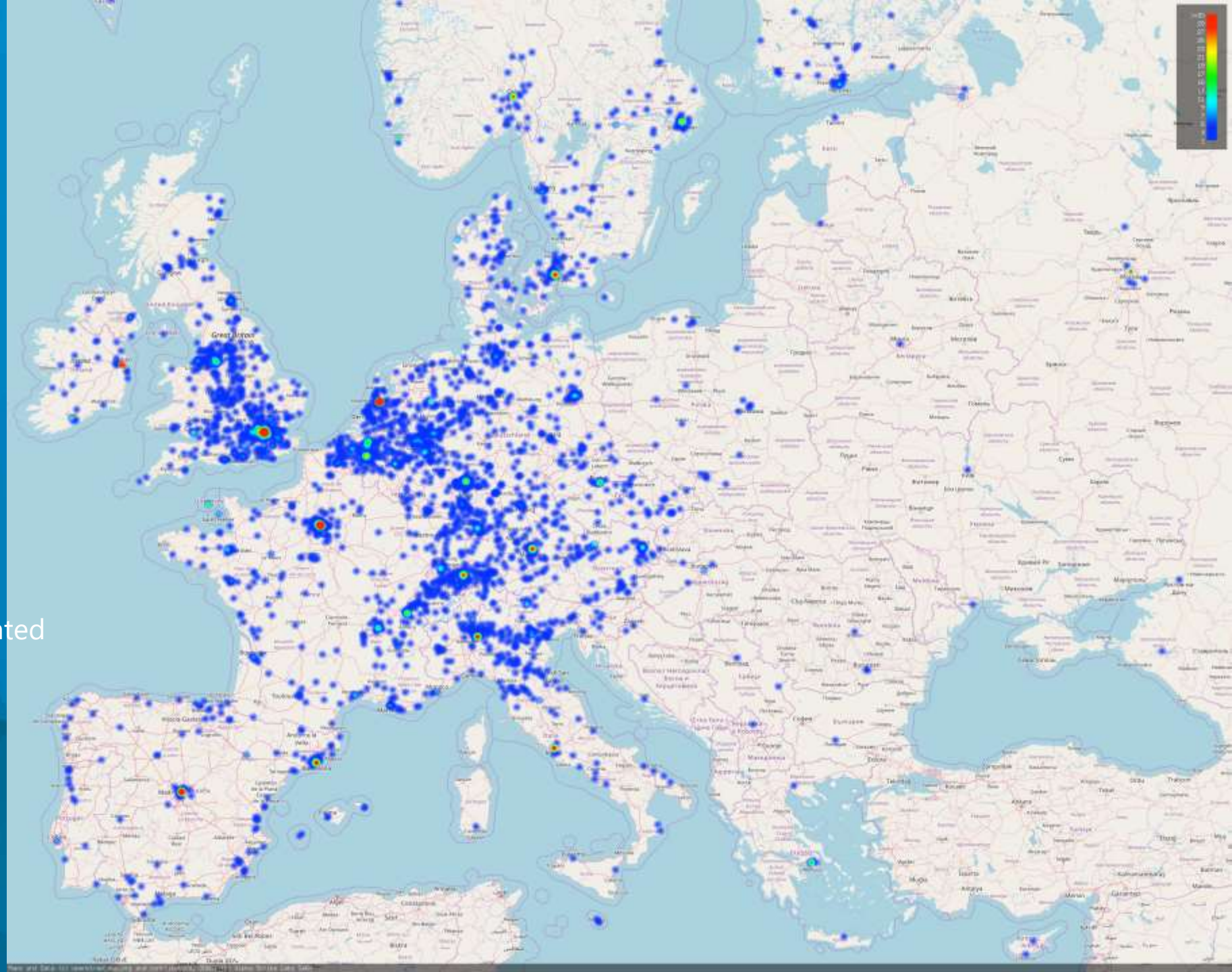
CVE-2019-19781 (unauthentica
remote code execution)



Verwundbare CITRIX Server

16.01.2020 Europa

CVE-2019-19781 (unauthenticated remote code execution)



CITRIX Cyber Situation Report

Findings

- Die Schweiz, die Niederlande und Deutschland reagierten schnell und **patchten die meisten Server**
- Das Vereinigte Königreich, Australien, Italien, die USA, Kanada und Frankreich haben gut reagiert und **mehr als 50 %** ihrer anfälligen Server **gepatcht**.
- China liegt **an letzter Stelle** und hat **nach 10 Tagen nur 24 %** seiner anfälligen Server **gepatcht**.

Country	11.01.2020	21.01.2020	Patch Rate *(after 10 days)*
Switzerland	2113	202	-0,90
Netherlands	1689	170	-0,90
Germany	5265	784	-0,85
United Kingdom	3920	1459	-0,63
Australia	2273	889	-0,61
Italy	1172	479	-0,59
United States	17341	7601	-0,56
Canada	1399	633	-0,55
France	1594	781	-0,51
China	870	660	-0,24

Ukraine Cyber Situation Report

Kombiniert mit Open Source Intelligence (OSINT)

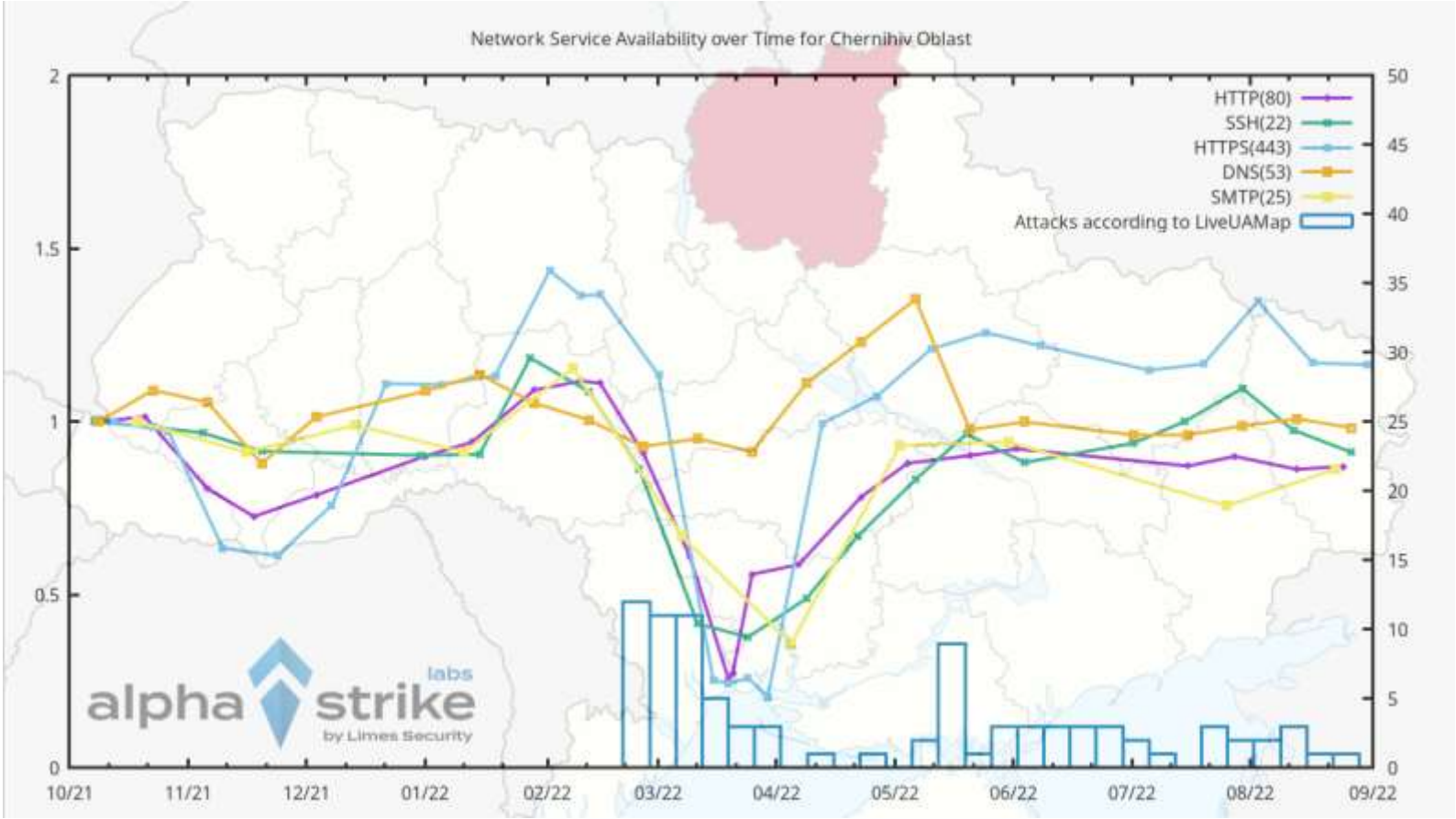
alpha strike labs
by Limes Security

Case Study: Ukraine Analyse

- Basierend auf unseren Scandaten haben wir **schwerwiegende Verluste bei der Verfügbarkeit von Netzwerkdiensten und Servern** in verschiedenen Regionen der Ukraine gemessen.
- Scandaten vom Oktober 2021 wurden ausgewählt und als Referenzwert (100 % oder 1) zum Vergleich herangezogen.
- Darüber hinaus wurden **OSINT-Informationen** z. B. aus sozialen Medien über Mörserangriffe, Artillerieangriffe und Luftangriffe von LiveUAmap (https://liveuamap.com/) extrahiert.
- Die Daten zeigen, dass schwere Angriffe, insbesondere in den ersten Wochen der russischen Invasion, zu **starken Einbußen bei der Verfügbarkeit von Netzdiensten** in der jeweiligen Region **führten**.

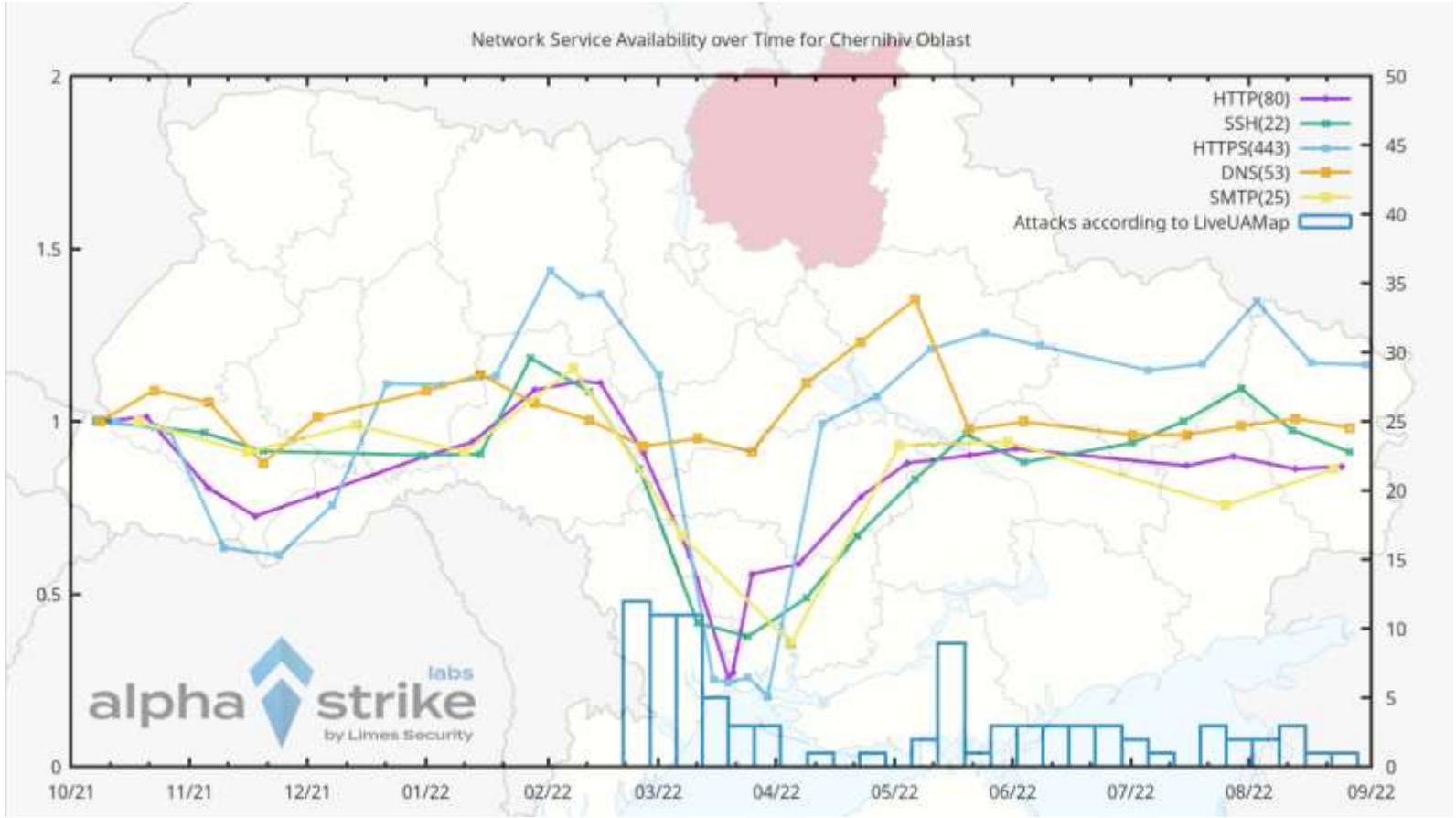
Ukraine Analyse – Oblast Chernihiv

Wahrend der vielen russischen Angriffe und der russischen Okkupation haben sich die Netzwerkdienste um mehr als 60% reduziert.



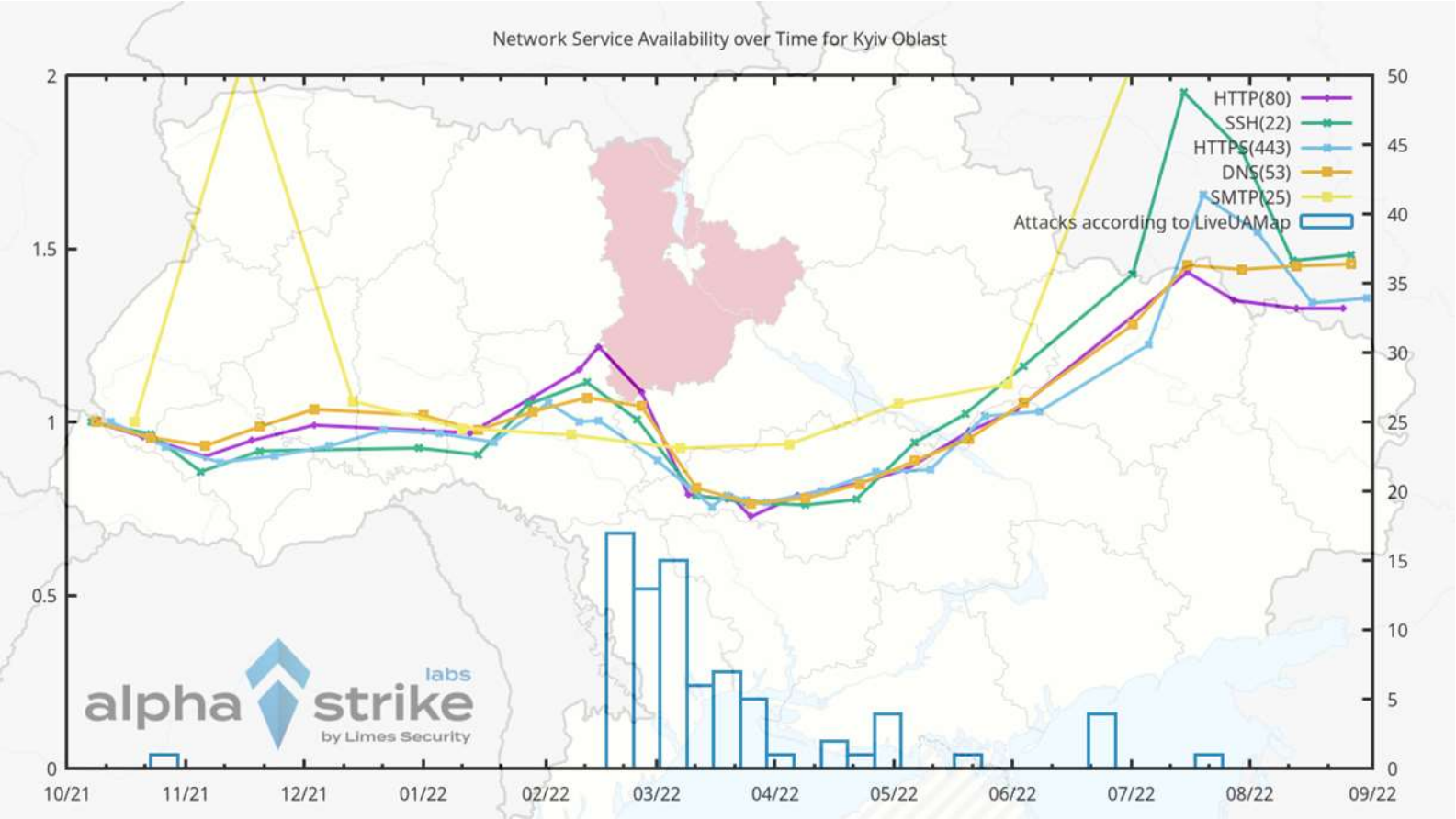
Ukraine Analyse – Oblast Chernihiv

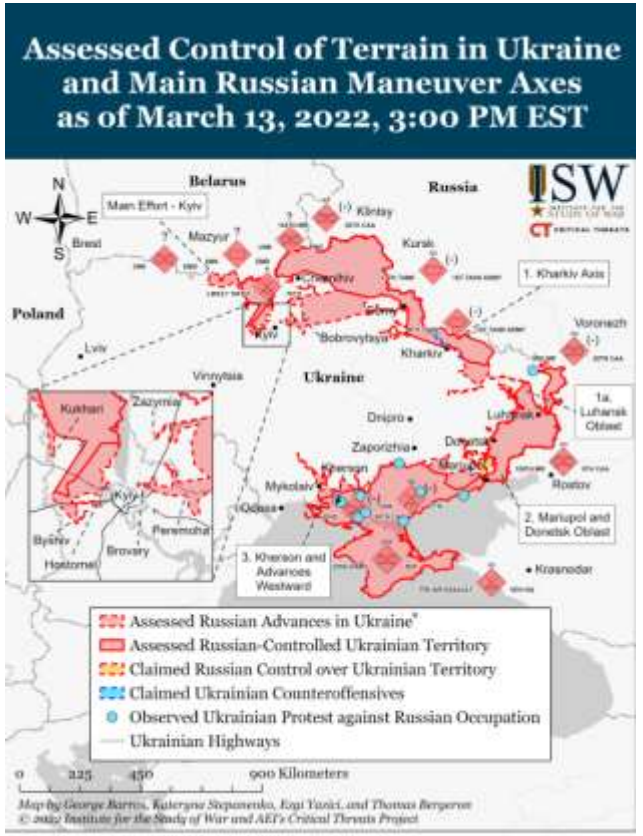
Nach dem Rückzug der russischen Kräfte Anfang April erholen sich die Netzwerkdienste wieder.



Ukraine Analyse – Oblast Kiev

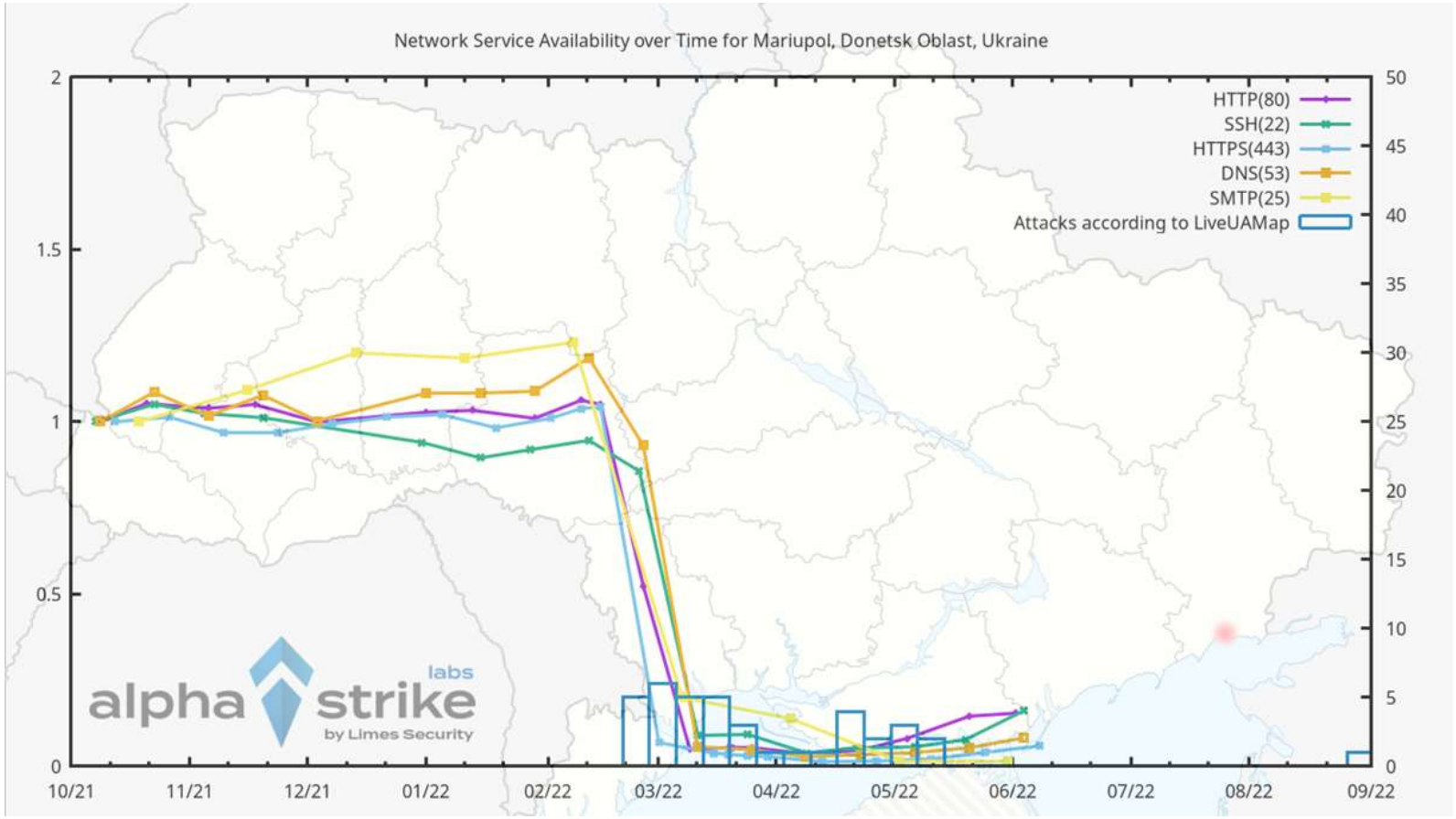
Der Oblast Kiev wurde ebenfalls beschossen, jedoch nur teilweise besetzt. Im Gegensatz zu Chernihiv betragen hier die Verfügbarkeitsverluste ca. 25%. Nach dem Rückzug der russischen Streitkräfte findet ebenfalls eine Erholung der Netzwerkdienste statt.

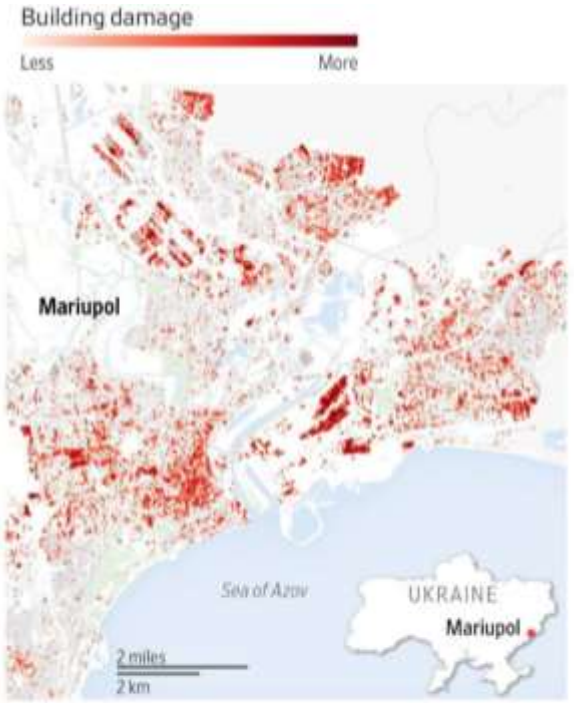




Ukraine Analyse – Mariupol

Gemäß Satellitenaufnahmen der ESA ist die Stadt Mariupol stark zerstört worden. Unsere Internet-Scans zeigen eine Reduktion der Verfügbarkeit der Netzwerkdienste um bis zu 90% und bestätigen damit die Satellitendaten.





Note: Destruction observation period from Feb. 20 to April 5.
Source: Analysis of European satellite Sentinel-1A (ESA) by Masae Analytics
Emma Brown/THE WALL STREET JOURNAL

Zusammenfassung Ukraine-Analyse

Unsere **Scan-Ergebnisse** in der Kombination mit den **OSINT-Daten**, **Satellitenbildern** und den **Truppen bzw. Bewegungsanalysen** des *Institutes for the Study of War* zeigen eine **starke Korrelation** für die verschiedenen Ereignisse.

Wir sind überzeugt, dass intensivere Internet-Scans genutzt werden können, um die Wirkung von eigenen oder fremden kinetischen Angriffen zu messen.

Des Weiteren können unsere Daten ebenfalls genutzt werden, um Berichte in sozialen Medien über flächendeckende schwere Angriffe zu verifizieren, ob dieser der Realität entsprechen oder eine gegnerische INFOOPS Kampagne darstellen.
(**Stichwort:** Fake-News-Detection)

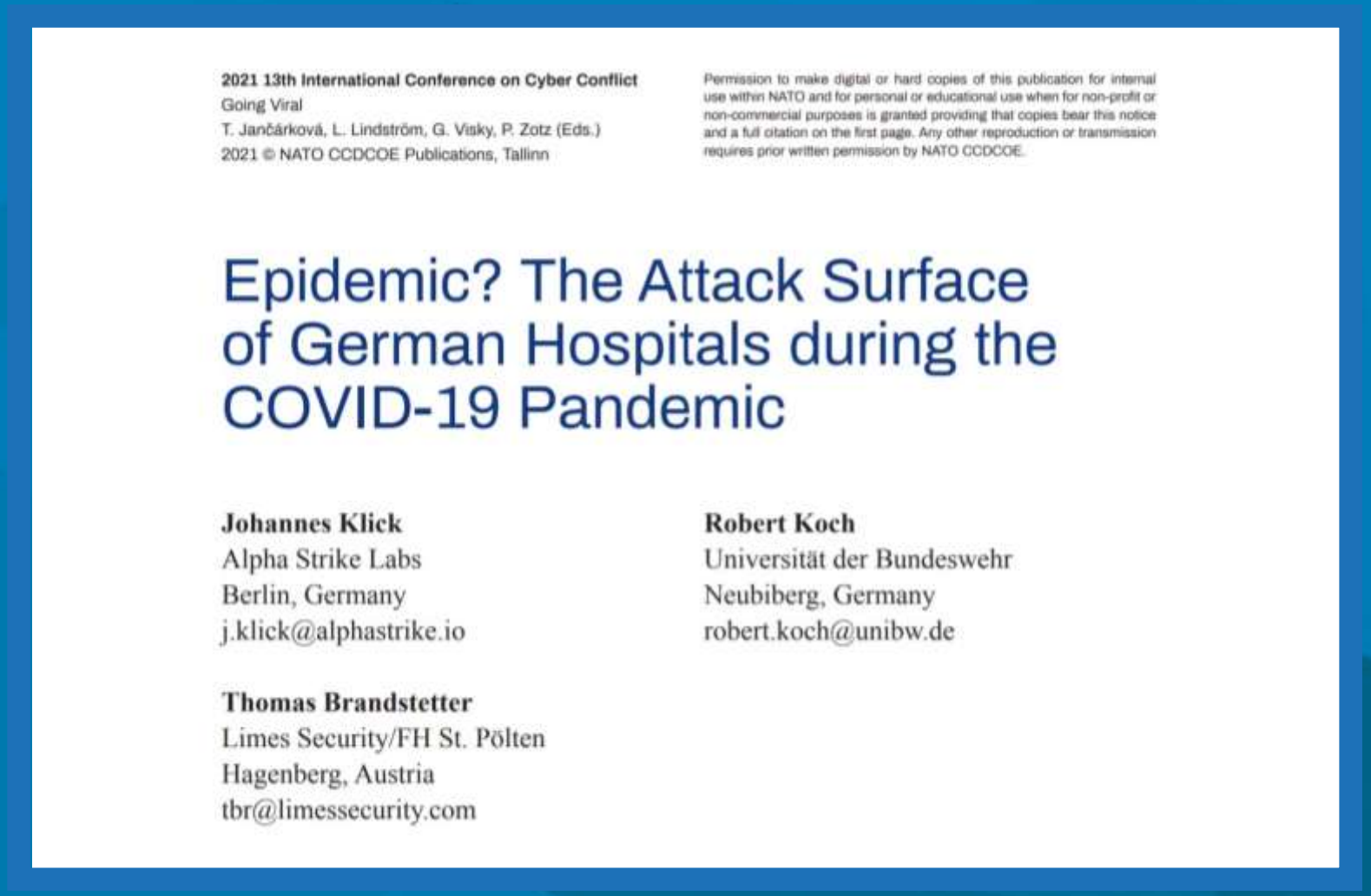
Fast Global Internet Scanning - Challenges and new Approaches

Chaos Communication Camp 2019

Link zum Video:

Epidemic? The Attack Surface of German Hospitals

NATO Conference on Cyber Conflict (CyCon) 2021



2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)

Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic

Johannes Klick
Alpha Strike Labs
Berlin, Germany
j.klick@alphastrike.io

Robert Koch
Universität der Bundeswehr
Neubiberg, Germany
robert.koch@unibw.de

Thomas Brandstetter
Limes Security/FH St. Pölten
Hagenberg, Austria
tbr@limessecurity.com

Link zum Paper:

Interesse an Cyber Intelligence und Situational Awareness im Cyberspace?

Johannes Klick

+49 176 444 30475

+49 30 120 877 420

j.klick@alphastrike.io

www.alphastrike.io