

Halyna Petrushka

The information policy of the energy company during the war

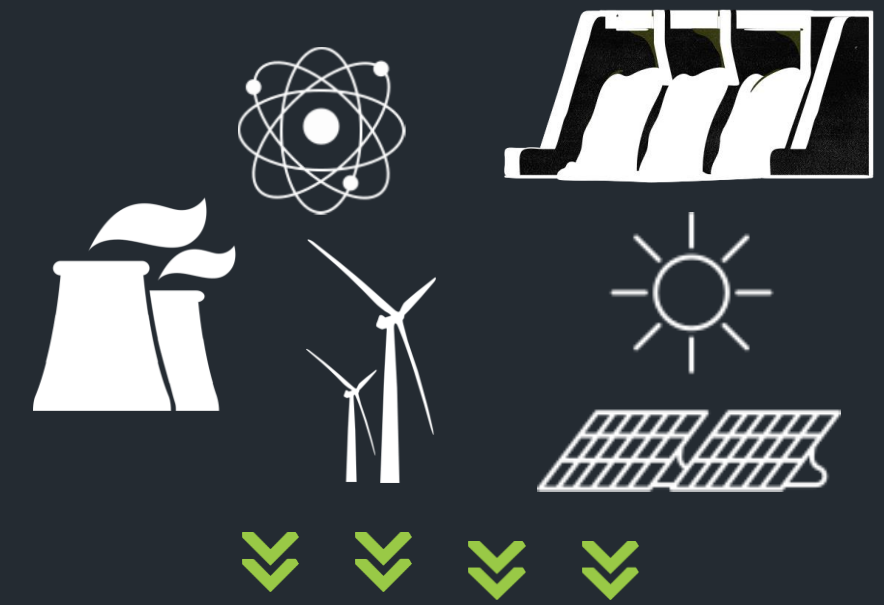
How Can Ukraine Enhance
Resilience and Protection in
Energy Production and Supply?



How does electricity get to the consumer?

Generation

Electricity production at nuclear, thermal, hydro, renewable power plants.



Transmission

Power transmission by 110-750 kW main networks from power plants to distribution system connection points.



Distribution

Delivery of electricity from backbone networks to consumers. Electricity goes through several stages of voltage reduction from 110 to 0.4 kV.



Poland

Russia

Lviv region



«Lvivoblenergo» 2023

The company provides services for the distribution of electric energy in the territory of the Lviv region. The number of clients of the company is more than 1 million.

Area of electric power supply	thousand of sq. km	21.8
Regional population	thousand of persons	2 476.1
Length of power lines	km	40 619.5
Household consumers	units/persons	978 405
Juridical persons consumers	units/persons	35 875
Number of employees	persons	3 982



Photos of railway station in Ukraine, 2022

SU "LvivenergoCommunication"

```
graph TD; A[SU "LvivenergoCommunication"] --> B[Call center]; A --> C[Corporate Relations Department]; A --> D[Museum of the History of Electrification]; A --> E[Printing house];
```

Call center

Corporate Relations Department

Museum of the History of
Electrification

Printing house



Photos of damaged energy infrastructure after enemy attacks

In November 2022, as a result of another missile strike by Russians on energy facilities, 1.5 million consumers were left without electricity. Lviv survived the blackout. Employees of Lvivoblenergo and NPC Ukrenergo managed to restore electricity supply in less than half a day.





Employees of Lvivoblenergo

Russian attacks in autumn – winter 2022-2023





Transformers

Outage schedule in Lviv region



Львівобленерго

Опубліковано Anastasia Kishun · 5 грудня 2022 р. ·

Графік відключень електроенергії залишається діючим. Додатково для Вашої зручності ми розділили графік по кожній групі окремо. Дізнатися, до якої групи належить Ваш будинок, можна на сайті «Львівобленерго» у розділі «Чому немає світла»: <https://poweroff.loe.lviv.ua/>

I група								II група								III група								
⌚	ПН	ВТ	СР	ЧТ	ПТ	СБ	НД	⌚	ПН	ВТ	СР	ЧТ	ПТ	СБ	НД	⌚	ПН	ВТ	СР	ЧТ	ПТ	СБ	НД	
1:00-5:00	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	1:00-5:00	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	1:00-5:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії
5:00-9:00	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	5:00-9:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	5:00-9:00	Немає енергії	Є світло	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Немає енергії
9:00-13:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	9:00-13:00	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	9:00-13:00	Є світло	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Немає енергії	Є енергія
13:00-17:00	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	13:00-17:00	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	13:00-17:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії
17:00-21:00	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	17:00-21:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	17:00-21:00	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Немає енергії
21:00-1:00	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	21:00-1:00	Немає енергії	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	21:00-1:00	Є енергія	Немає енергії	Немає енергії	Є енергія	Немає енергії	Немає енергії	Немає енергії	Є енергія



Russian attacks in spring – summer 2024



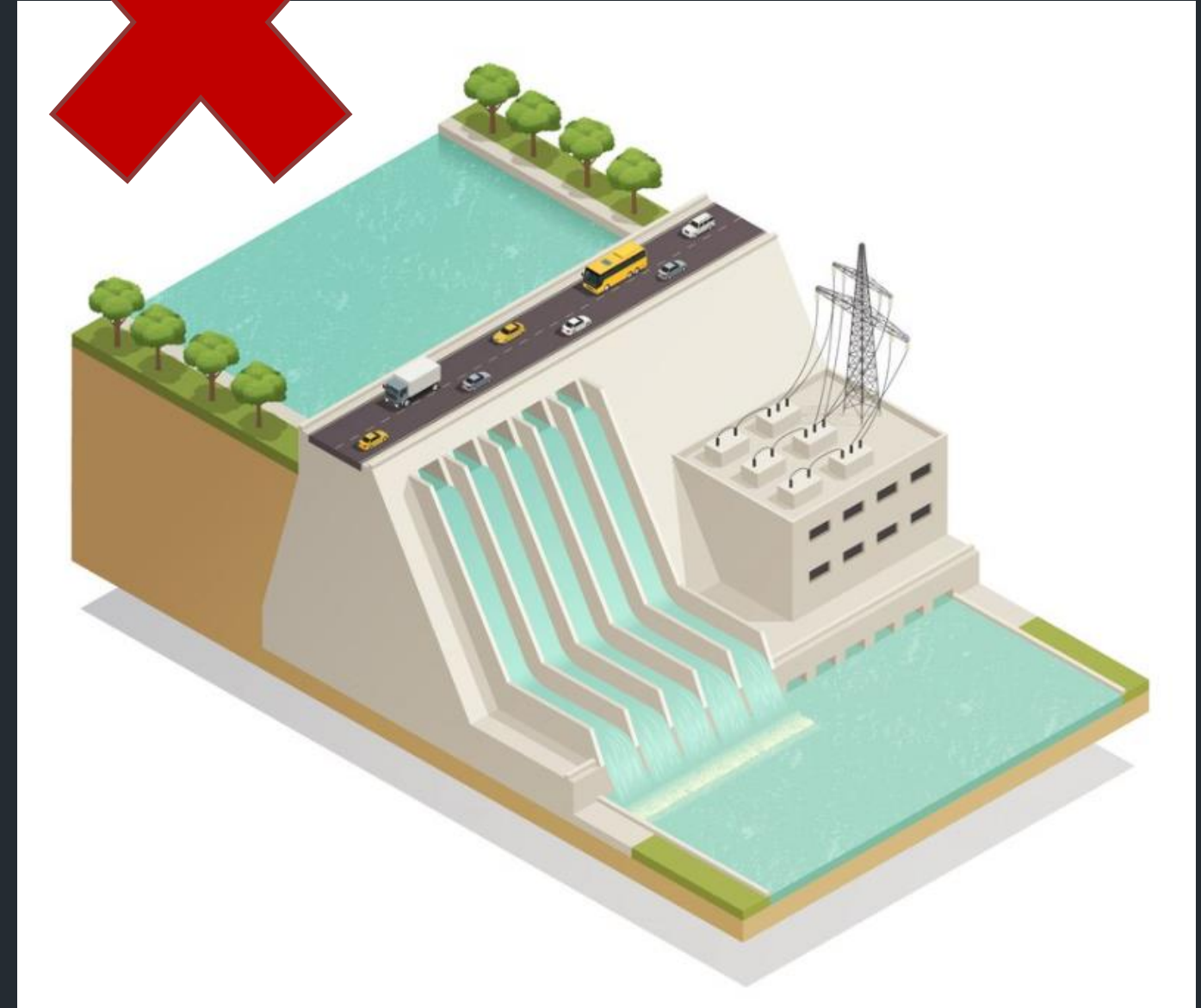
Nuclear power stations



Other power stations



Thermal

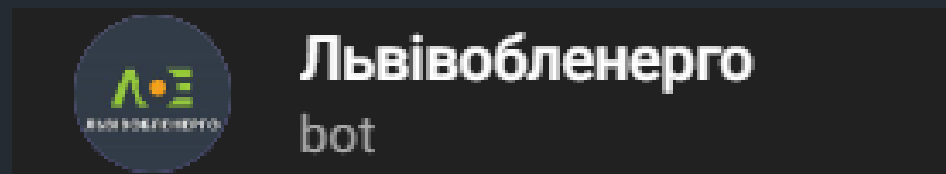
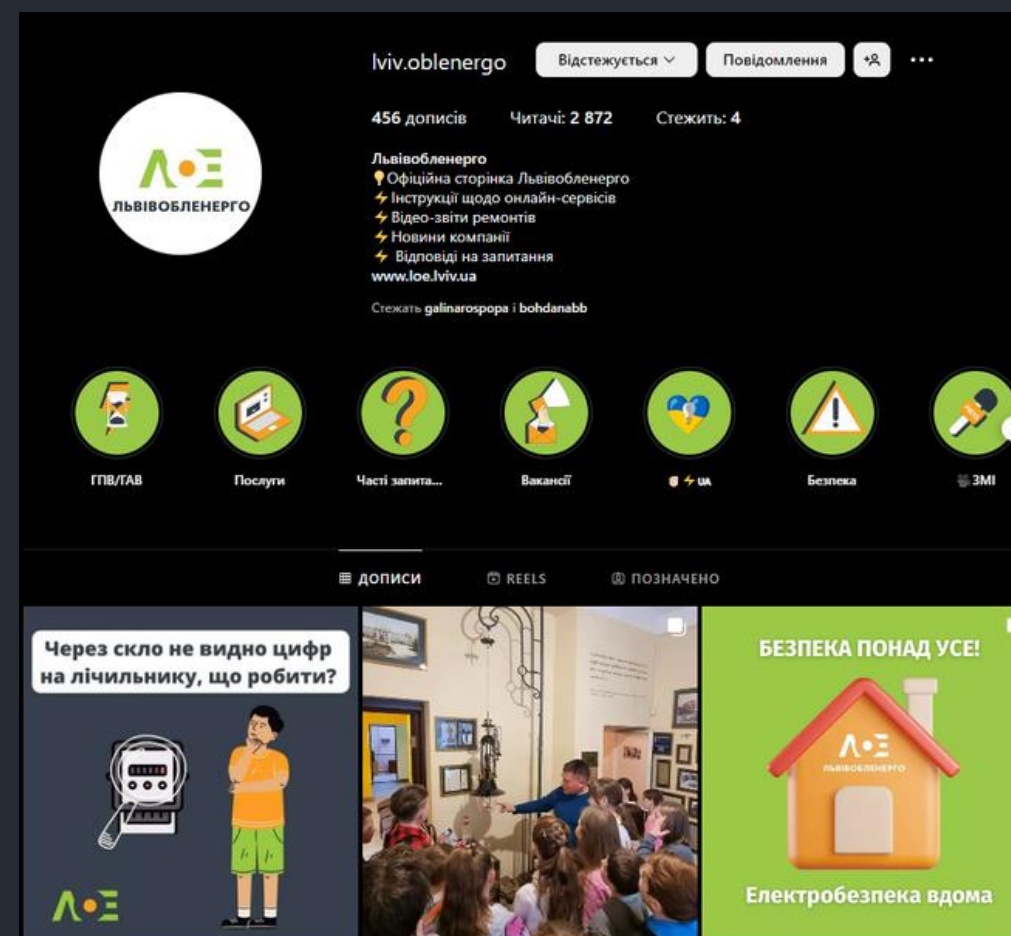
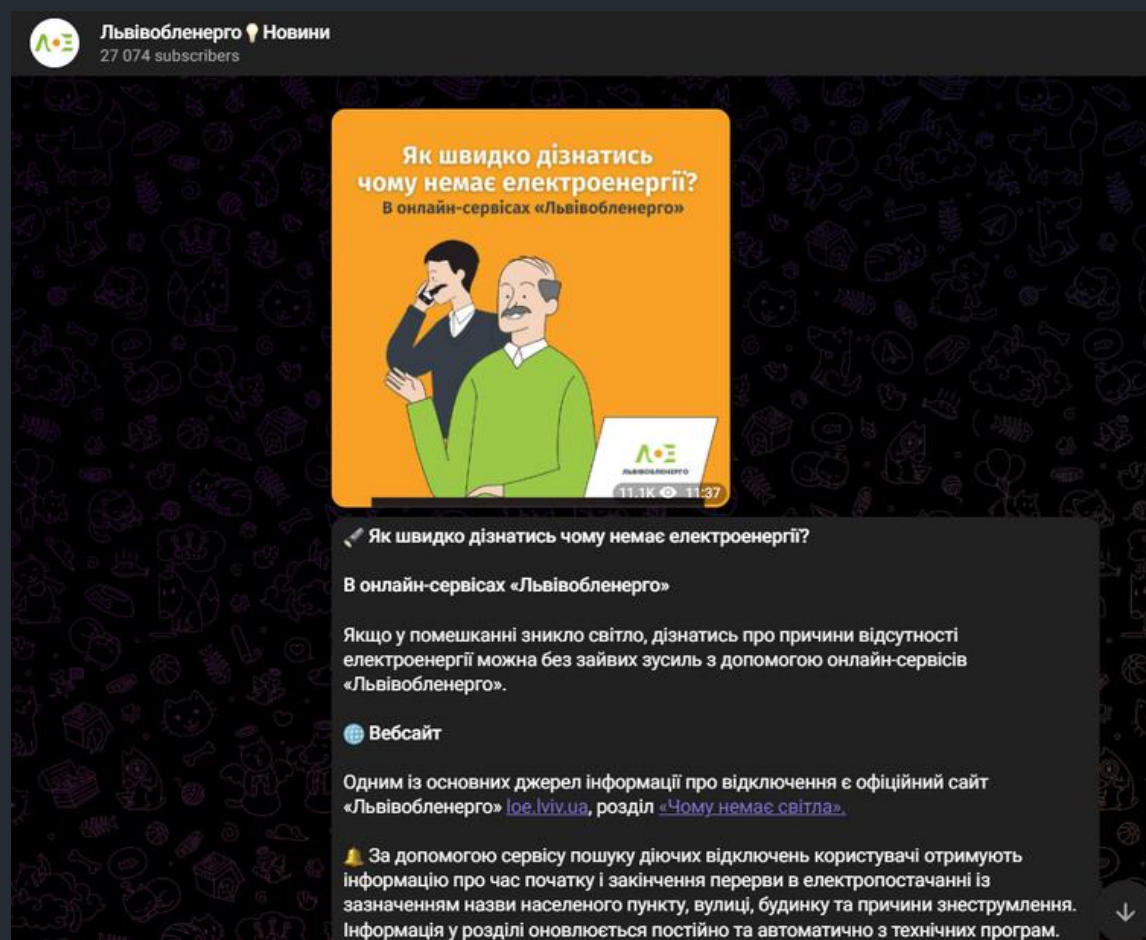
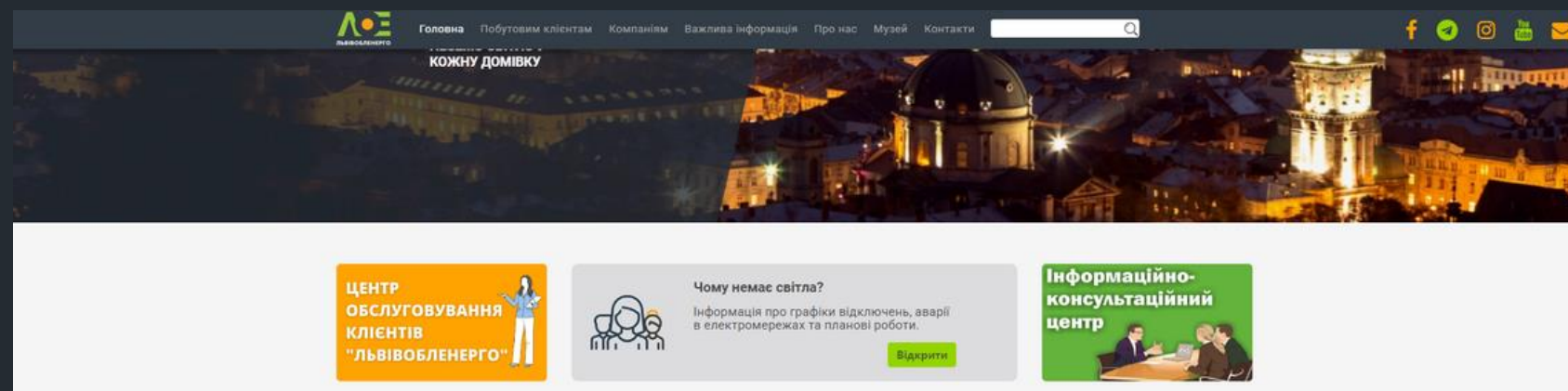


Hydro

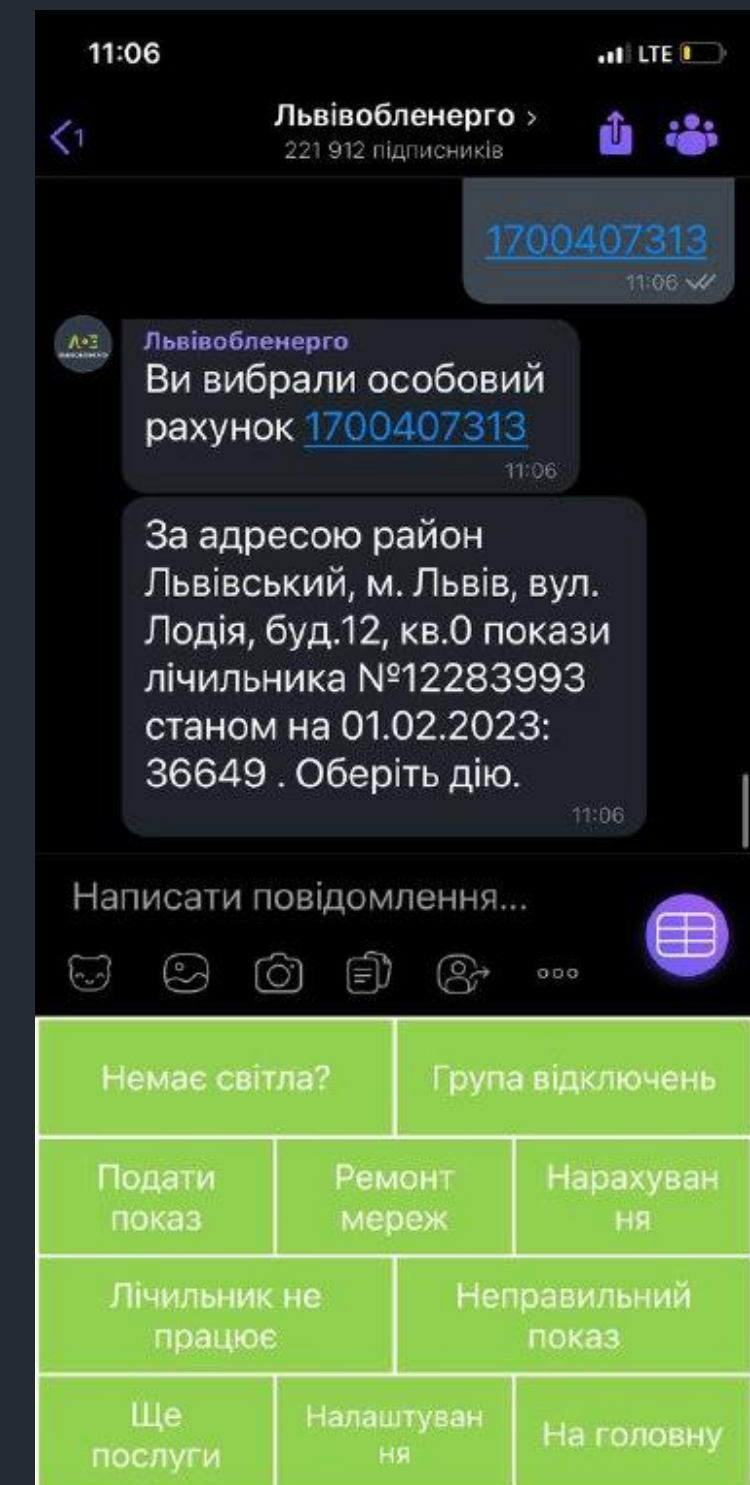
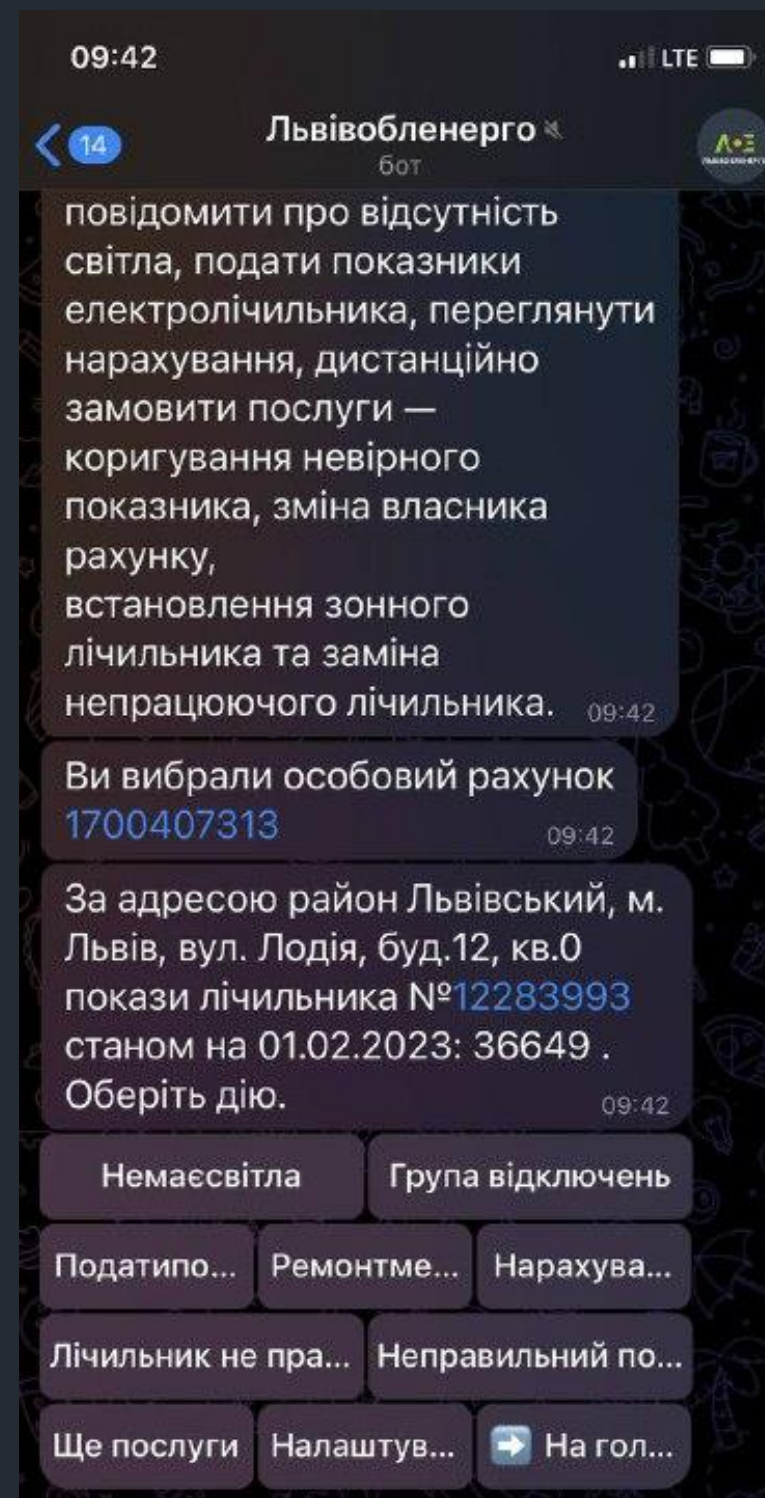
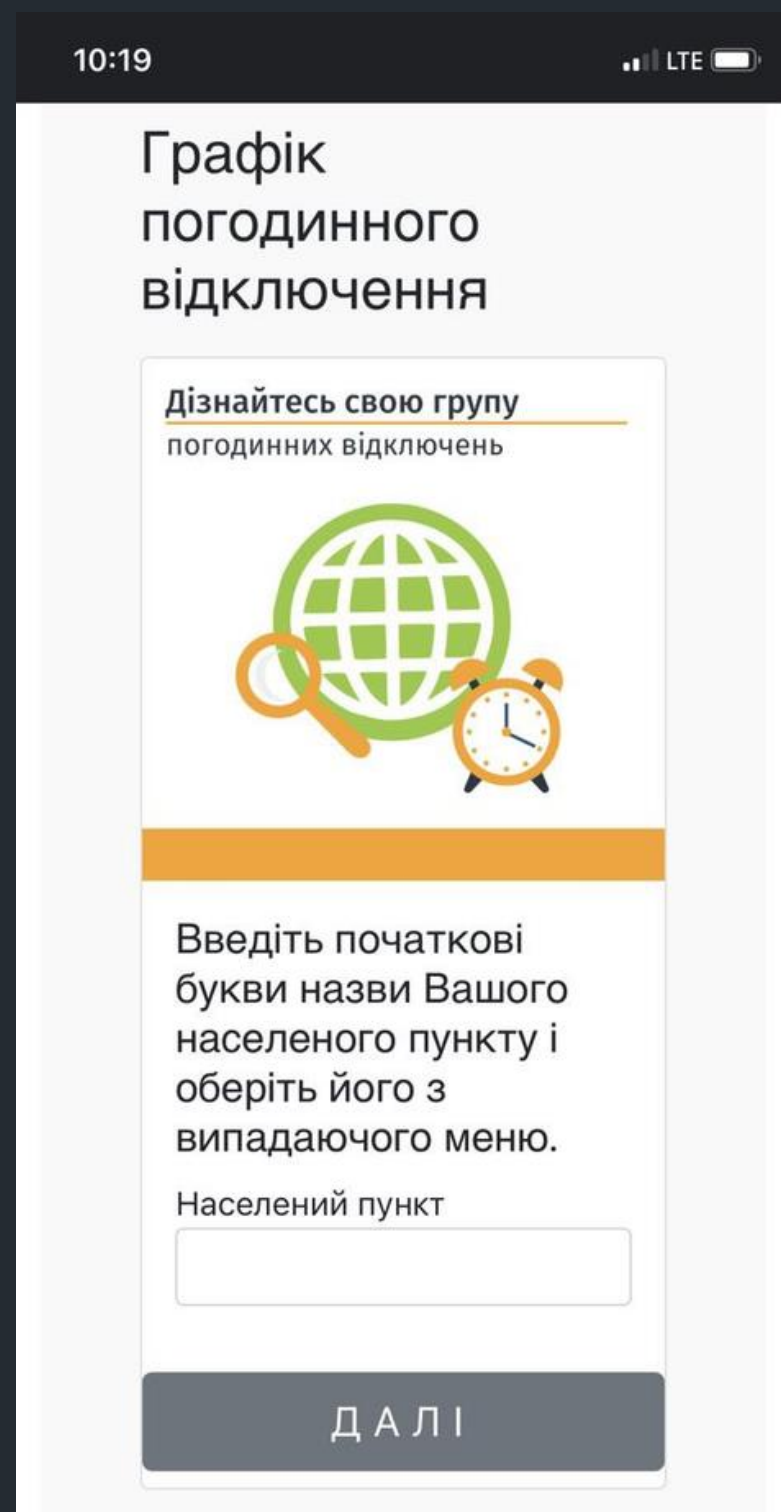


Attacks

Communication channels



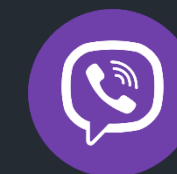
Lvivoblenergo online services



Official site: 1.2 million users per year



Telegram: 366 thousand users



Viber: 321 thousand users

Lviv 2024



In addition, people were not informed about how these schedules work and what they are needed for



Fake comments about selling electricity to Europe



Mort Mort

Нас матимуть за бидло аж поки Народ не зрозуміє , що з 26 твт, які необхідні для цивільного сектору, Рівненська АЕС виробляє 24 твт в рік. І вона одна знайслабших в Україні атомних І що в нас Сонячна генерація навіть узимку забезпечує 1.7 - 3.2 атомних реактори типу ВВЕР на 1 гвт коден. А влітку потужність Сонячної енергетики наближається до 1.7 потужностей найпотужнішої в Україні і в Європі запорізької АЕС.



Топовий прихильник

Anna Oleksandrivna Zubova

Наша економія-Міцність енергосистеми Німеччини і збагачення наших чиновників і влади



Уляна Дьорка

Люди добрі,та нема ніякого дифіциту ,просто два дяді не можуть домовитись,а страждає простий люд



Степан Качинський

потрібно контракти свої припинити за кордон,і людям хватить!!

Fake: selling electricity to Europe

**В Україні АЕС потужність
9 гВт виробляють в місяць
6 480 000 000 кВт*ч**

**1 квартира споживає за місяць
210 кВт*ч**



**АЕС можуть забезпечити
31 млн.квартир або
100 млн.громадян**

**25 млн.живе в Україні, а де
інші 100 млн???**

Fake: selling electricity to Europe



№ 07/520 від 10.06 2024 р.

на № _____ від _____ 202_ р.

НАЦІОНАЛЬНА
АТОМНА
ЕНЕРГОГЕНЕРУЮЧА
КОМПАНІЯ

Україна, 01032, Київ, вул. Назарівська, 3
Тел. +38(044)201-09-88, факс: 277-78-83

Рахунок 26009200019275
в АТ «Укресімбанк» м. Київ.
Код банку: 322313, код ЗКПО 24584661

Міністру клімату та навколишнього
середовища Польщі
Пауліне Хенніг-Клоске

Шановна пані Пауліна!

Цім листом НАЕК «Енергоатом» підтверджує свою готовність з 30 червня 2024 року приступити до виконання довгострокового контракту з поставок електроенергії у Польщу з енергоблоків №1 і №2 Хмельницької АЕС.

Запевнюємо Вас, що після аналізу проведених заходів щодо продовження терміну експлуатації енергоблоку №1 Хмельницької АЕС Державною інспекцією ядерного регулювання України був складений висновок про відсутність потреби в проведенні повного планово-попереджувального ремонту енергоблоку. Здійснення підготовчих робіт з 10 квітня по 28 травня 2024 року було визнано достатнім для подальшого функціонування реактору у понад проектний термін. Таким чином на момент початку поставок електроенергії ми гарантуємо безпечне та стабільне функціонування двох енергоблоків Хмельницької АЕС.

Також ми вважаємо важливим розвіяти сумніви Ваших колег щодо здатності Хмельницької АЕС виробляти електроенергію в повному об'ємі для поставок у Польщу. Для безперебійного забезпечення електроенергією польських споживачів Міністерством енергетики та вугільної промисловості України було прийнято остаточне рішення відімкнути два енергоблоки Хмельницької АЕС буде повністю переорієнтовано на експорт електроенергії.

З повагою,

Президент
ДП «НАЕК «Енергоатом»

Петро КОТІН

MAPA KSE

Mapa prezentuje planowe i chwilowe przepływy mocy na przekrojach handlowych

ZAPOTRZEBOWANIE [MW]	20 075
GENERACJA [MW]	21 247
el. ciepne	9 483
el. wodne	118
el. wiatrowe	1 788
el. fotowoltaiczne	9 857
el. inne odnawialne	0
SALDO WYMIANY CAŁKOWITEJ [MW]	1 172 EKSPORT
CZĘSTOTLIWOŚĆ [Hz]	49,990



09-08-2024 13:40:45

WIĘCEJ O PRACY KSE

Facebook posts about fakes

ОБЕРЖНО! ФЕЙКИ!

Де роздають повістки? Львів | Львівська область

Львівчани | Новини

Нагадаємо, сьогодні відбувається засідання "Радиштами".

Слово і Діло

Львівчани | Паласателі

249 ❤️ 64

19.01.2022

Від сьогодні по Україні діють нові правила відключень на період воєнного стану!

Електроенергія може не бути по 6 годин!

Щоб переглянути оновлені графіки на найближчі дні оберіть район проживання:

- Шаргородський
- Львівський
- Залозецький
- Фьолківський
- Смілянський
- Калишівський

Графіки по районах Львівської області:

- Дрогобицький
- Львівський
- Золочівський
- Новооворосийський
- Новомиргородський
- Смілянський

Львівобленерго

НЕ КОРИСТУЙТЕСЬ ІНФОРМАЦІЄЮ ПРО ВІДКЛЮЧЕННЯ З НЕПЕРЕВІРЕНИХ ДЖЕРЕЛ

Львівобленерго

ОБЕРЕЖНО! РЕСУРСИ З НЕПЕРЕВІРЕНОЮ ІНФОРМАЦІЄЮ ПРО ВІДКЛЮЧЕННЯ!

Є світло? Львів та ок

2243 учасники, 874 в мережі

Прикріплене повідомлення

У середу (25 січня) НЕК «Укренерго» вст...

Везучі Нам включали 11-13 і во 16-...
Сьогодні трошки більше, ніж іншим...

16:37

Марія

Катерина

Везучі Нам включали 11-13 і во 16-...
яка група?

16:37

вікусік

Можете будь ласка сказати коли будуть ще виключати світло з групи

16:38

Елена Руденко

Марія

яка група?

1 група

16:39

ЮЮ

Демнянська 26 належить до 1 групи ..в них світло виключили тільки на 2 год ...то як так ((((((

16:39

Відключення світла Львів

бот

Що вміє цей бот?

Даний бот створений для оповіщення користувачів "Львівобленерго" про відключення світла згідно нових графіків. Бот не є офіційним!

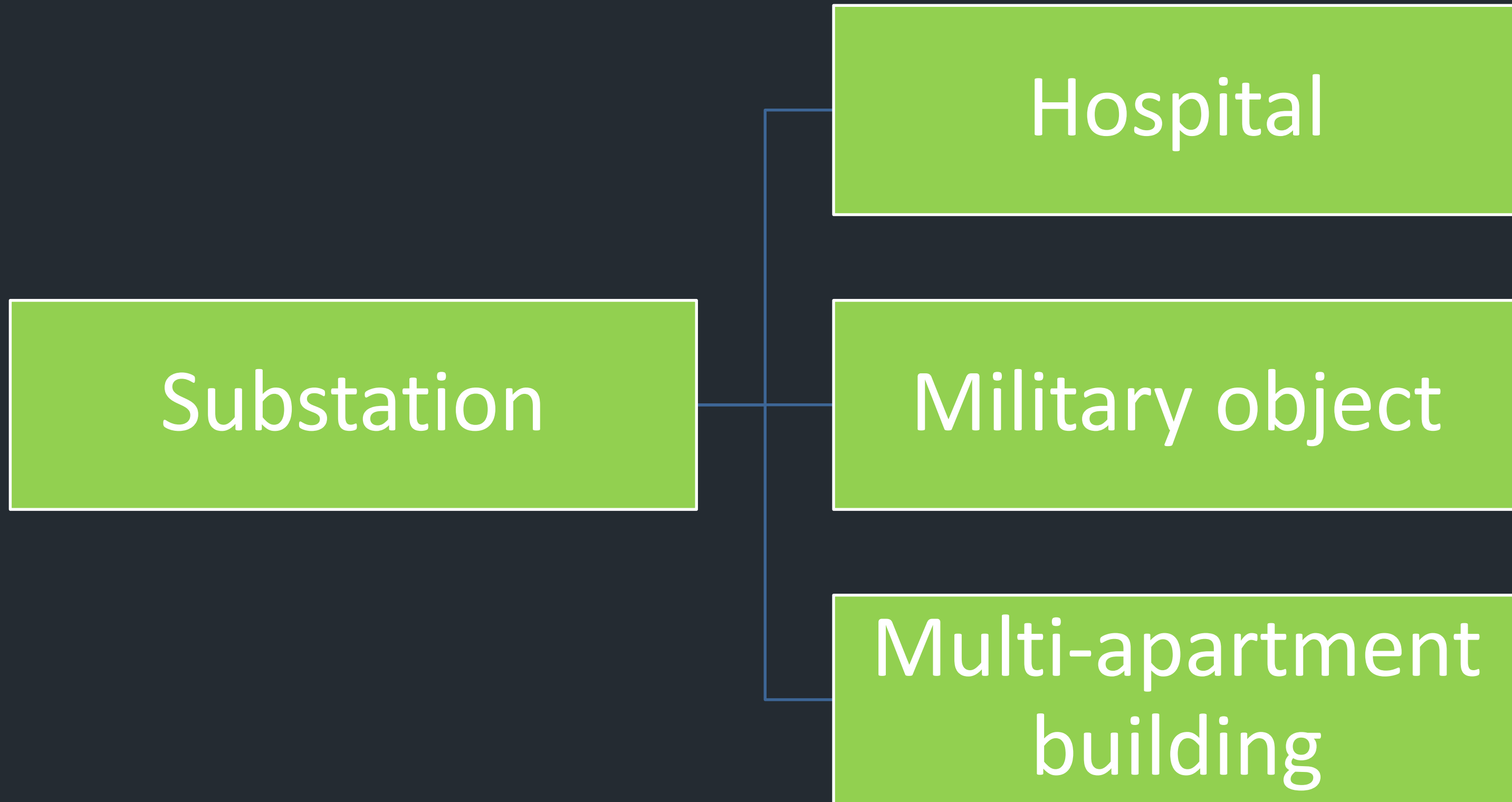
Львівобленерго Графік В

бот

Що вміє цей бот?

Цей бот є НЕОФІЦІЙНИМ, він показує графік відключення електроенергії. Розробник: @Tommy4chan

According to the another fake the electricity was distributed unfairly



False activists





Employees of Lvivoblenergo answer questions from Ukrainian journalists during shutdown schedules in Lviv region

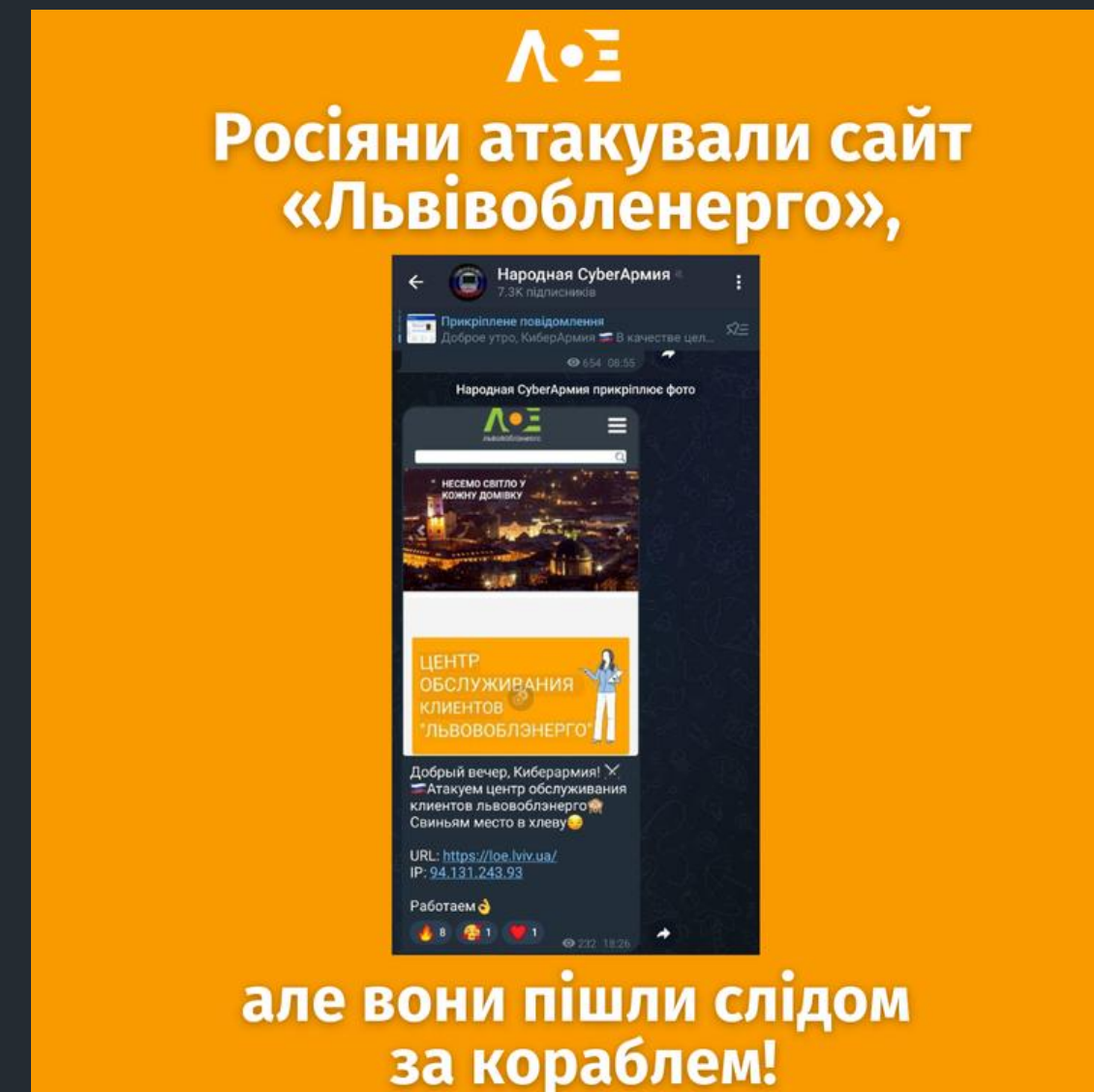
At the same time, the work of power engineers during the war aroused great interest not only of Ukrainian journalists, but also many representatives of foreign media turned to Lvivoblenergo for comments and explanations on the energy situation:

- Singapore National Media Network "MediaCorp";
- Japanese television channel Nikkei;
- Polish national television channel "TVN24";
- Polish radio "Polskie Radio Lublin";
- American copper company "Bloomberg";
- The New York Times;
- Swiss Radio.



Cyber attack

In December 2022, Lvivoblenergo's IT network was attacked by Russians. Thanks to the prompt actions of IT specialists, Lvivoblenergo, together with the Security Service of Ukraine and the Cyber Police, managed to stop third-party interference without loss. All data in internal systems has been saved.



Facebook post about Cyber attack



ЛЬВІВОБЛЕНЕРГО



STRATEGIC CYBER ATTACK: HOW RUSSIA PREPARED FOR THE WAR WITH UKRAINE YEARS IN ADVANCE

**LYUDMYLA
POLOVA**

Deputy IT Director,
Lvivoblenergo, Ukraine.

Practical experience in
cybersecurity of critical
infrastructure during
wartime.

THE WAR IN CYBERSPACE IS CLOSELY LINKED TO POLITICAL TENSIONS.

- 2007 – a coordinated hacker cyber attack on the computer systems of Estonian government institutions in April 2007 during the escalation of Russian-Estonian relations.
- 2008 – a cyber attack on Georgia during the Russian-Georgian war resulted in the successful hacking of 54 Georgian military, government, and finance websites.
- 2013-2014 – attacks on the information systems of private enterprises and government institutions in Ukraine, along with the mass use of netbots to clutter the information field, mislead people, and spread rumors during the Revolution of Dignity and the Russian armed invasion of Crimea and Eastern Ukraine.
- 2015 – an attack on Ukraine's power industry. Three regional electric power distribution companies experienced coordinated cyber attacks, resulting in a power outage lasting more than 6 hours.
- 2016 – an attack on Ukraine's largest energy company, Ukrenergo, on December 17-18, resulting in a power outage of about 1 hour and 15 minutes in roughly half of Kyiv.
- 2017 – a large-scale hacker attack using a variant of the Petya virus caused disruptions in the operations of Ukrainian state enterprises, institutions, banks, media, and industrial companies.

As Russian aggression increases, the frequency of events on this list is growing.

Hacker group	Affiliation	Main goals
APT28	military division 26165 Main Intelligence Directorate (GRU), russia	Military sector, electricity grids infrastructure, state institutions, and diplomatic institutions
APT29	Foreign Intelligence Service SVR, russia	Military sector, diplomatic institutions
Sandworm	military division 74455 Main Intelligence Directorate (GRU), russia	Telecommunications providers, critical infrastructure
Turla	military division 71330 Federal Security Service (FSB), russia	Military sector
Callisto	military division 64829 Federal Security Service (FSB), russia	State institutions, diplomatic institutions
Gamaredon	Federal Security Service (FSB) office in Crimea	Military organizations, law enforcement agencies, state and diplomatic institutions
WinterVivern	Activities for interests of Russia and Belarus	Military organizations, state institutions
Ghostwriter	Military forces of Belarus	State institutions
DaVinci Group (UAC-0050)	Law enforcement agencies, russia	Private and public sector organizations
Smokeloader Group (UAC-0006)	Financially motivate criminals, russia	Private and public sector organizations
NoName057(16)	Pseudo hacktivists Main Intelligence Directorate (GRU), russia	Private and public sector organizations
CyberArmyofRussia	Pseudo hacktivists, Main Intelligence Directorate (GRU), russia	Private and public sector organizations

THE MOST ACTIVE HACKER GROUPS WERE IDENTIFIED BY THE INSTITUTE OF CYBER WARFARE RESEARCH.

GOALS OF THE ATTACKS

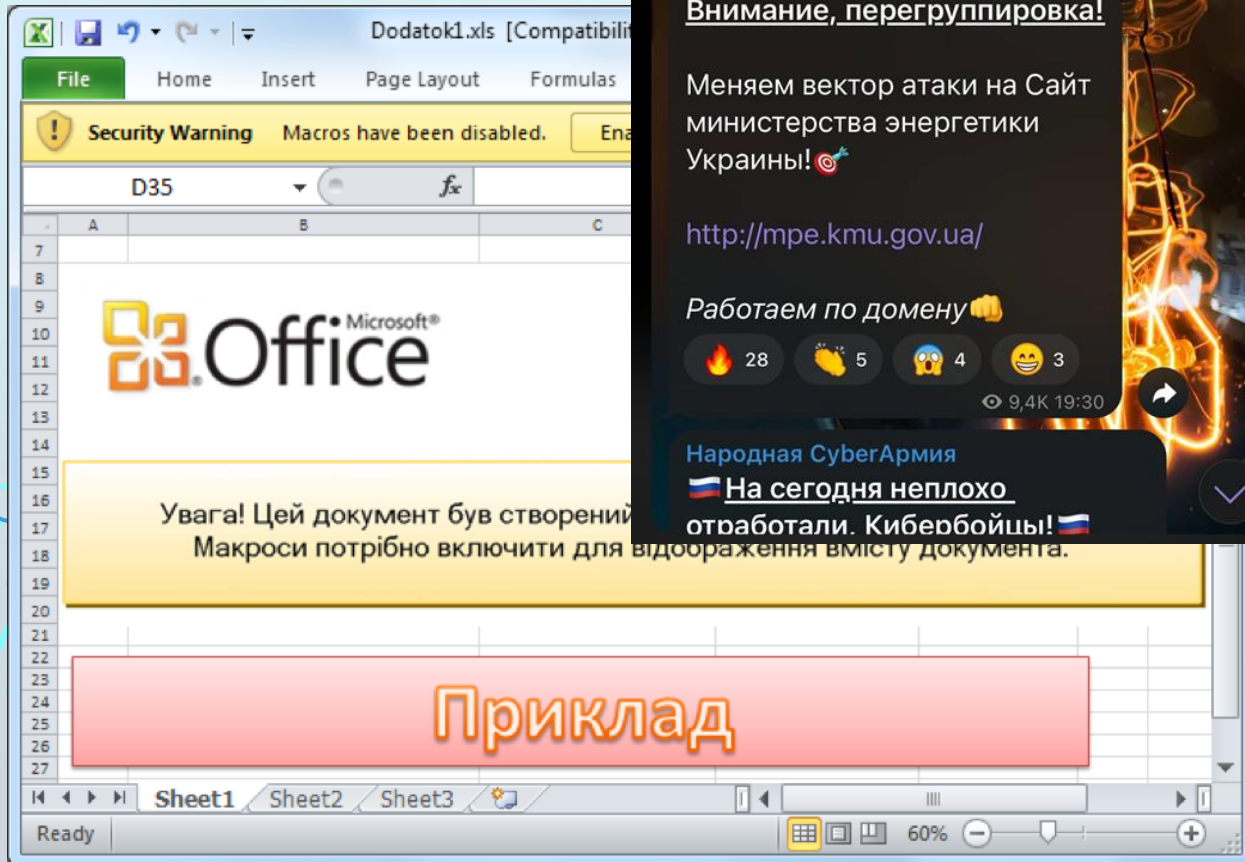
Cyberwarfare

- Espionage
- Disruption
- Discreditation
- Falsifications

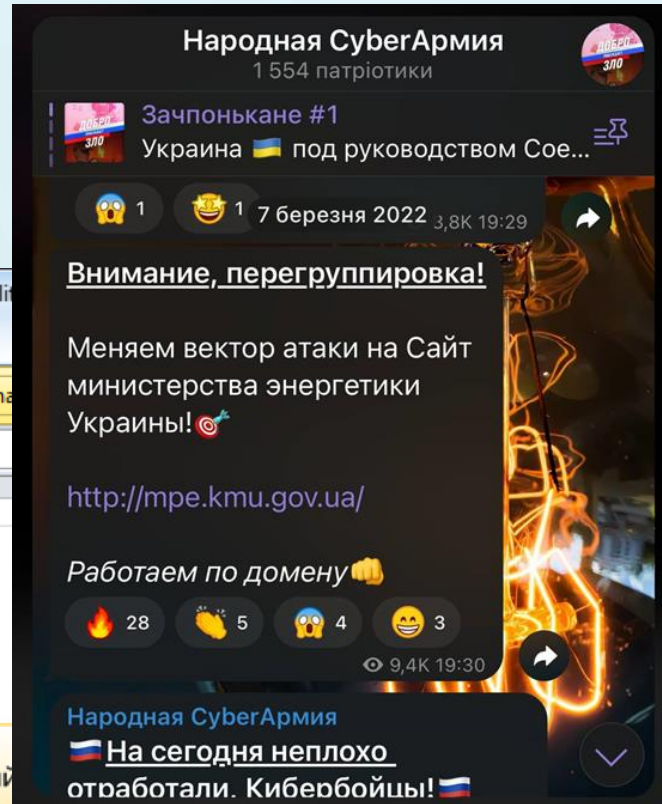
Cybercrime

- Fraud
- Extortion
- Industrial espionage

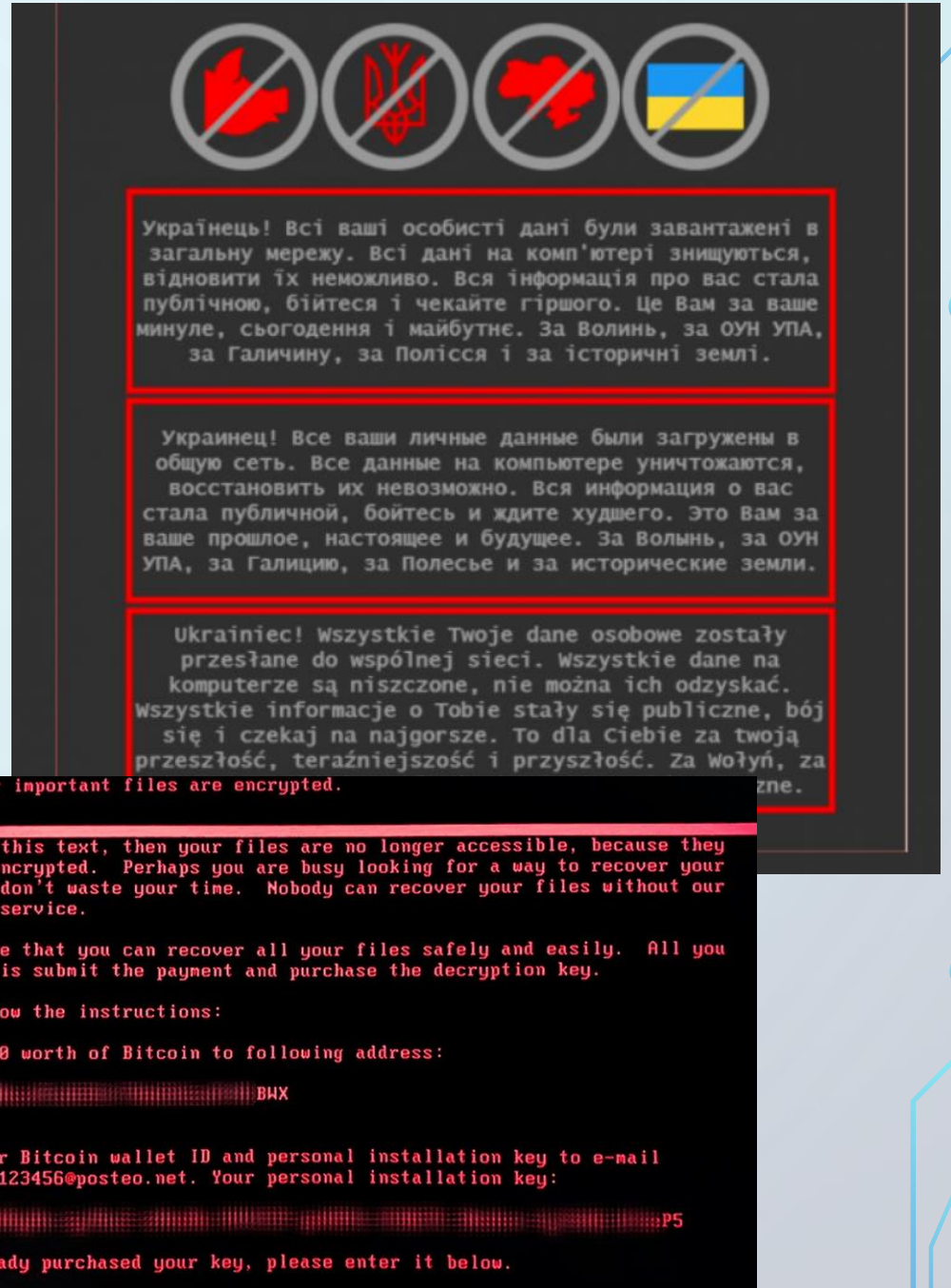
Many attacks are aimed at destabilizing society and spreading disinformation. The second priority area involves attempts to damage critical infrastructure.



The image shows a screenshot of a Microsoft Office spreadsheet application. At the top, a yellow security warning banner reads "Security Warning: Macros have been disabled." Below this, the spreadsheet grid is visible, with a large redacted area in the center. A yellow box at the bottom of the spreadsheet contains the text "Увага! Цей документ був створений Макроси потрібно включити для відображення вмісту документа." Below the spreadsheet, a red box contains the word "Приклад" (Example).



The image shows a screenshot of a Telegram channel post from "Народная CyberАрмия" (1554 patriotes). The post is titled "Зачпоськане #1" and "Украина под руководством Сое...". The main text reads: "Внимание, перегруппировка! Меняем вектор атаки на Сайт министерства энергетики Украины! <http://mpe.kmu.gov.ua/> Работаем по домену". The post has 28 fire emojis, 5 clapping hands, 4 shocked faces, and 3 smiley faces. A second message from the same channel says "На сегодня неплохо отработали. Кибербойцы!".



The image is a collage of ransomware messages. At the top, there are four icons: a red map of Ukraine, a red map of Ukraine with a black cross, a red map of Ukraine with a black cross, and the Ukrainian flag, all with a diagonal line through them. Below these are three red-bordered boxes containing ransom messages in Ukrainian, Russian, and Polish. At the bottom, there is a black box with red text containing a ransom message in English.

Ukrainian: Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це Вам за ваше минуле, сьогоднішня і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі.

Russian: Украинец! Все ваши личные данные были загружены в общую сеть. Все данные на компьютере уничтожаются, восстановить их невозможно. Вся информация о вас стала публичной, бойтесь и ждите худшего. Это Вам за ваше прошлое, настоящее и будущее. За Волинь, за ОУН УПА, за Галицию, за Полесье и за исторические земли.

Polish: Ukrainiec! Wszystkie Twoje dane osobowe zostały przesłane do wspólnej sieci. Wszystkie dane na komputerze są niszczone, nie można ich odzyskać. Wszystkie informacje o Tobie stały się publiczne, bój się i czekaj na najgorsze. To dla Ciebie za twoją przeszłość, teraźniejszość i przyszłość. Za wołyń, za...

English: ...our important files are encrypted. ...e this text, then your files are no longer accessible, because they ... encrypted. Perhaps you are busy looking for a way to recover your ... it don't waste your time. Nobody can recover your files without our ... on service. ...rantee that you can recover all your files safely and easily. All you ... to is submit the payment and purchase the decryption key. ... follow the instructions: ...nd \$300 worth of Bitcoin to following address: ...?BXH ...nd your Bitcoin wallet ID and personal installation key to e-mail ...smith123456@posteo.net. Your personal installation key:P5 ... already purchased your key, please enter it below.

The schedule of planned power outages due to electricity shortages and the search form for outages are available on our website.

Almost half a million consumers use our information services on Viber and Telegram

poweron.loe.lviv.ua

Львівобленерго Чому немає світла? Планові відключення Аварійні вимкнення (архів)

9:00-11:00	Є енергія	Немає енергії	Є енергія	Є енергія	Можливе відключення	Є енергія	Є енергія
11:00-13:00	Є енергія	Можливе відключення	Є енергія	Є енергія	Немає енергії	Є енергія	Є енергія
13:00-15:00	Немає енергії	Є енергія	Є енергія	Можливе відключення	Є енергія	Є енергія	Можливе відключення
15:00-17:00	Можливе відключення	Є енергія	Є енергія	Немає енергії	Є енергія	Є енергія	Немає енергії
17:00-19:00	Є енергія	Є енергія	Немає енергії	Є енергія	Є енергія	Можливе відключення	Є енергія
19:00-21:00	Є енергія	Є енергія	Можливе відключення	Є енергія	Є енергія	Немає енергії	Є енергія
21:00-23:00	Є енергія	Немає енергії	Є енергія	Є енергія	Можливе відключення	Є енергія	Є енергія
23:00-1:00	Є енергія	Можливе відключення	Є енергія	Є енергія	Немає енергії	Є енергія	Є енергія

[Завантажити графік](#)

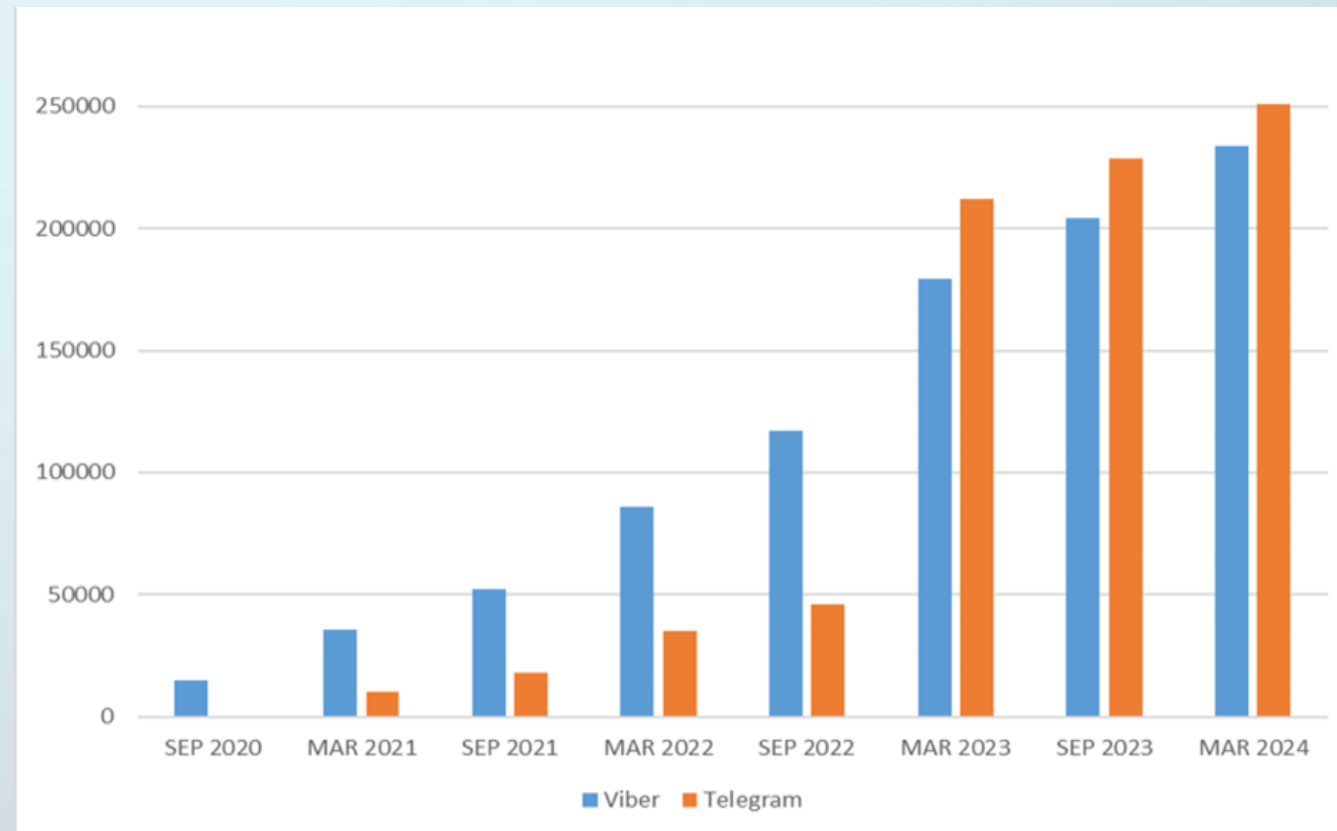
Аби дізнатись про відключення, які є в мережі на цей час, скористайтесь формою пошуку:

Об'єднана територіальна громада

Оберіть ОТГ

Населений пункт

Оберіть ваш населений пункт



Events summary

[About Firewall Events](#)

Action Host Country ASN IP Path ...

Total

1.12M

● Ukraine

1.08M

● Poland

35.11k

● United States

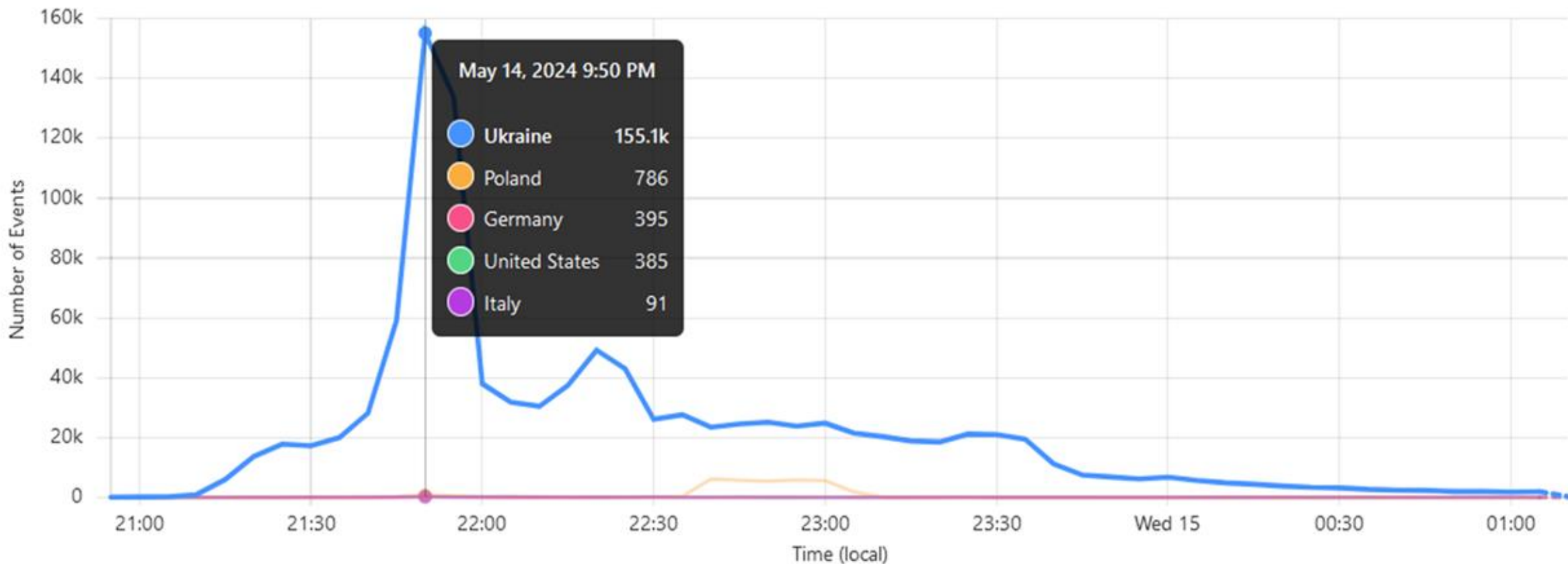
4.82k

● Germany

2.24k

● Italy

1.09k



KEY TRENDS IN CYBER ATTACKS DURING WAR ACCORDING TO THE INSTITUTE OF CYBER WARFARE RESEARCH:

- **More sophisticated and targeted attacks on organizations of interest using social engineering**
- **Attacks on accounts**
- **Use of legitimate services and tools during cyber attacks**
- **Better coordination between cyber attacks and military and information operations**
- **Greater control over the activities of hacktivist groups by intelligence agencies**

MANY OF ATTACKS IN THE UKRAINIAN CYBERSPACE IN 2023 ARE CLASSIFIED AS APT (ADVANCED PERSISTENT THREAT)

- **Attacks are carried out in several stages, stretched over time**
 - **Constant attempts are made to penetrate through different vectors**
 - **Primary infection modules have a digital signature and do not contain malicious code that can be detected by antivirus programs**
 - **Account takeovers and privilege escalations are performed**
 - **Infection files are covertly spread within the compromised infrastructure**
 - **Hackers establish secure communication channels to their Command and Control (C&C) servers**
 - **The active phase of the attack occurs without using files and storing data**

May 2022: Hackers attacked the services of the Lviv City Council, stealing and publishing some work files on Telegram channels.



Львівська
міська
рада



Сегодня Киберармия собирает кровавую жатву в виде целой толпы украинских провайдеров

Мы уничтожили 5 украинских провайдеров, а именно Империял, Копейка, Комитекс, Skyline и G-net

Теперь их клиенты останутся на долгое время без интернета. Хотя зачем хохлам интернет, если у них нет света?

В следующих постах мы опубликуем пруфы взлома и пользовательские базы, которые нам удалось добыть

December 2022: Several major internet providers in the region stopped providing services due to a hacker attack.



Impact of FrostyGoop ICS Malware on Connected OT Systems

January 2024: The Sykhiv residential area in Lviv was left without hot water and heating due to a hacker attack on a utility company.

March 2024: The transport service e-ticket in Lviv was subjected to a hacker attack, resulting in the disruption of certain services.



December 2023: Mobile operator Kyivstar suffered a large-scale hacker attack, resulting in the loss of connection and internet for subscribers. The Russian group Solntsepyok claimed responsibility for the attack.



COMMON WEAKNESSES IN CYBERSECURITY THAT LEAD TO SUCCESSFUL HACKER ATTACKS:

- **Inadequately Protected Infrastructures:** (Unsegmented network infrastructure; poorly secured communication channels and data access; delayed updates of operating systems and software)
- **Outdated Security Approaches:** (No systematic approach to building cybersecurity; lack of intrusion detection systems; no tools for responding to cyber incidents; no attack response procedure; no recovery plan after an attack)
- **Decentralized Approach to Cybersecurity:** (No centralized monitoring and management of cybersecurity; lack of enforcement of security policies; no accreditation procedures for partners; no overall infrastructure plan and complete information about assets)
- **Staffing Issues:** (Lack of understanding of cybersecurity issues; insufficient qualified specialists)

Lyudmyla Polova

lpolyova@loe.lviv.ua

www.loe.lviv.ua



Thanks to the **INSTITUTE OF CYBER WARFARE RESEARCH** for providing the materials:
www.facebook.com/CyberWarfareInstitute
info@understandingcyberwar.org

understandingcyberwar.org



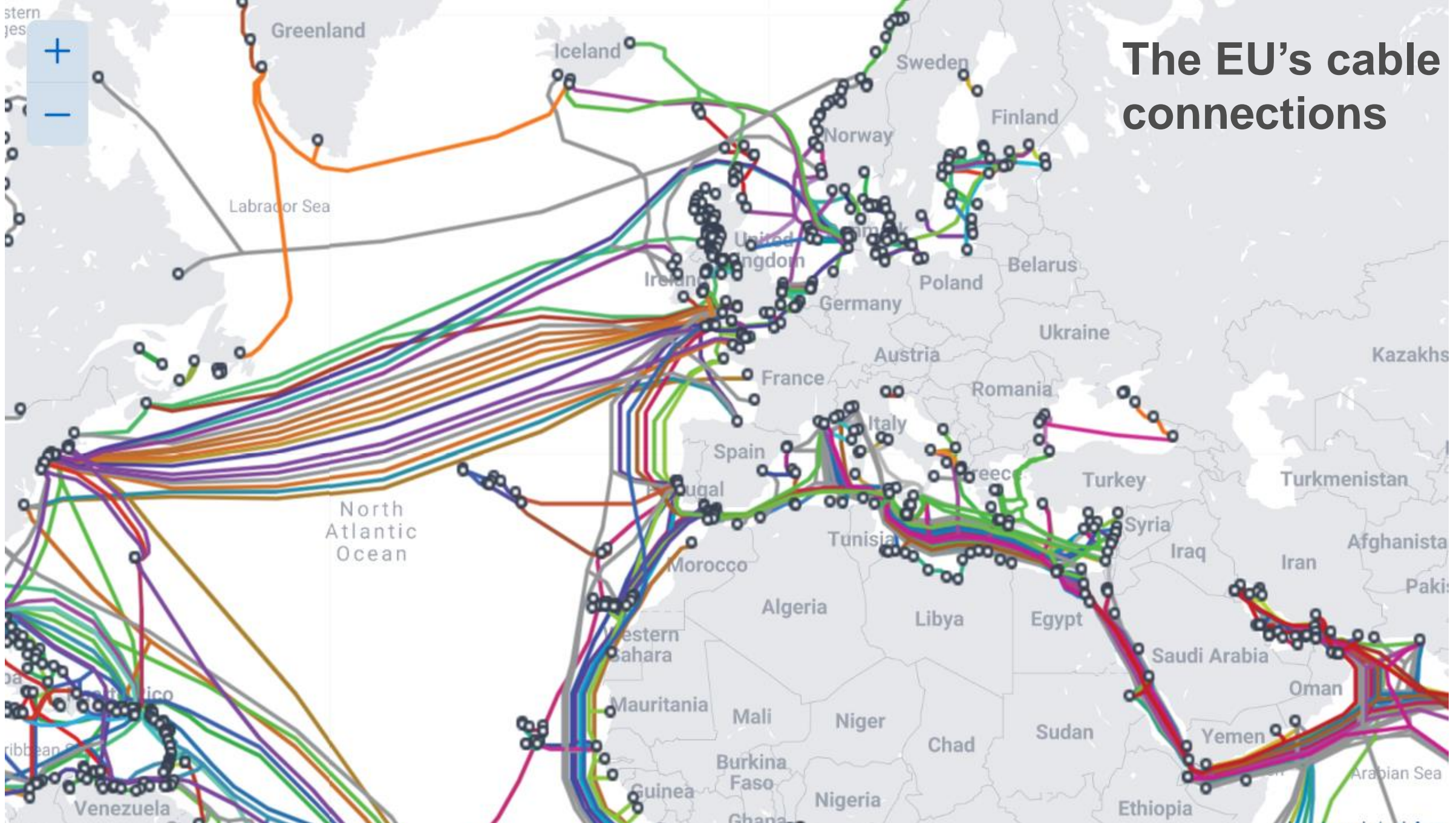


Key Areas for Resilience and Critical Infrastructure Protection: the case of submarine cable infrastructures

*Agustin Diaz-Pines, Deputy Head of Unit, DG
CNECT E.1*

4 September 2024

The EU's cable connections



Relevance of submarine cable infrastructures

- Security & resilience of infrastructures: **complementary** role of terrestrial, satellite and submarine connectivity
- **Over 99% of intercontinental data traffic** is carried through submarine cables
- **More than 60%** of the international traffic transits through submarine cables not managed by public operators
- Since 2012: **large non-EU providers** investing in **own infrastructures** → **strategic dependencies**
- **NATO Critical Undersea Infrastructure Coordination Cell** aims at addressing the security of submarine cables

EU Policy Context

- 2021 European Data Gateways [Ministerial Declaration](#)
- [2022 Council Recommendation](#) on resilience of critical infrastructure
 - Mandate for Commission to carry out study and present appropriate measures
- Geopolitical and security situation in Europe, with several incidents on critical infrastructure during recent years
 - Repeated calls from Member States & stakeholders for immediate action (e.g., [Informal TTE Telecoms Council](#) in León (10/2023), [TTE Telecoms Council](#) (12/2023))
- [2024 Commission Recommendation](#) on secure and resilient submarine cable infrastructures
 - Basis for dedicated Expert Group
- 2024 Report on the cybersecurity and resiliency of the EU communications infrastructures and networks ([Nevers Report](#))
 - Relevant for deliverables of Expert Group
- [2024 White Paper](#) on “How to master Europe’s digital infrastructure needs?”
 - Longer term scenarios building on the work under Recommendation

Commission Recommendation: Secure and Resilient Submarine Cable Infrastructures

Scope

- Intra-EU and international connectivity
- Cables but also landing stations, repair centres, ships for deployment, maintenance and repair

National level actions:

- Promoting high security level when transposing NIS 2 and CER Directives
- Mapping, risk/vulnerability/dependency assessments, stress tests
- Fast-track permit granting

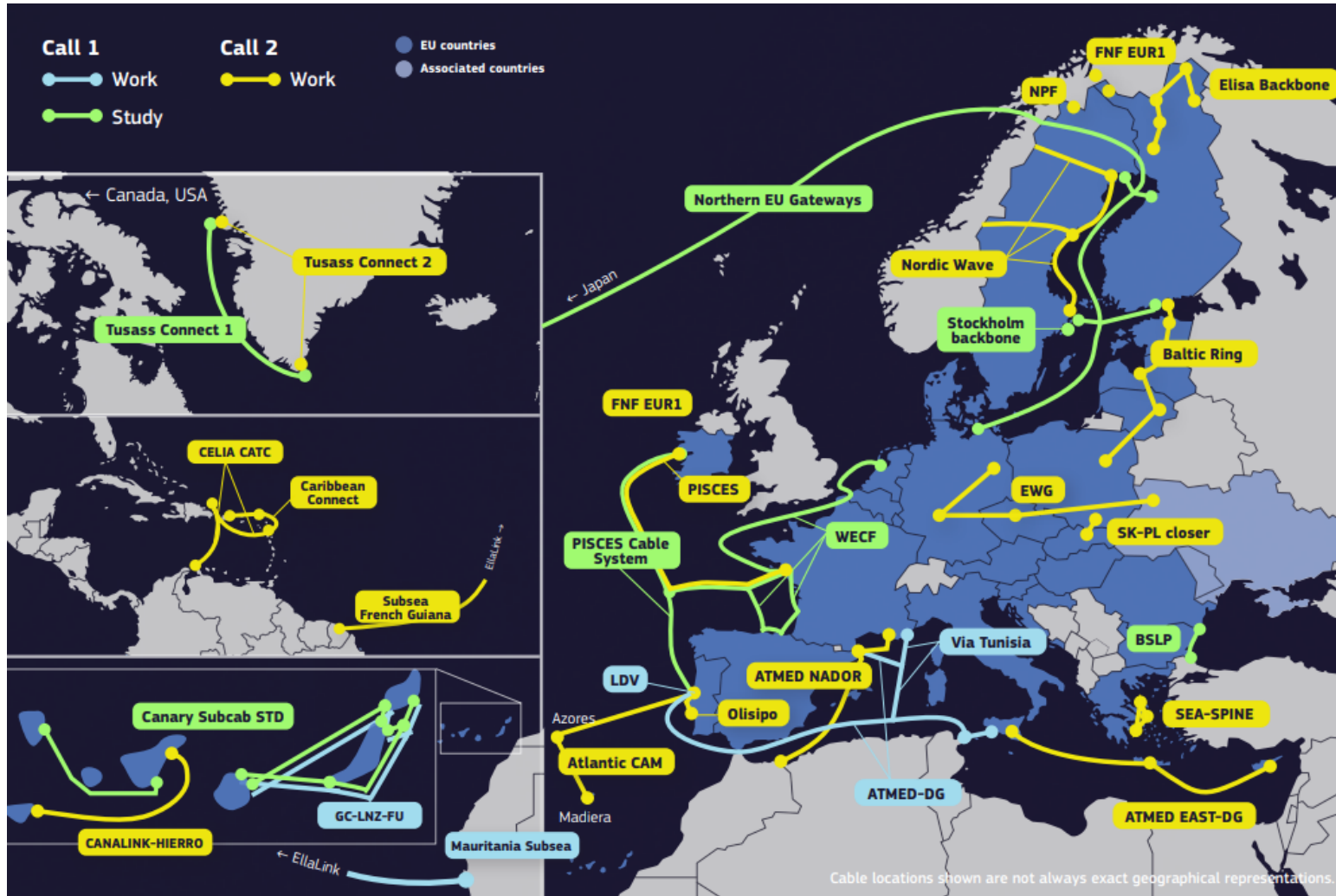
Union level actions:

- Consolidated mapping and assessments
- Cable Security Toolbox
- Criteria for Cable Projects of European Interest (CPEIs) as potential mitigation measure
- Coordinated Team Europe approach internationally

→ Follow-up: Expert Group, met first on 27 June

Connecting Europe Facility (CEF)

Results from CEF Digital Global Gateways Calls 1 and 2

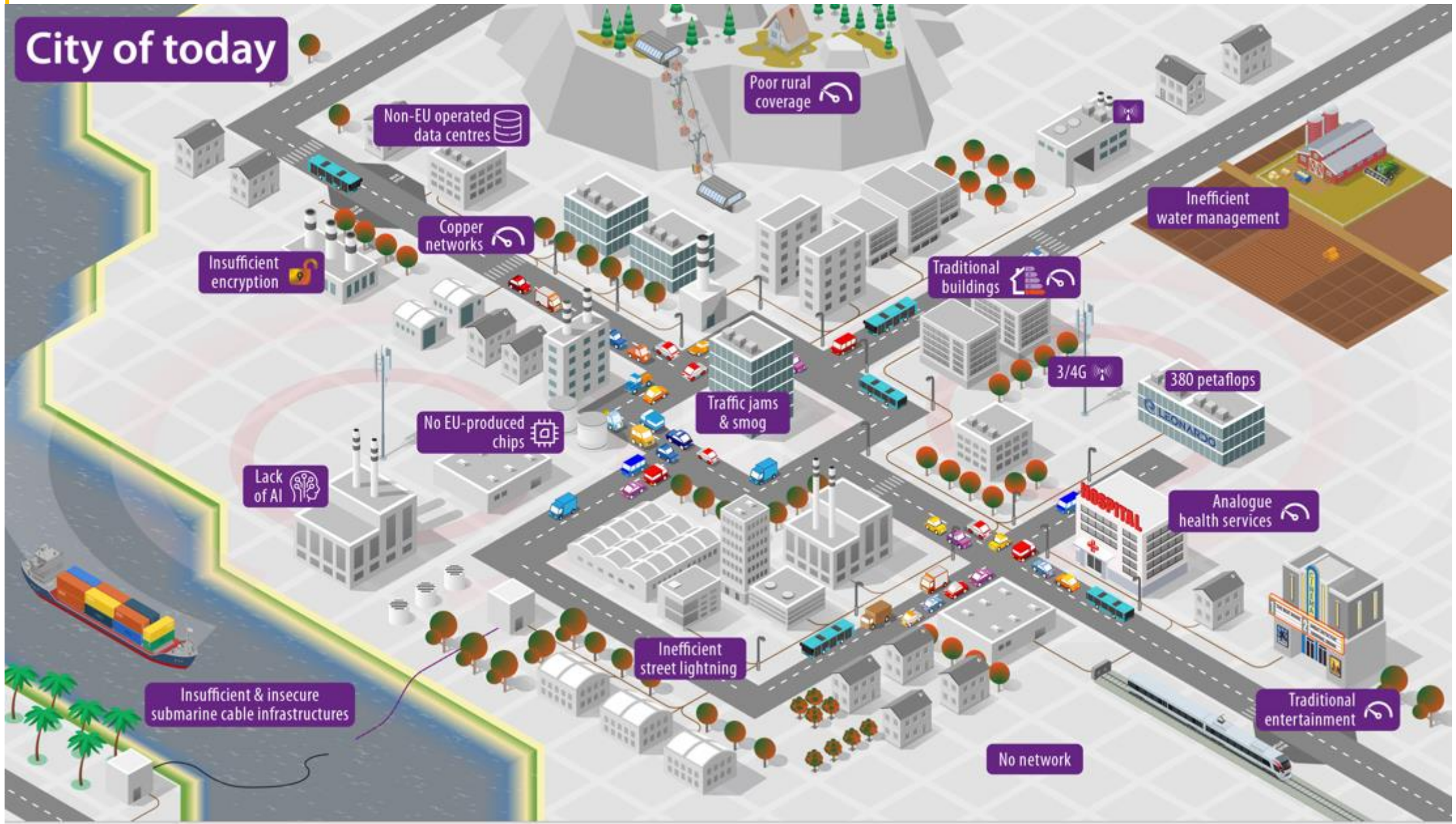


- 30 Projects
- € 277 million
- Wide coverage
- OTCs (Overseas Territories and Countries) and OMRs (Outermost Regions)

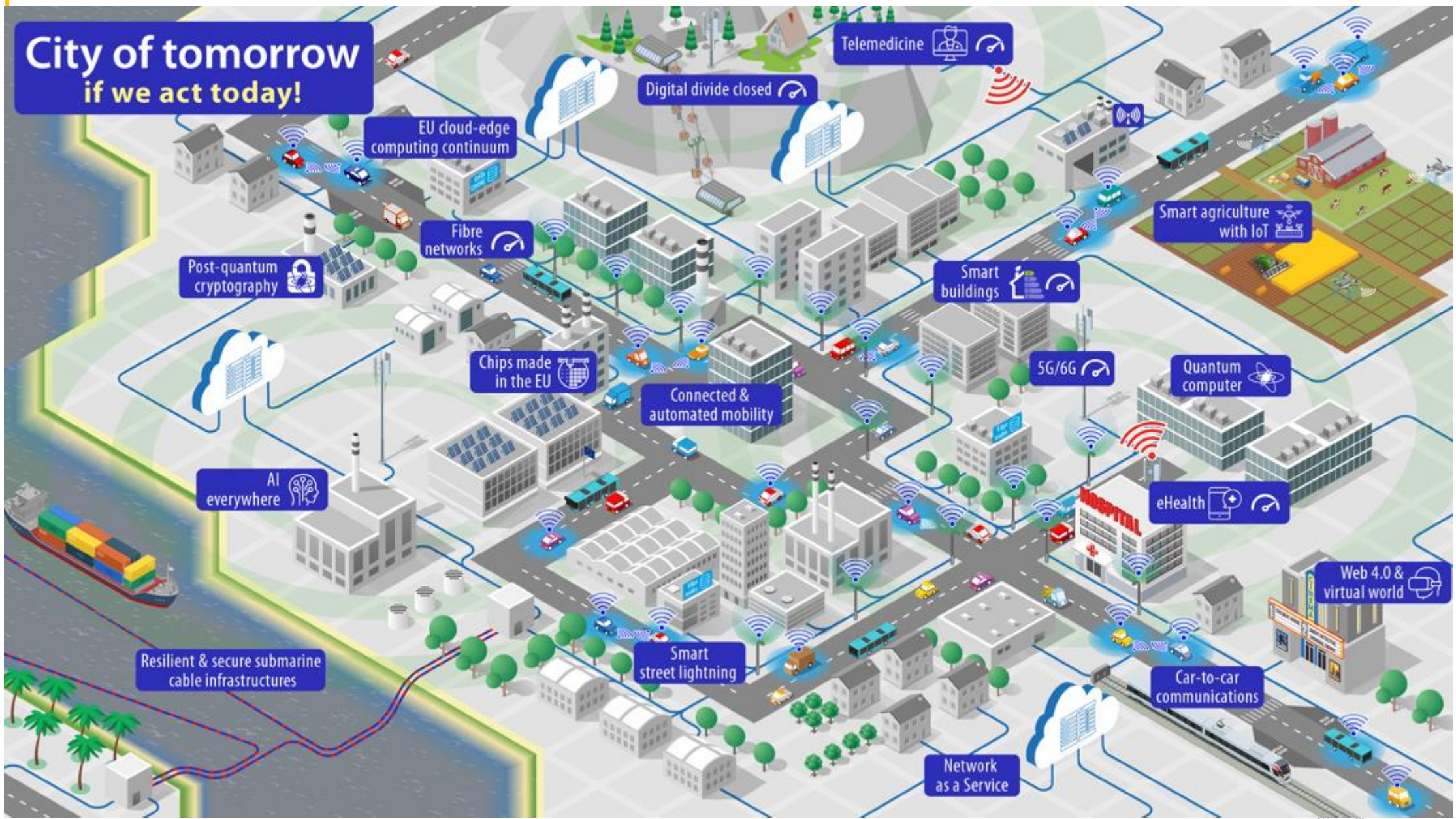
White Paper: How to master Europe's digital infrastructure needs

- **Pillar I:** Creating the “Connected Collaborative Computing” Network (“3C Network”)
- **Pillar II:** Completing the Digital Single Market
- **Pillar III:** Creating secure and resilient digital infrastructures in Europe

City of today



City of tomorrow if we act today!



White Paper: How to master Europe's digital infrastructure needs

Pillar I: Creating the “Connected Collaborative Computing” Network (“3C Network”):

- **Large-scale pilots** that set up end-to-end integrated infrastructures and platforms for telco cloud and edge
- Possibility of a **new infrastructure-focussed IPCEI**
- **Different options in order to frame the massive investments** required into a simplified and coordinated support framework for a truly digital single market drawing on European and national, public and private investments (incl. possibility to assign to the Smart Networks and Services Joint Undertaking (**SNS JU**) a **coordinating role**)

White Paper: How to master Europe's digital infrastructure needs

Pillar II: Completing the Digital Single Market

- **Adapt regulatory framework:** realise full potential of digital single market
 - rethink scope of application and objectives
 - ensure regulatory level playing field (equivalent rights and obligations for all actors and end-users of digital networks)
- **EU core network operators:** leverage full potential of single market
 - application of a single set of rules (Country of origin)
 - change to access policy (EU wholesale access product; no markets for presumptive ex ante regulation)
- **Spectrum:** more integrated governance at EU level; more aligned authorisation and selection conditions
- **Copper switch-off:** measures to accelerate it by 2030
- **Sustainability:** all players to contribute to increasing transparency on the emissions related to service usage (e.g. codecs' performance labels)

White Paper: How to master Europe's digital infrastructure needs

Pillar III: Creating secure and resilient digital infrastructures for Europe

On submarine cable infrastructures:

- Reinforcement of advanced **R&I activities** for new fibre and cable technologies
- **Joint EU governance system** on submarine cable infrastructures
- **Harmonised security requirements** in international fora, potentially dedicated EU certification scheme
- **Delegated Act under the Connecting Europe Facility** on CPEI list and related labelling system
- Review of available funding and financing instruments, incl. **possible equity fund**

11 April 2024: Recommendation on **Post Quantum Cryptography**

Next steps

- **White Paper:** Assessment of feedback (closed on 30 June 2024)
- **Recommendation:** Work within Expert Group (next meeting: Oct/Nov 2024)

Thank you

Improving the Resilience of Power and Telecommunication Networks in Germany

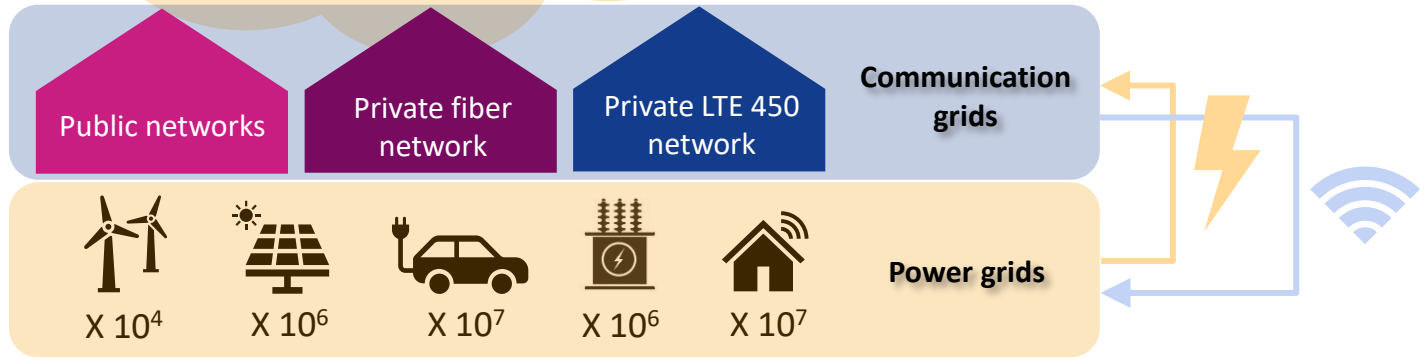
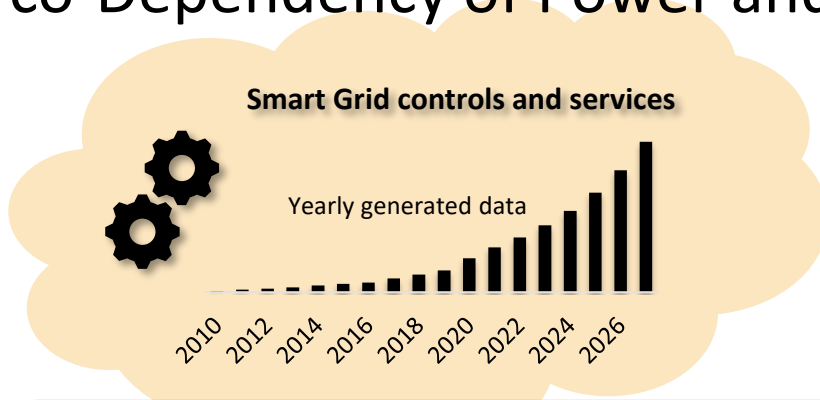
Westenergie AG · Dr. Stefan Küppers · 4. September 2024



Content

1. Introduction and motivation
2. Definition of resilience
3. Key challenges in energy and information systems
4. VDE approach in Germany
5. How we do it at E.ON and Westenergie
6. Summary

Digitisation and Energy Transition increase co-Dependency of Power and Communication Grids



Resilience in Power- and Information systems

The ability of any system to continue to:

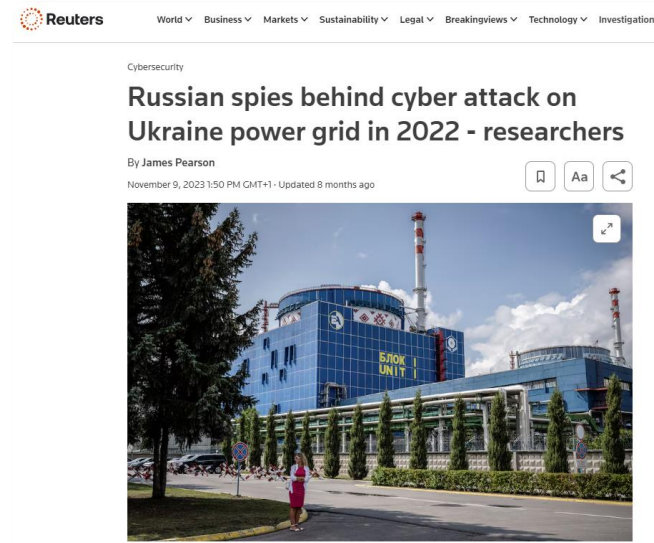
- I. **Operate under adverse conditions or stress**, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and
- II. **Recover to an effective operational posture** in a time frame consistent with mission needs.

Based on: [NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View](#)

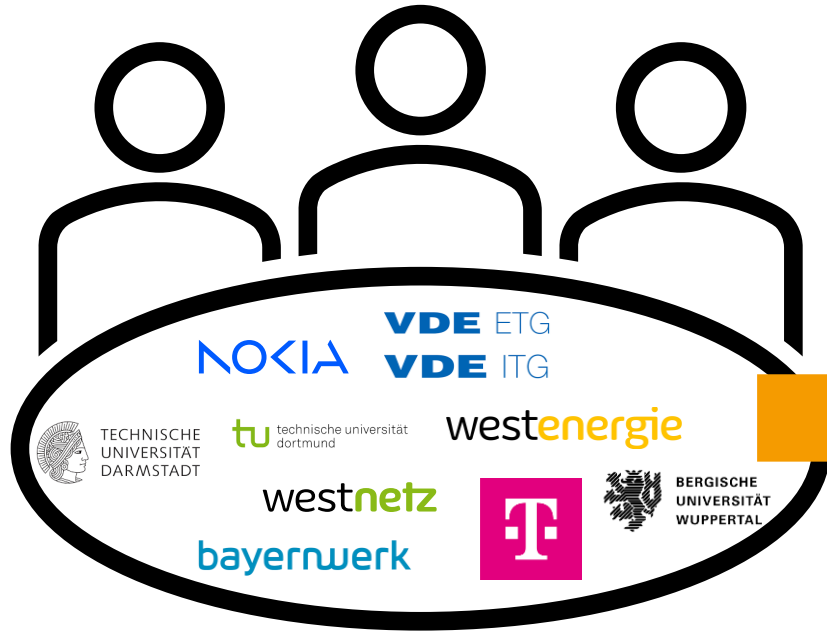
Climate change and cyber warfare pose growing risks to the infrastructure we rely on



Photo taken immediately after the flood in the Ahr valley



Cross-industry experts have developed recommendations to improve grid resilience



VDE Impulspapier

Mehr Resilienz für die Strom- und Kommunikationsnetze in Deutschland

Wie gehen wir mit den zunehmenden gegenseitigen Abhängigkeiten um?
by VDE ETG ITG

44-page discussion paper

VDE

Key takeaways

Build **awareness** for increasing mutual dependencies

Think and act **across sectors** and industries

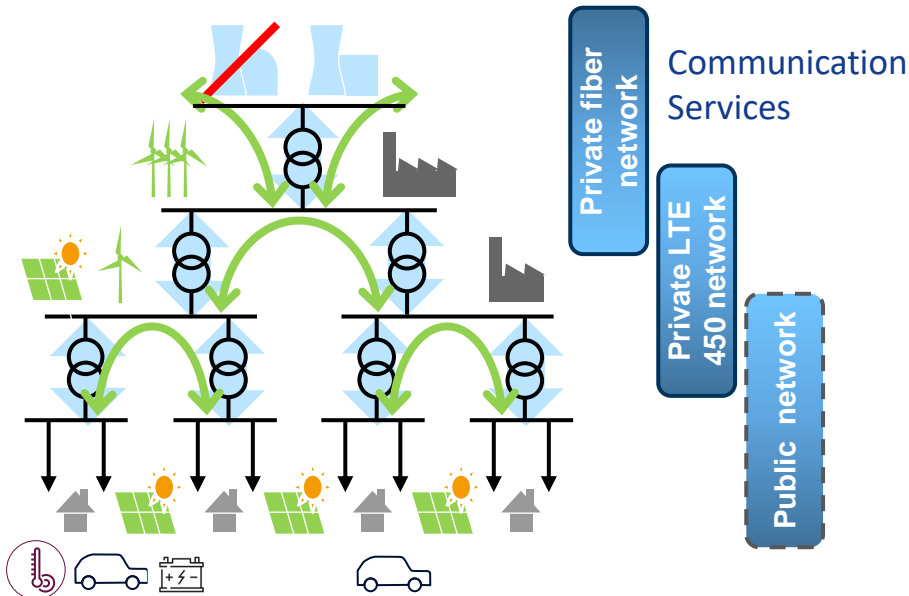
Consider potential **disasters** (man made and natural)

Systematically **plan and implement measures** to address potential risks

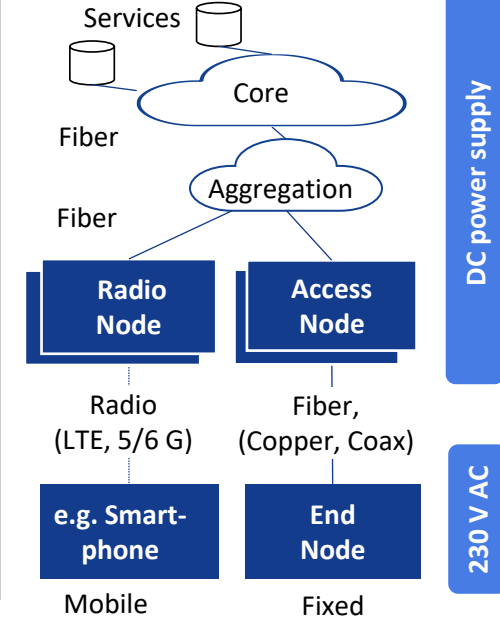
Evolution of Power Grids and (Public) Communication Networks

Source: VDE

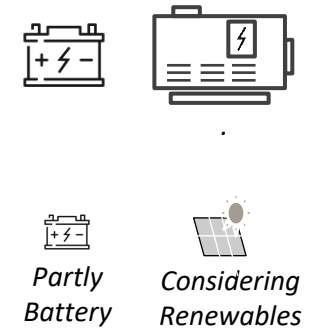
Power Grid



Public Comm. Networks



Power supply



Multi party value chain

Key Trends for Power Grids and Communication Networks

Source: VDE

Power grids

- Growing demand for electrical power
- Transition to renewables. Decentralization
- Digitalization, need for reliable comms

Public communication networks

- Exponential traffic growth
- Broadband, small cells, optics, all IP, cloud
- Reliable power supply needed

Digitalization, Electrification, Energy Transition

- Reliable communication networks and electrical power grids are paramount for our life
- Increasing complexity and interdependency between communication networks and power grids

Climate change, cyber crime, geo-political challenges

- Natural disasters, cyber attacks, sabotage, (war)
- More “intertwined” critical infrastructures, power and communications are essential for all

Is mutual interdependency an issue for network resilience*?

* Resilience comprises the **resistance** of a system against faults/disruptions and its **recovery** afterwards

Our company-wide approach to rapid recovery

Steps towards
resilience

1

2

3

4

Goal



Transparency



Get to know all your assets! To recover implies, you know what assets can be disrupted in the first place.

“Know what you have and where to look”

Classification



Once you know your assets, you can categorize them by criticality. Which is the most important, which is negligible?

“Know what to value the most”

Business Continuity Management



Based on identified and assessed critical processes, measures (Business Continuity Plans (BCP) / Disaster Recovery Plans (DRP)) can be developed and implemented. Remember to check these plans regularly!

“Know how long you can survive without it”

Crisis Management (Exercises)



Train the implementation of the developed plans in realistic scenarios repeatedly! On paper, a plan might seem perfect. Reality often proves otherwise!

“Know what to do by heart to act quickly”

Rapid Recovery



Unleash the resilience:

1. **Identify** the affected assets (transparency)
2. **Prioritize**, which assets need to be recovered first (criticality)
3. Start to **roll out** the developed the BCP/ DRP (BCM)
4. Perform a **Lessons Learned** and improve the plans!

Practical examples: Business Continuity Management and Crisis Management



Mobile substations as part of our business continuity management (BCM)



Crisis Management (Exercises)



Practical example: Categories of flood resilience in our power grids

Category	Operating state	Functionality	Example
Flood-proof through location	Flooding does not occur	ensured	<ul style="list-style-type: none">• Relocation of assets outside the HQextreme zone (flood every 200 years)• Placement of assets above the expected flood levels
Flood-proof through technology	Flooding is permissible	ensured	<ul style="list-style-type: none">• Asset design according to IP68• Example streetlights “Hamburg Fischmarkt”
Flood resistant	Flooding is defined	not ensured; no restoration measures required	<ul style="list-style-type: none">• Automatic activation/deactivation of flood zones• Remotely controllable assets
Flood protected	Flooding is defined	not ensured; measures required for restoration	<ul style="list-style-type: none">• No house connections in basements• No basement substations• Electrically disconnectable flood zones

This is how we keep the lights on

Digitisation and energy transition increase co-dependency of power and communication grids.

We are **working together across industries** to tackle these challenges.

Climate change and **cyber warfare** pose **growing risks** to that infrastructure.

We can **improve resilience** by

- ↳ **Creating transparency**
- ↳ **Classifying our assets**
- ↳ **Planning**
- ↳ **Training**

Any Questions?

Thank you!