Crisis engineering, digital resilience, and free software

How I’m helping digital resilience in Europe and how you can too

Valerie Aurora, Bow Shock Systems

https://bowshock.nl

Valerie Aurora, Bow Shock Systems

- Systems software consultant with 25 years of experience in FOSS file systems, networking, etc.
- Developer on rpdfs, a new FOSS distributed network file system
- Special rapporteur for CRA operating systems and network interfaces
- Moved from San Francisco to Amsterdam in 2023

Submarine cables at Museu das Comunicações in Lisbon

Outline

- Why Europe needs independence and resiliency more than ever
- What crisis engineering tells us about how this transition will happen
- Three ways I'm improving European independence and resiliency with FOSS:
  - Easy: Moving my online life to European owned and controlled services
  - Moderate: Starting an Internet Resiliency Club
  - Hard: Developing Cyber Resilience Act standards
- How you can improve European independence and resiliency too!

Disruption is the new normal for Europe

- Danish intelligence service assesses that Russia is conducting a hybrid war with Denmark and the West
- The U.S. has threatened to take over or occupy parts of Greenland and Ukraine (among many others)
- The U.S. used sanctions to cut off access to Microsoft email for members of the ICC
- 10+ hour Iberian peninsula blackout, caused by regulation falling behind changes in power generation

Newnew Polar Bear, suspected of causing Balticconnector cut

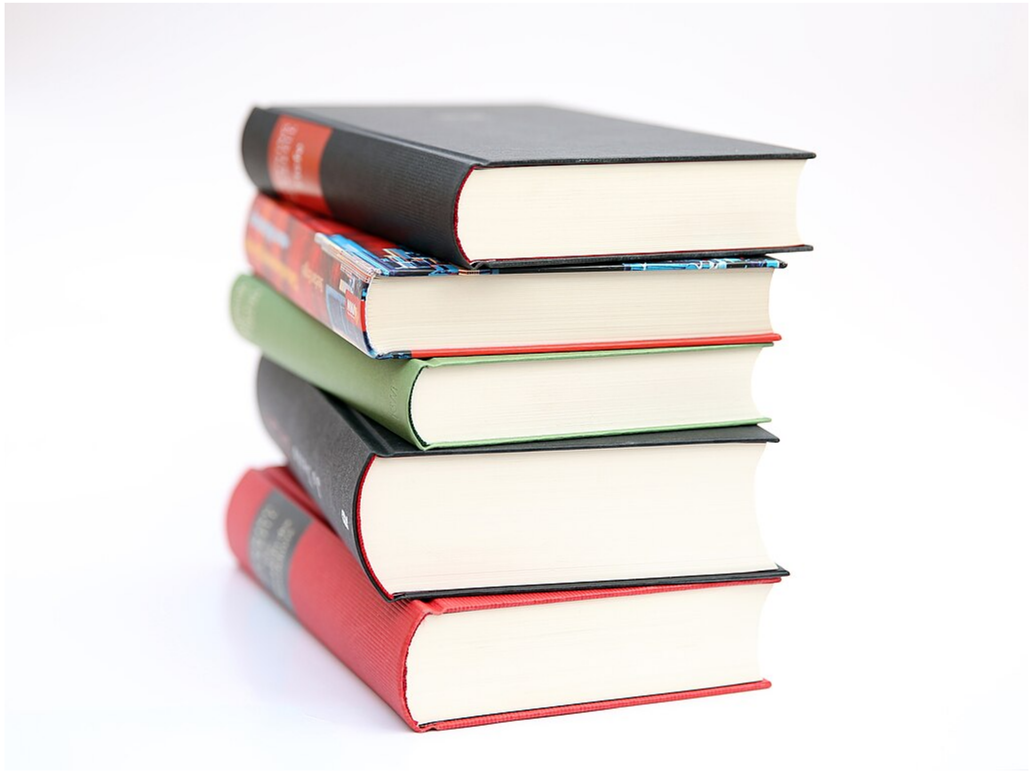
Credit: Alf van Beem

What if we lose internet AND power?

Repairing damage from Russian attacks in Ukraine
Source: https://ripe90.ripe.net/archives/video/1582/

What is Europe doing to prepare?

- ENISA published lots of good recommendations to improve security and resiliency of communications infrastructure
- Unfortunately, most member states have not implemented the recommendations
- When governments do have plans to improve security and resiliency, they won't be in place for several years



Valerie Aurora, Bow Shock Systems http://bowshock.nl/

What is Europe doing to prepare?

- **Ukraine is leading the way on both implementation and knowledge sharing**
- Ukrainian IXP IX-1 has concrete advice for network operators to improve resiliency
- Finland, Estonia, Latvia, Lithuania all doing better than average
- Is there a pattern?

What is Europe doing to prepare?

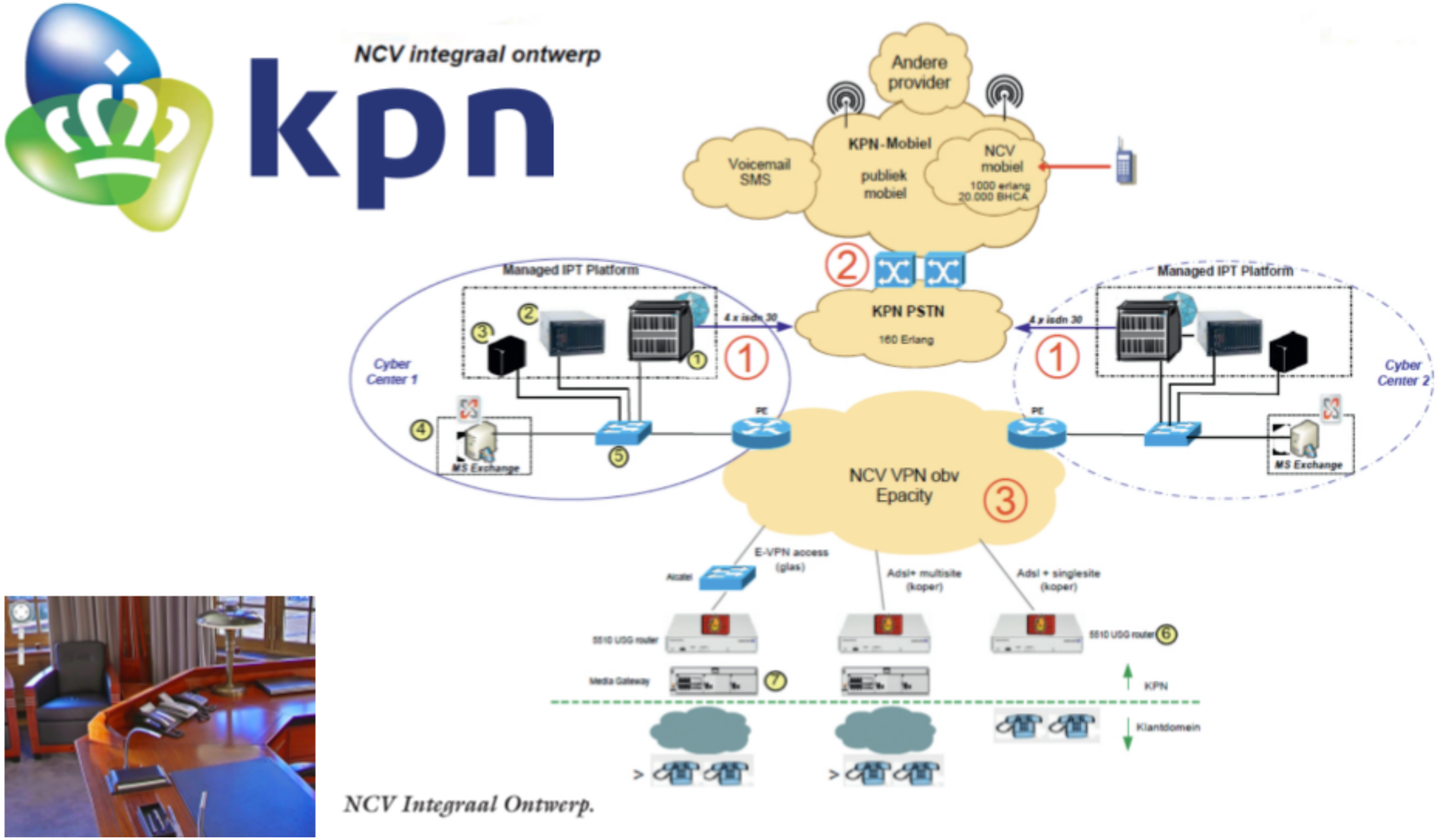
- **Ukraine is leading the way on both implementation and knowledge sharing**
- Ukrainian IXP IX-1 has concrete advice for network operators to improve resiliency
- Finland, Estonia, Latvia, Lithuania all doing better than average
- Is there a pattern?

Source: https://www.thescottishsun.co.uk/news/1995321/russia-secretly-practised-full-scale-invasion-of-europe-with-bombing-raids-on-germany-during-vladimir-putins-military-drills/

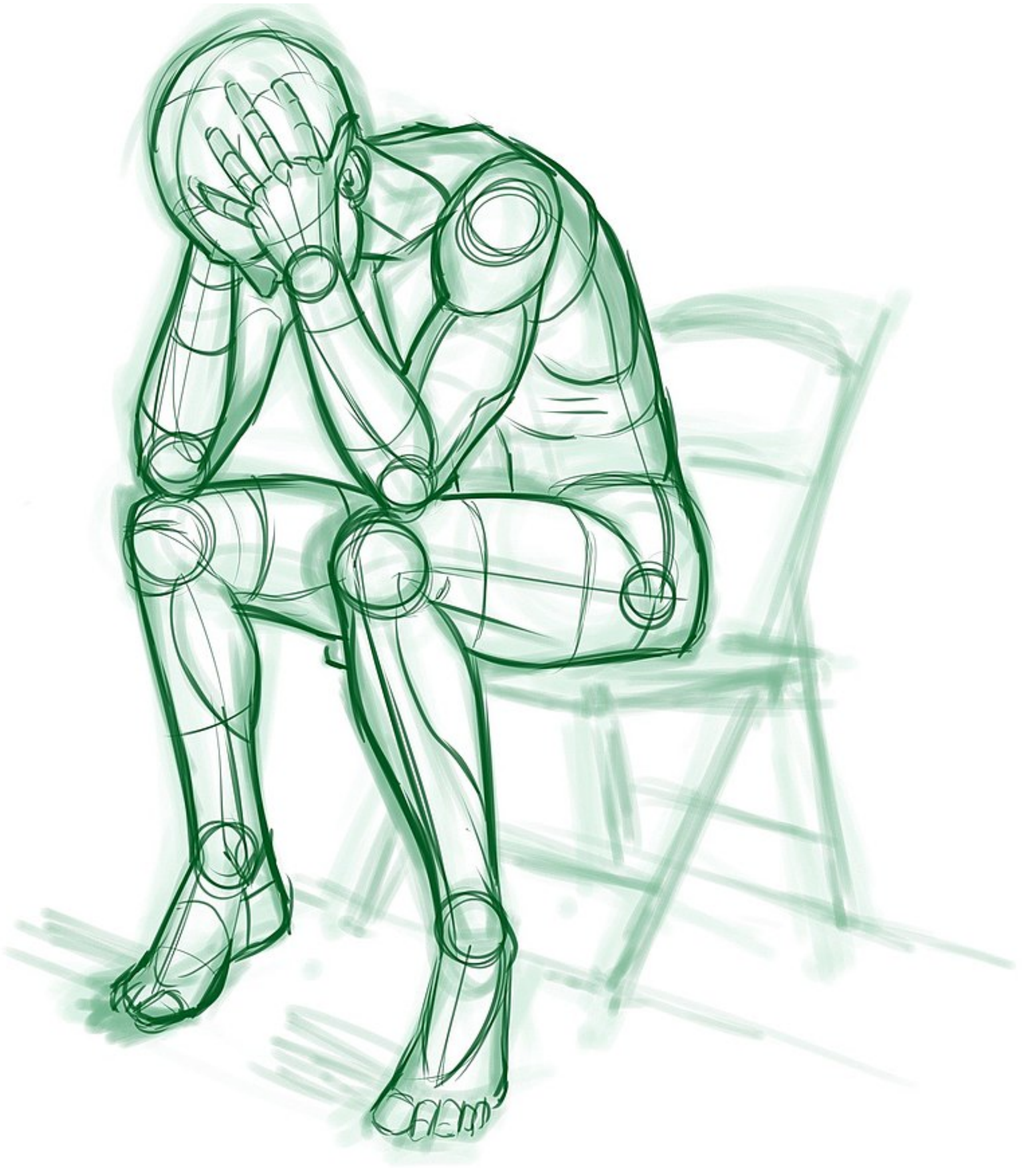
What is the Netherlands doing to prepare?

- Dutch government has a plan for improving cybersecurity… by 2028
- Dutch national and local government and corporations are moving to U.S.-owned clouds
- Even if a service is owned by a Dutch company, the tech workers may not be in the Netherlands, which makes it hard to fix when there's no internet
- Even the Dutch national emergency communication system is implemented in the cloud!!

Dutch “emergency” national communications



Source: https://berthub.eu/articles/posts/cyber-security-pre-war-reality-check/



What can we do?

- If government and businesses aren't preparing for the crisis, can we force them to take action by warning them of the possible crisis?
- Answer: Generally, **no**
- But when the crisis arrives, suddenly they are more open to change!

Enter crisis engineering

- Crisis engineering is the study of structural transformation of organizations during crises that threaten their core functions
- Developed by a bunch of site reliability engineers while fixing a bunch of broken U.S. government systems and other organizations
- Based entirely on real-world experience
- Now they do this full-time at Layer Aleph, a consulting company
- A book is coming soon!!! It is very good
- More on crisis engineering at https://layeraleph.com/

Organizations don’t like change

- “If it ain’t broke, don’t fix it” - good advice, **when things are stable**
- People and organizations LOVE to operate on auto-pilot and avoid thinking, because it is easier and more efficient
- Organizations usually avoid risky or expensive changes when things are working, like changes necessary to prepare for crises
- Individual people within the system are incentivized to not break things or challenge the status quo
- Result: major change is almost impossible - **except during a crisis**

Valerie Aurora, Bow Shock Systems http://bowshock.nl/

What is a crisis?

Five elements of a crisis, as defined by Layer Aleph:

1. Fundamental surprise
2. Perception breakdown
3. Degradation or change of process or outcomes
4. High visibility
5. Rigid timing constraints

Fundamental surprise

- An event that violates the consensus reality of the organization around:
  - How things work
  - What is happening
  - What their relationship to the outside world is
  - What their purpose is
- E.g. “We route internet traffic. Now we have no power to any of our data centers, and the generators are running out of fuel, at which point we will no longer be routing internet traffic.”

Valerie Aurora, Bow Shock Systems http://bowshock.nl/

Perception breakdown

- **Sensemaking** is the automatic continuous process of making decisions that governs most actions by most people and organizations most of the time
- Daniel Kahneman calls it “thinking fast,” as opposed to “thinking slow”
- In a crisis, sensemaking stops working because the usual ways of gathering information and making decisions don’t work in the new circumstances
- During a crisis, the organization must learn new ways of observing, deciding, and acting

Degradation or change of process or outcomes

- The organization cannot fulfill its core mission: routing network traffic, or fighting fires, or selling health insurance to U.S. residents
- Or the organization's core mission changes to something very different
- I'm seeing this firsthand working on CRA standards - more later

High visibility

- If an organization is having some kind of major disruption or change, and no one knows about it… it will often just pretend that it is working
- Visibility can come from within the organization or from outside (e.g., internal discussion on chat, news stories)
- High visibility means there are potential consequences for not fixing the problem
- High visibility paradoxically can make the problem harder to solve, as people become **more** conservative and fearful

Rigid timing constraints

- Without a deadline, a failing organization can go on forever
- Deadlines can be created by physics, courts, legislation, markets, weather, people's health, etc.
- One of the reasons fighting climate change is so hard: there's no agreed-upon obvious deadline (scientists identify possible "tipping points" but can't prove them)
- Hard deadlines can be a gift!

Public Domain OpenClipArt

A crisis is an opportunity to make change

- When an organization can no longer operate on autopilot and must change before a hard deadline, changes that were impossible become trivial
- If you know the crisis is coming, can perceive it, have tools to deal with it, and have a plan for moving forward, you can often transform an organization
- Crisis engineering is: setting up an incident command center, finding some key metrics, getting the most accurate information possible, building a map, and then taking action and seeing what happens (sensemaking)
- How does this relate to European independence and resilience?

We don’t have a crisis in Europe - yet

Which elements of a crisis are happening now?

1. Fundamental surprise: YES
2. Perception breakdown: YES
3. Degradation or change of process/outcomes: Some
4. High visibility: Some
5. Rigid deadline: NOT YET

What can we do before the crisis?

- Make a plan
- Gather a like-minded community and work together
- Get to know all the people who can help implement your plan
- Build tools, practice, run drills
- Prioritize what needs to be done BEFORE the crisis starts
- When the crisis arrives, present your plan to the people who can implement it

My personal plan to improve internet resiliency

1. Move my online life to European-owned, European-hosted infrastructure
2. Start an Internet Resiliency Club
3. Develop Cyber Resilience Act standards

Moving to European online services

- My goals: move my social media, web hosting, domain name registrar, at least one domain's TLD, email, calendar, and online document editing to European owned and hosted services
- Used https://european-alternatives.eu/ to find good options
- Waited until I had two weeks of little-to-no business activity
- Started with US Mastodon, Dreamhost, WordPress, one .org and one .com domain, Gmail, GCalendar, and Google Docs
- Currently using NL Mastodon, Cloud86, hugo, OVH.nl, one .nl, one.org, one archival .com, Mailbox email and calendar, and Infomaniak online documents

FOSS and European online services

- In theory, there are lots of FOSS online document editing suites
- In practice, I could not get good enough performance or security from any option available for fewer than 100 licenses
- E.g.: I could get a NextCloud instance hosted in the Netherlands, but online editing was unusably slow and calendar sync was once a week
- Simply buying a service can take days
- Calendaring is a nightmare in general
- Everything is slower, buggier, and harder to use

Moving to FOSS and European online services

- At OW2Con 2024, I heard a lot of “If everyone just…”
  - Switched to an FOSS document suite
  - Donated €20/month to a FOSS project they use
  - Used a FOSS phone
- Everyone is not “just” changing their behavior for good reasons
- Migration is difficult, costly, and the end result is often not as good
- I only did it because I’m sure I will have to eventually, and now is easier

Valerie Aurora, Bow Shock Systems http://bowshock.nl/

You can help migrate services to Europe too

- At some point, the cost of NOT migrating to European hosted/controlled and/or FOSS services WILL be obviously greater than the cost of migrating
- Prepare for your organization realizing this by:
  - Picking out replacement services and products
  - Doing a test migration and documenting the weird parts
  - Writing a migration plan and any necessary scripts or tools
  - Identifying anything that must be done BEFORE the crisis happens

My personal plan to improve internet resiliency

1. Move my online life to European-owned, European-hosted infrastructure
2. Start an Internet Resiliency Club
3. Develop Cyber Resilience Act standards

Starting an Internet Resiliency Club

- What if I could set up up an ad hoc emergency communications network between networking experts that could bootstrap recovery efforts?
- Everyone would have to be a volunteer, so it has to be easy, cheap, and fun
- Must be able to communicate for days with any centralized infrastructure, including power
- Goal is to provide a text message capability for a few days to organize fixing the internet, not provide voice calls or transmit TCP/IP packets
- Ham radio is too difficult, expensive, power-hungry - and overkill

Valerie Aurora, Bow Shock Systems http://bowshock.nl/

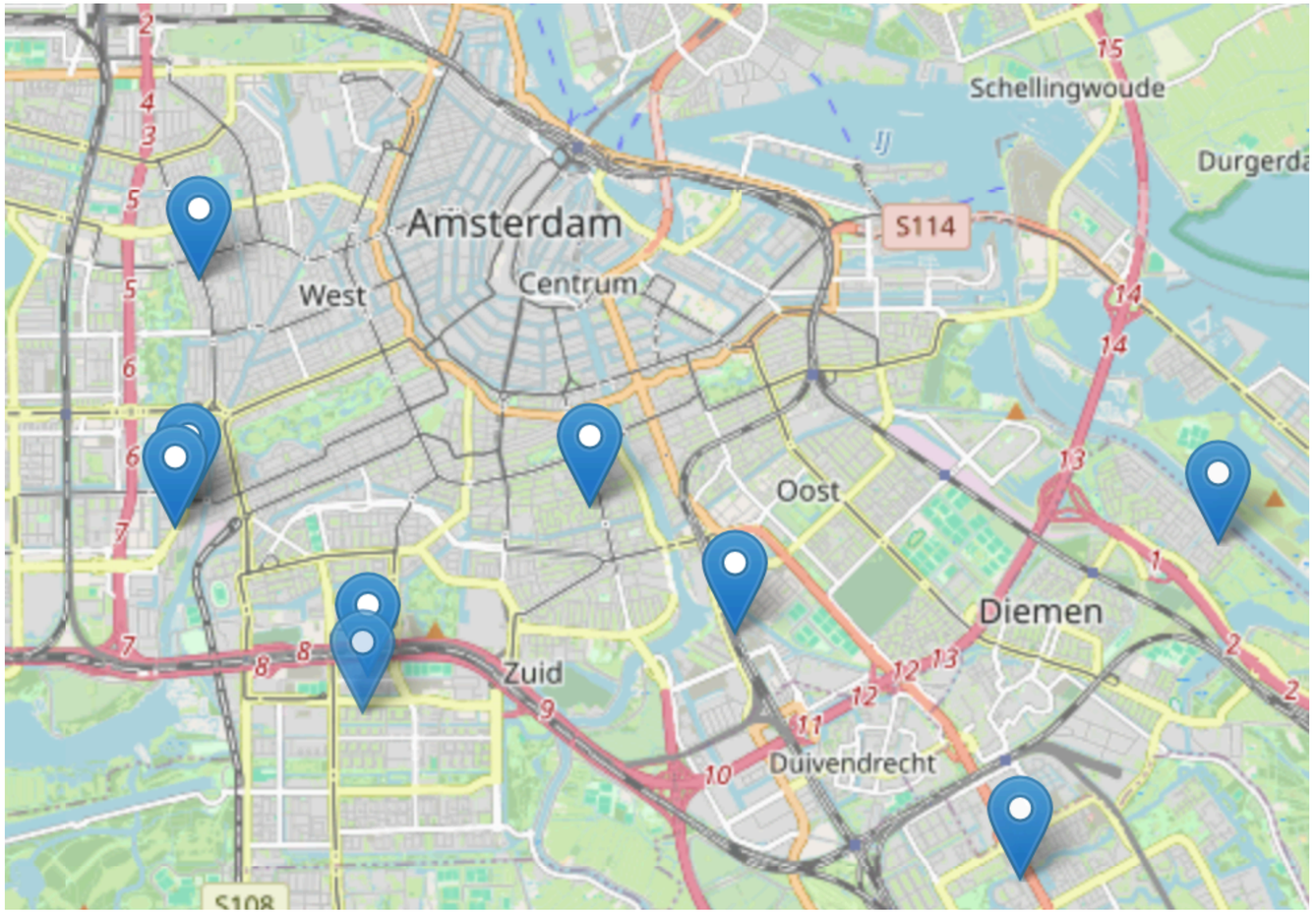
LoRa to the rescue!

- LoRa (Long Range) radios use chirped spread-spectrum to send small short messages to other LoRa radios in line-of-sight
- LoRa radios are cheap (€20), low power (< 1 W), don’t need a license
- Uses Bluetooth or WiFi to connect to phone/computer so you don’t need to pay for or power a separate keyboard or big screen
- Can run for days from an ordinary mobile phone powerbank or with a small solar panel
- Uses so little power that wiring and batteries are trivial

Meshtastic to the rescue!

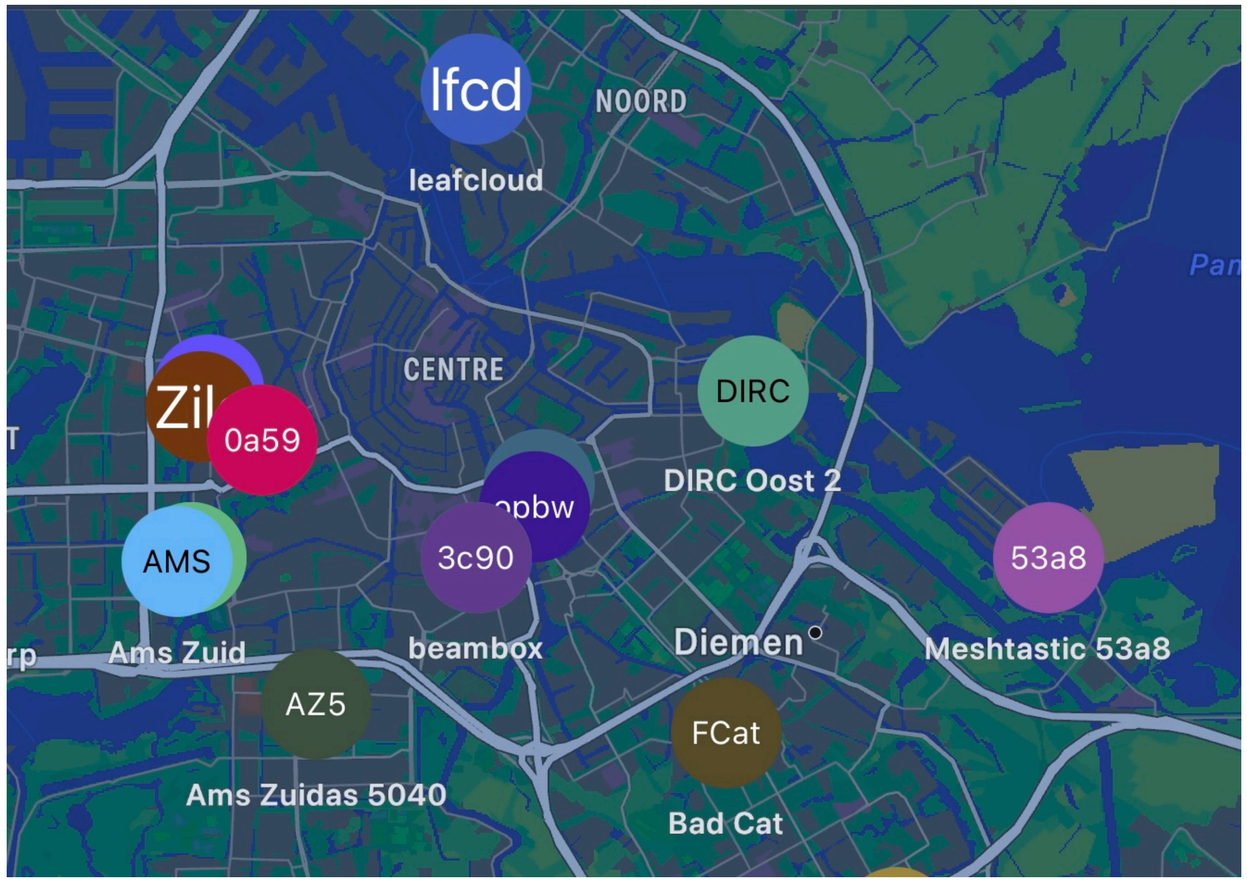
- Install Meshtastic open source firmware to send text messages to other Meshtastic nodes
- Uses simple 3 - 7 hop flood-forward protocol (maybe too simple!)
- Allows multiple encrypted channels to separate traffic
- Already ~2500 nodes in Europe on MeshMap.net (many more unregistered)
- There are other open source LoRa messaging options, such as MeshCore, but Meshtastic is the most popular and has the most coverage

Amsterdam MeshMap



Valerie Aurora, Bow Shock Systems http://bowshock.nl/

Amsterdam nodes in Meshtastic map



Valerie Aurora, Bow Shock Systems http://bowshock.nl/

So I started an Internet Resiliency Club

- Invited fun nice internet-y people to hang out every couple of months
- Established normal comms (Matrix, Signal, mailing list)
- Bulk bought LoRa radios/batteries/solar panels and handed them out
- Picked a LoRa channel to chat, send ASCII art, plan meetups, etc.
- Gave talks at conferences full of people who can fix the internet
- Wrote grant proposals (€10K granted to Waag Futurelab, €45K in progress)
- Now in touch with city of Amsterdam and Dutch Ministry of Defense

Quick start HOWTO

Buy one of:

- More time than money: Heltec V3, ~€20, Bluetooth/WiFi, no battery/GPS
- More money than time: LILYGO T-Echo: ~€80, ~24h battery, Bluetooth, GPS

Just click “Buy” - that’s 90% of the work!

Note that many LoRa devices don’t implement USB-C PD, so you have to connect via USB-A to USB-C to charge properly

IMPORTANT: never power on without the antenna connected or it might fry!

Some of my gear

Valerie Aurora, Bow Shock Systems http://bowshock.nl/

You can start an Internet Resiliency Club too

- You can start a club with:
  - About an hour a week
  - A large personal network
  - Frequent use of https://doodle.com/
- Ask your employer to give LoRa radios and power banks to interested staff members!
- Detailed instructions and non-Amazon European links to purchase hardware:

https://bowshock.nl/irc/

My personal plan to improve internet resiliency

1. Move my online life to European-owned, European-hosted infrastructure
2. Start an Internet Resiliency Club
3. Develop Cyber Resilience Act standards

Developing Cyber Resilience Act standards

- The Cyber Resilience Act essentially applies product safety requirements to anything that can connect to a network (even through a file or a UNIX pipe)
- The initial version was **VERY BAD for FOSS**
- The final version is **VERY GOOD for FOSS** (thank you everyone who did this)
- Non-commercial FOSS has absolutely no obligation or liability under the CRA
- 100% FOSS commercial products can always “self-assess” using any process they like (except for Critical products which always include hardware)
- This is one of many CRA incentives to open source a product!

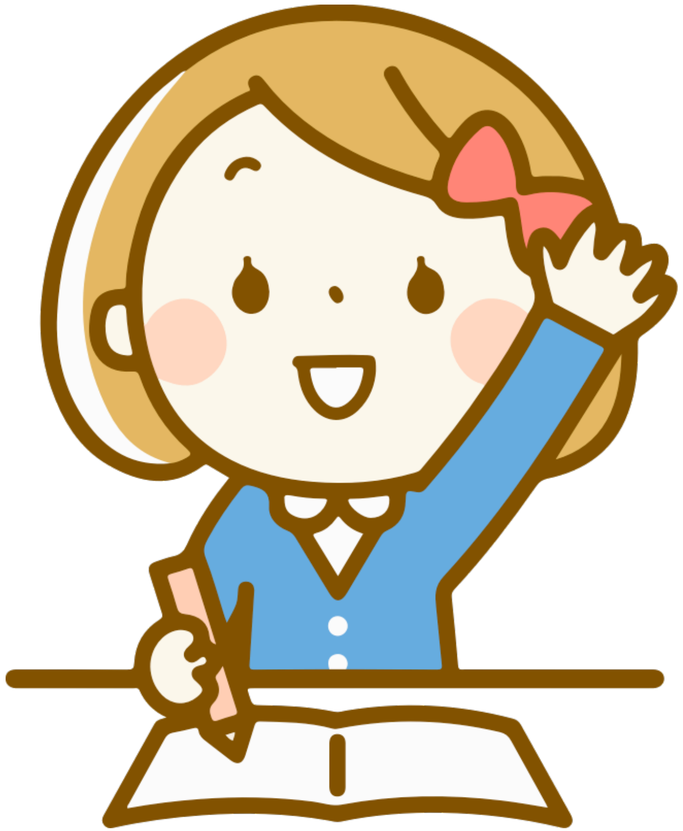
Valerie Aurora, Bow Shock Systems http://bowshock.nl/

CRA creates a funding stream for FOSS

- Organizations trying to make a profit with their product must do “due diligence” on the FOSS parts of their product
- They must also track and fix any vulnerabilities in the FOSS components
- If they write the fix to the vulnerability, they must contribute it upstream to the original FOSS project!
- CRA creates “Open Source Stewards” who can do most of the work for a CRA assessment without any liability, as long as they aren’t “making a profit”
- Open Source Stewards can charge licensing fees for using their work

“But charging money isn’t the FOSS way!”

- Raise your hand if you like doing standards assessment preparation in your spare time
- (Almost) no one will do this for free! You will have to pay them!
- Only organizations who are trying to make a profit need this work!
- The FOSS maintenance crisis is real!
- **Don’t mess this up!!!**



Public Domain OpenClipArt

I’m a special rapporteur!

- “Vertical standards” are simplified standards for CRA compliance focused on a particular type of product
- Allows vendors to self-assess when they otherwise couldn’t and provides “presumption of conformity” (translation: very good if they end up in court)
- The EC is funding FOSS experts to lead the development of many of the vertical standards
- Bow Shock is leading Operating Systems, Network Interfaces, VPNs, Network Management Systems, and Security Information and Event Management

Welcome to standards world

- The three European Standards Organizations (ESOs) by default get to write EC-mandated standards: CEN, CENELEC, and ETSI
- But they are used to writing standards that:
  - Are bottom-up - manufacturers WANT them for interoperability
  - Focused on hardware and telecom
  - Take ~5 years to develop
- Crisis element #3: change in processes or outcome

This work is my love letter to the EU

- Work on verticals didn’t start till June 2025 and are due 6 months later :(
- Most vertical rapporteurs are writing the majority of their standards :(
- I hate standards work and hope I never do it again
- But if the CRA works, we will have more security, software freedom, freedom of use for consumers => more European independence and digital resilience

And that’s why I have worked every weekend since June 🤡

You can help the CRA standards too

- Best way to help: follow me on the fediverse and filter for #CRA @vaurora@mstdn.social
- Comment at https://labs.etsi.org/rep/stan4cra
- Ask your employer to become an ETSI member (surprisingly cheap) https://www.etsi.org/membership/dues
- You can be an ETSI delegate for free if you represent a FOSS project
- Get paid €450/day to contribute https://cyberstand.eu/9th-specific-service-procedure

How you can help digital resilience in Europe

- Prepare for when the crisis arrives!
- Move to European/FOSS services: https://european-alternatives.eu/
- Start your own Internet Resiliency Club: https://bowshock.nl/irc/
- Help develop CRA standards: https://labs.etsi.org/rep/stan4cra
- Follow me on the fediverse: @vaurora@mstdn.social