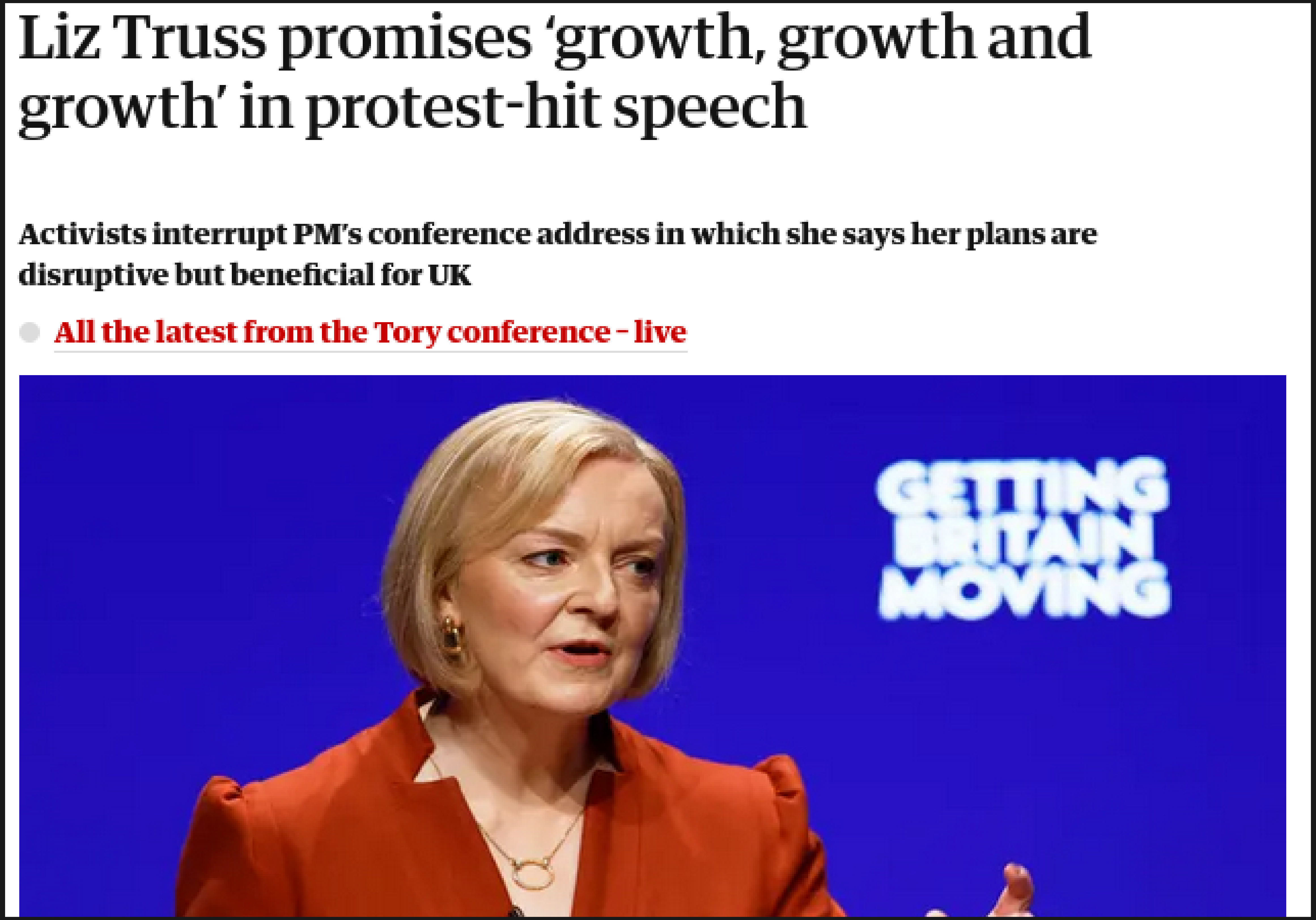
COMPLEXITY KILLED THE CAT

RENÉ „LYNX“ PFEIFFER

DEEPSEC IN-DEPTH SECURITY CONFERENCE 2022

EVERYTHING IS BASED ON GROWTH



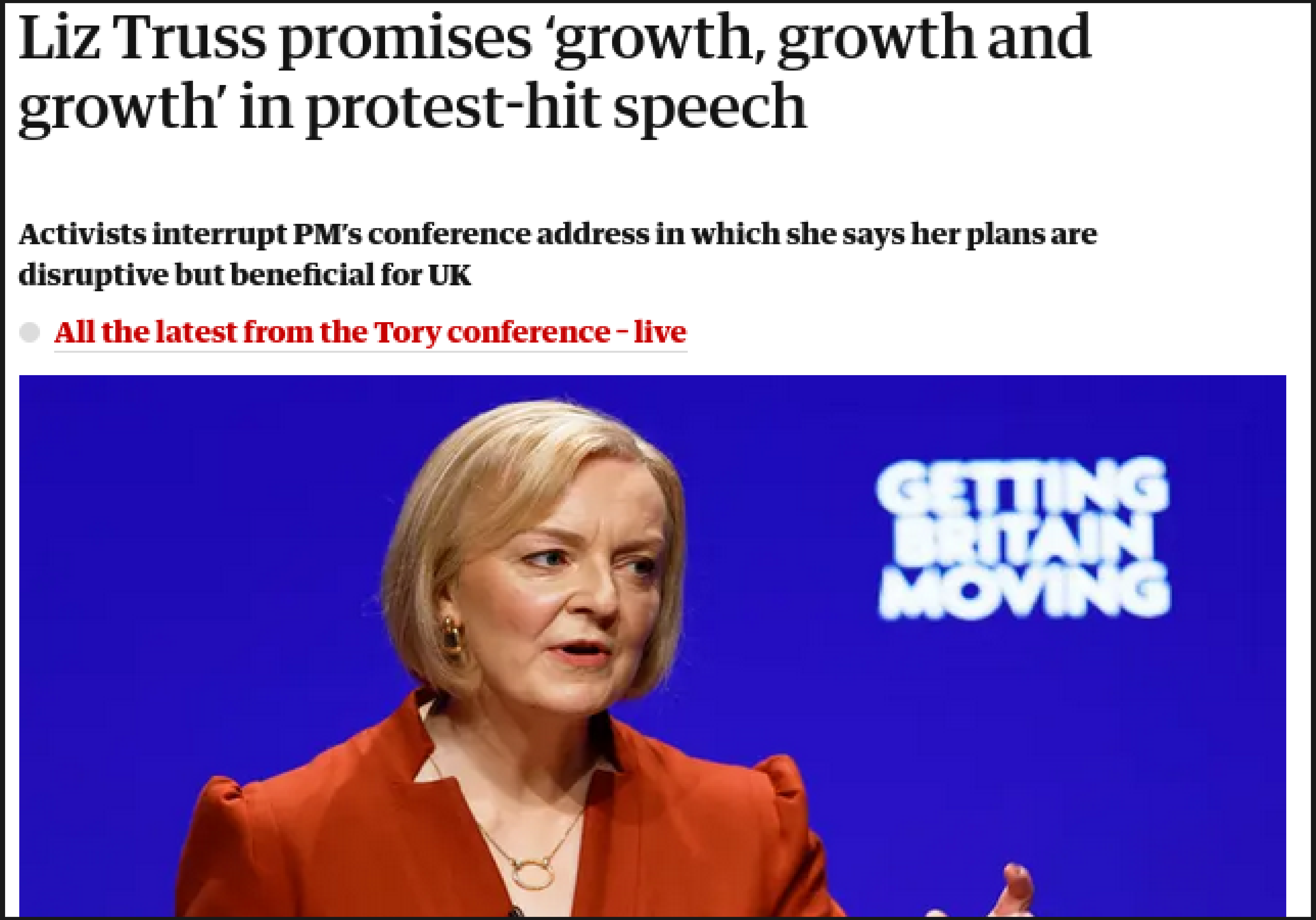
Liz Truss promises 'growth, growth and growth' in protest-hit speech

Activists interrupt PM's conference address in which she says her plans are disruptive but beneficial for UK

● All the latest from the Tory conference - live

Source: The Guardian

EVERYTHING IS BASED ON GROWTH



Liz Truss promises 'growth, growth and growth' in protest-hit speech

Activists interrupt PM's conference address in which she says her plans are disruptive but beneficial for UK

- **All the latest from the Tory conference – live**

Source: The Guardian

IT CAN RELATE TO GROWTH

```
am-id. hello-world.

dure division.
play "Hello, World!"

ack
```

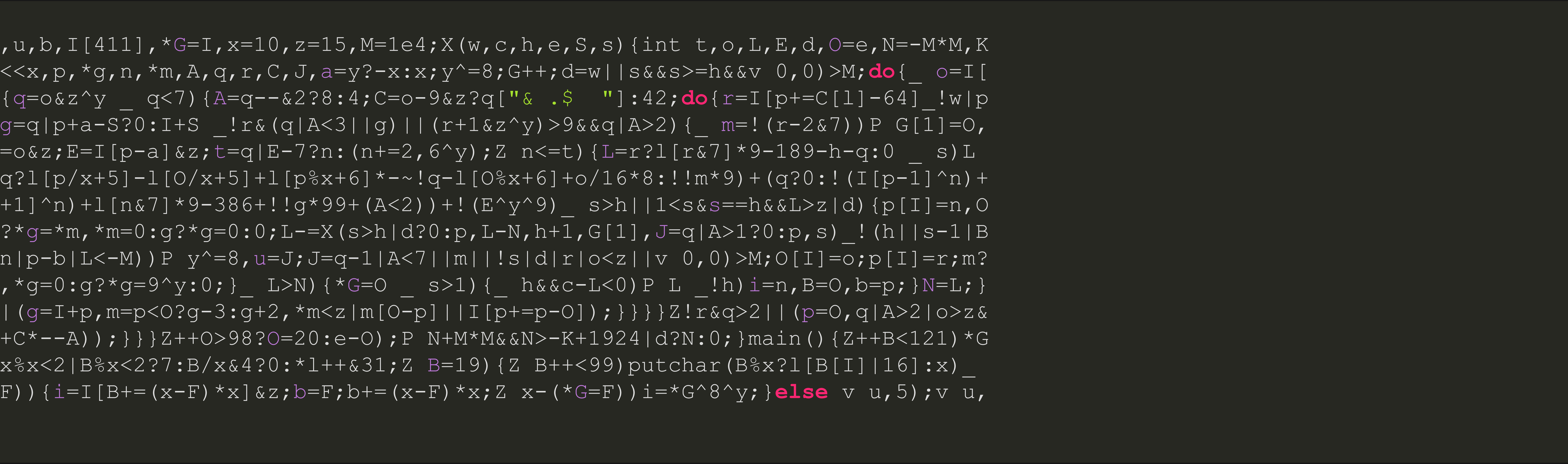
Code grows over time (source Rosetta Code).

IT CAN RELATE TO GROWTH (2)

```
sage:       .asciz "Hello world. \n"
LGMESSAGE, . -  szMessage  // compute length of message

al main

ov x0,1                    // output std linux
dr x1,qAdrMessage          // adresse of message
ov x2,LGMESSAGE            // sizeof(message)
ov x8,64                   // select system call 'write'
vc 0                       // perform the system call

ov x0, 0                   // return code
ov x8,93                   // select system call 'exit'
vc 0                       // perform the system call
essage:       .quad szMessage
```

Code expands to other programming languages (source Rosetta Code).

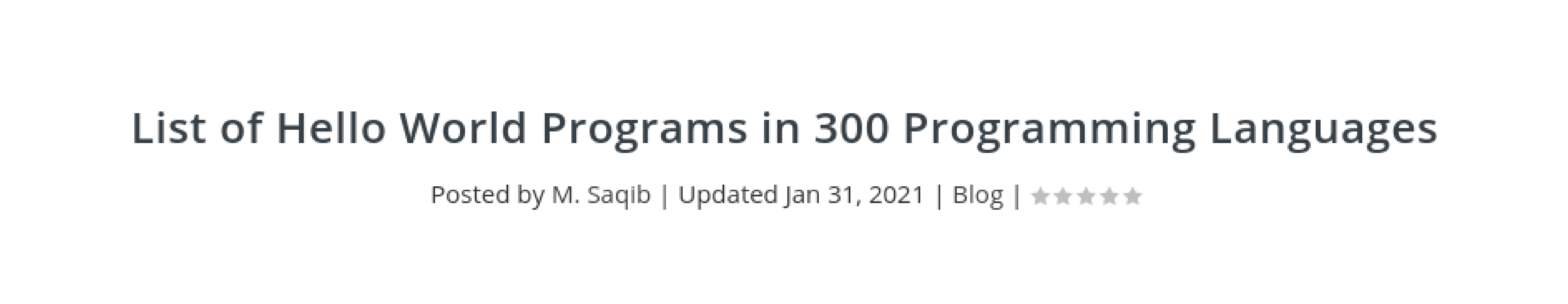
IT CAN RELATE TO GROWTH (3)



```
,u,b,I[411],*G=I,x=10,z=15,M=1e4;X(w,c,h,e,S,s){int t,o,L,E,d,O=e,N=-M*M,K
<<x,p,*g,n,*m,A,q,r,C,J,a=y?-x:x;y^=8;G++;d=w||s&&s>=h&&v 0,0)>M;do{_ o=I[
{q=o&z^y _ q<7){A=q--&2?8:4;C=o-9&z?q["&  .$   "]:42;do{r=I[p+=C[l]-64]_!w|p
g=q|p+a-S?0:I+S _!r&(q|A<3||g)||(r+1&z^y)>9&&q|A>2){_ m=!(r-2&7))P G[1]=O,
=o&z;E=I[p-a]&z;t=q|E-7?n:(n+=2,6^y);Z n<=t){L=r?l[r&7]*9-189-h-q:0 _ s)L
q?l[p/x+5]-l[O/x+5]+l[p%x+6]*-~!q-l[O%x+6]+o/16*8:!!m*9)+(q?0:!(I[p-1]^n)+
+1]^n)+l[n&7]*9-386+!!g*99+(A<2))+!(E^y^9)_ s>h||1<s&s==h&&L>z|d){p[I]=n,O
?*g=*m,*m=0:g?*g=0:0;L-=X(s>h|d?0:p,L-N,h+1,G[1],J=q|A>1?0:p,s)_!(h||s-1|B
n|p-b|L<-M))P y^=8,u=J;J=q-1|A<7||m||!s|d|r|o<z||v 0,0)>M;O[I]=o;p[I]=r;m?
,*g=0:g?*g=9^y:0;}_ L>N){*G=O _ s>1){_ h&&c-L<0)P L _!h)i=n,B=O,b=p;}N=L;}
|(g=I+p,m=p<O?g-3:g+2,*m<z|m[O-p]||I[p+=p-O]);}}}}Z!r&q>2||(p=O,q|A>2|o>z&
+C*--A));}}}Z++O>98?O=20:e-O);P N+M*M&&N>-K+1924|d?N:0;}main(){Z++B<121)*G
x%x<2|B%x<2?7:B/x&4?0:*l++&31;Z B=19){Z B++<99)putchar(B%x?l[B[I]|16]:x)_
F)){i=I[B+=(x-F)*x]&z;b=F;b+=(x-F)*x;Z x-(*G=F))i=*G^8^y;}else v u,5);v u,
```

Code can become more complex (source IOCCC).

VARIATIONS



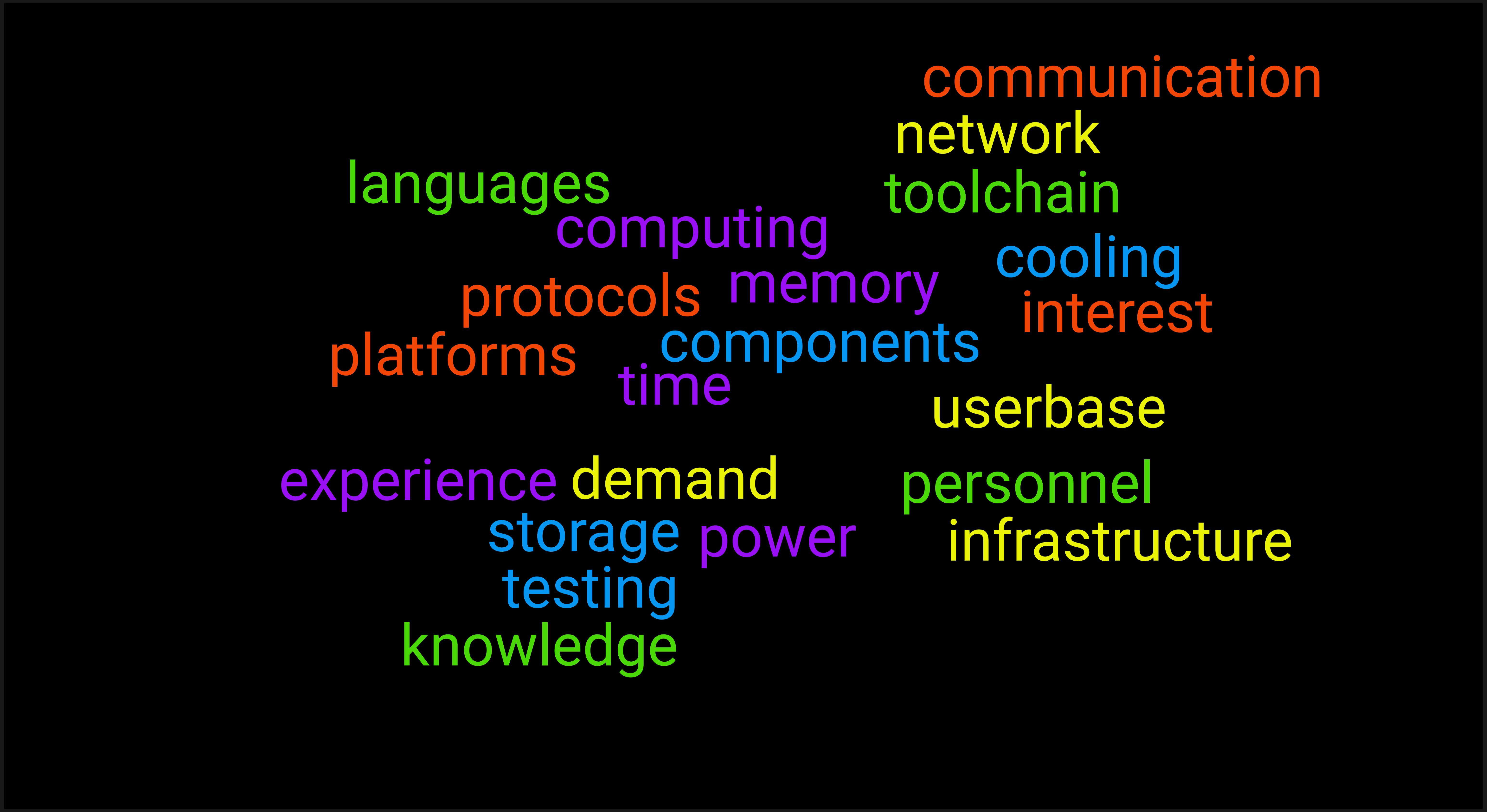
List of Hello World Programs in 300 Programming Languages

Posted by M. Saqib | Updated Jan 31, 2021 | Blog | ☆☆☆☆☆

Source: List of Hello World Programs in 300 Programming Languages

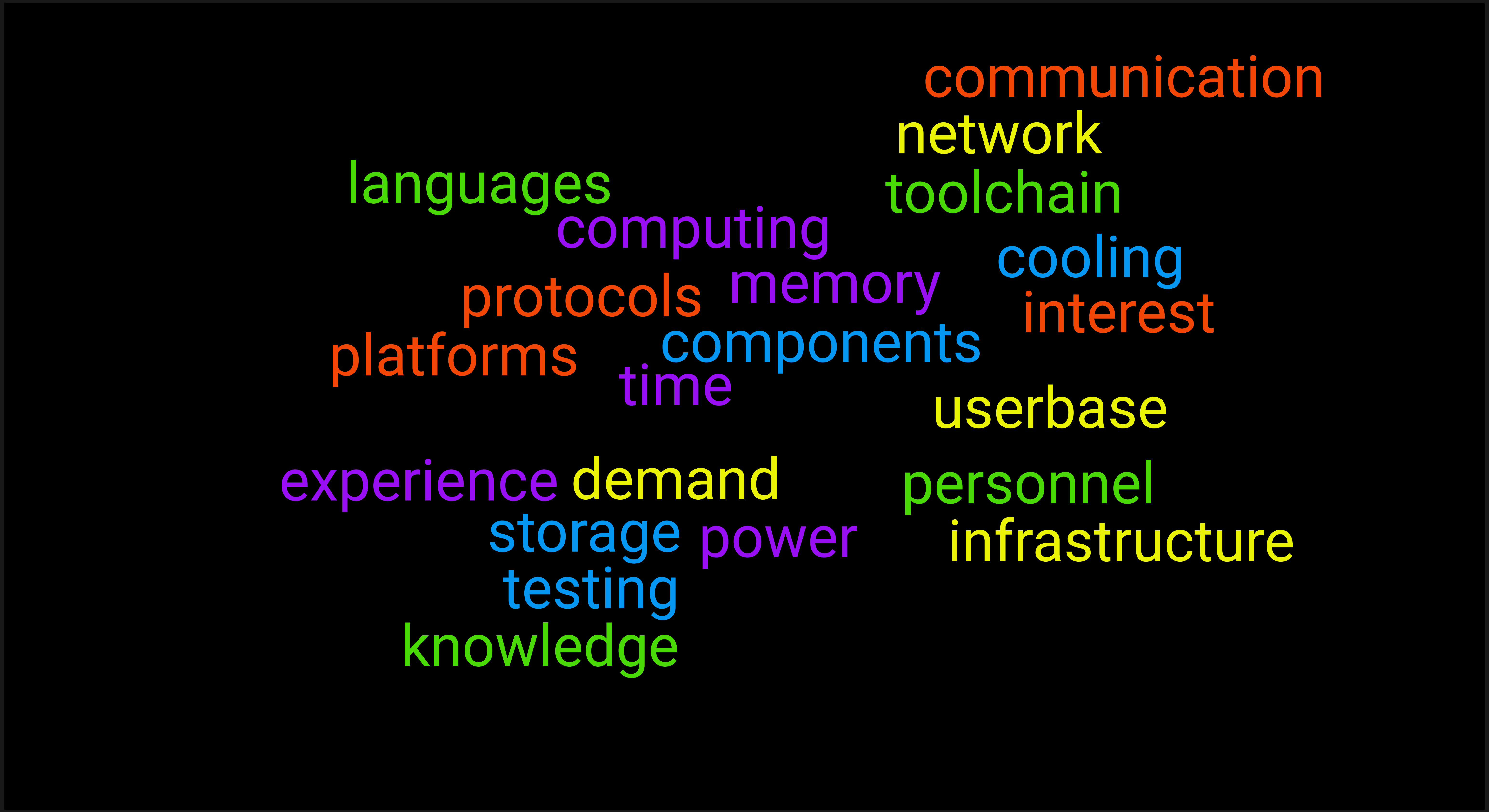
PREREQUISITES

PREREQUISITES



communication
network
languages
toolchain
computing
cooling
protocols memory
interest
platforms
components
time
userbase
experience demand
personnel
storage power
infrastructure
testing
knowledge

PREREQUISITES



Let's keep this in mind.

GROWTH AND PROSPERITY

GROWTH AND PROSPERITY

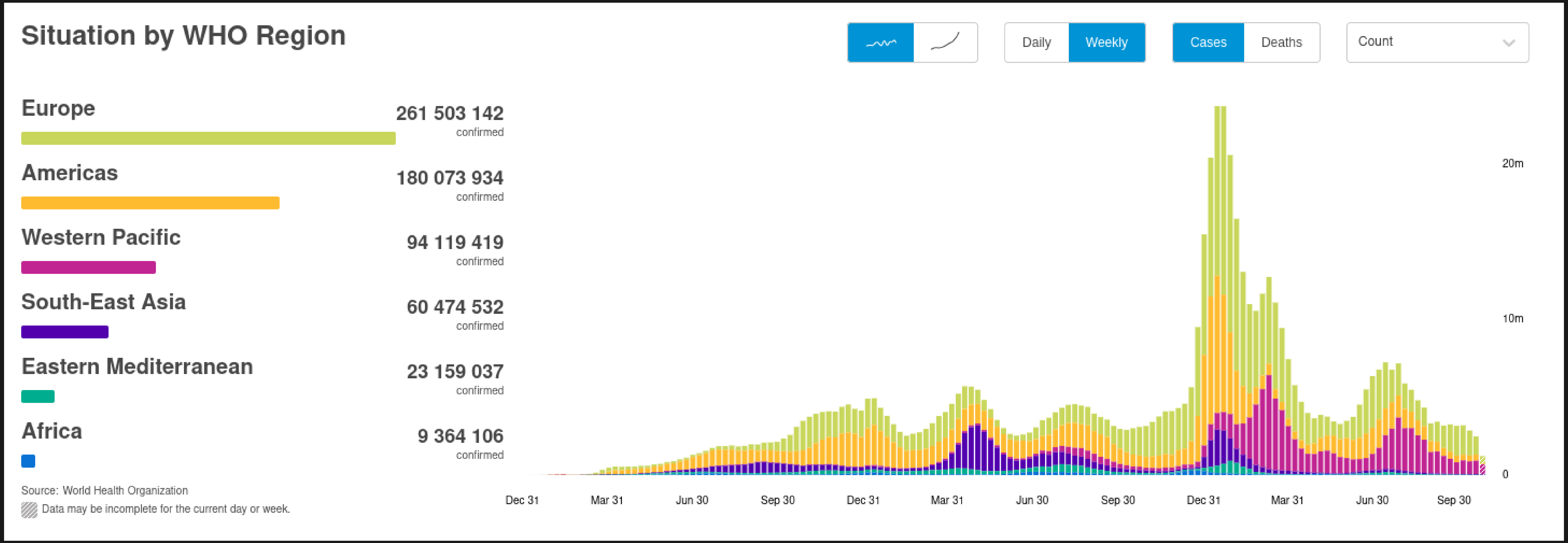
If everything (?) is based on growth, where is the problem?

GROWTH AND PROSPERITY

If everything (?) is based on growth, where is the problem?

Limits! Or limiting factors.

COVID-19 CASES



Situation by WHO Region

Europe	261 503 142 confirmed
Americas	180 073 934 confirmed
Western Pacific	94 119 419 confirmed
South-East Asia	60 474 532 confirmed
Eastern Mediterranean	23 159 037 confirmed
Africa	9 364 106 confirmed

Source: World Health Organization

▨ Data may be incomplete for the current day or week.

Source: WHO

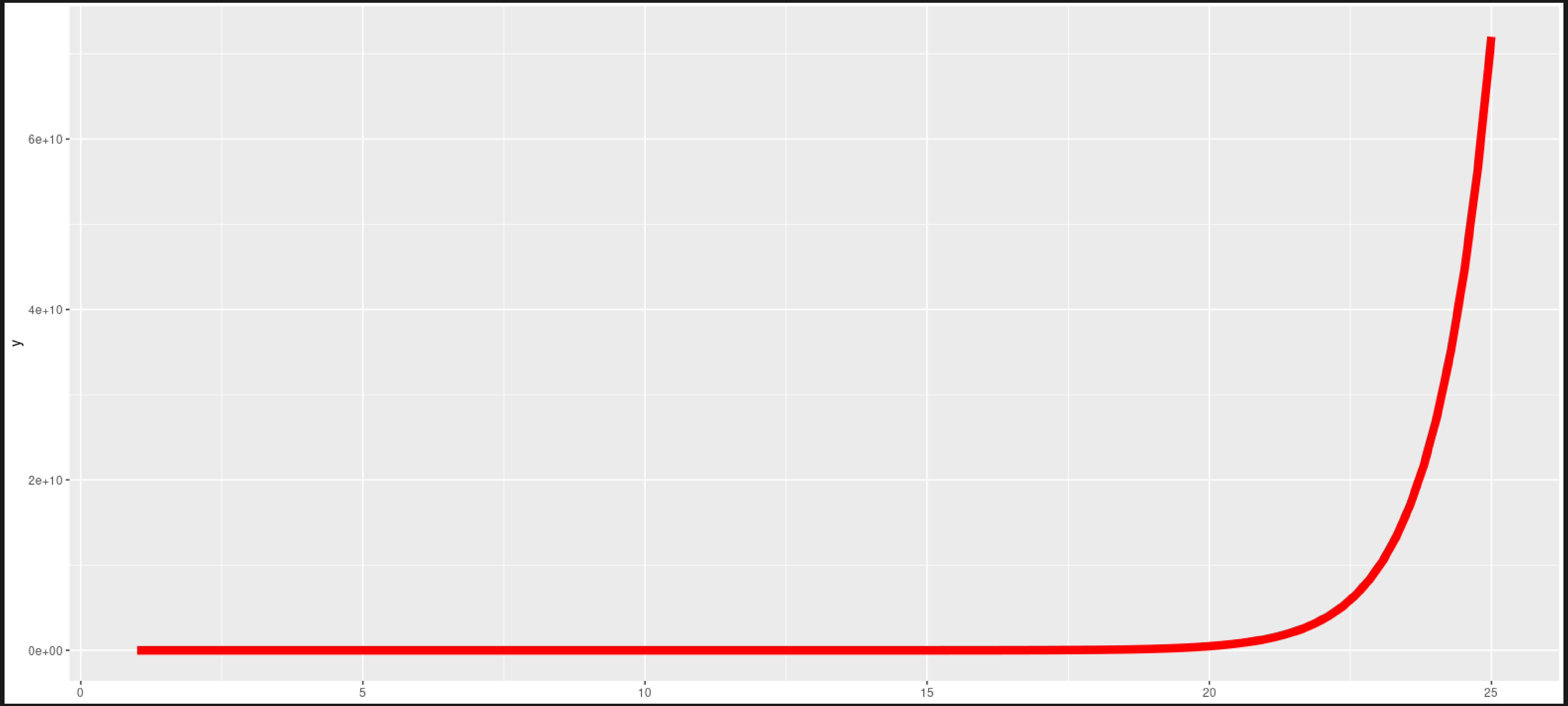
EXPONENTIAL FUNCTION

EXPONENTIAL FUNCTION

„Well-known“ since COVID-19…

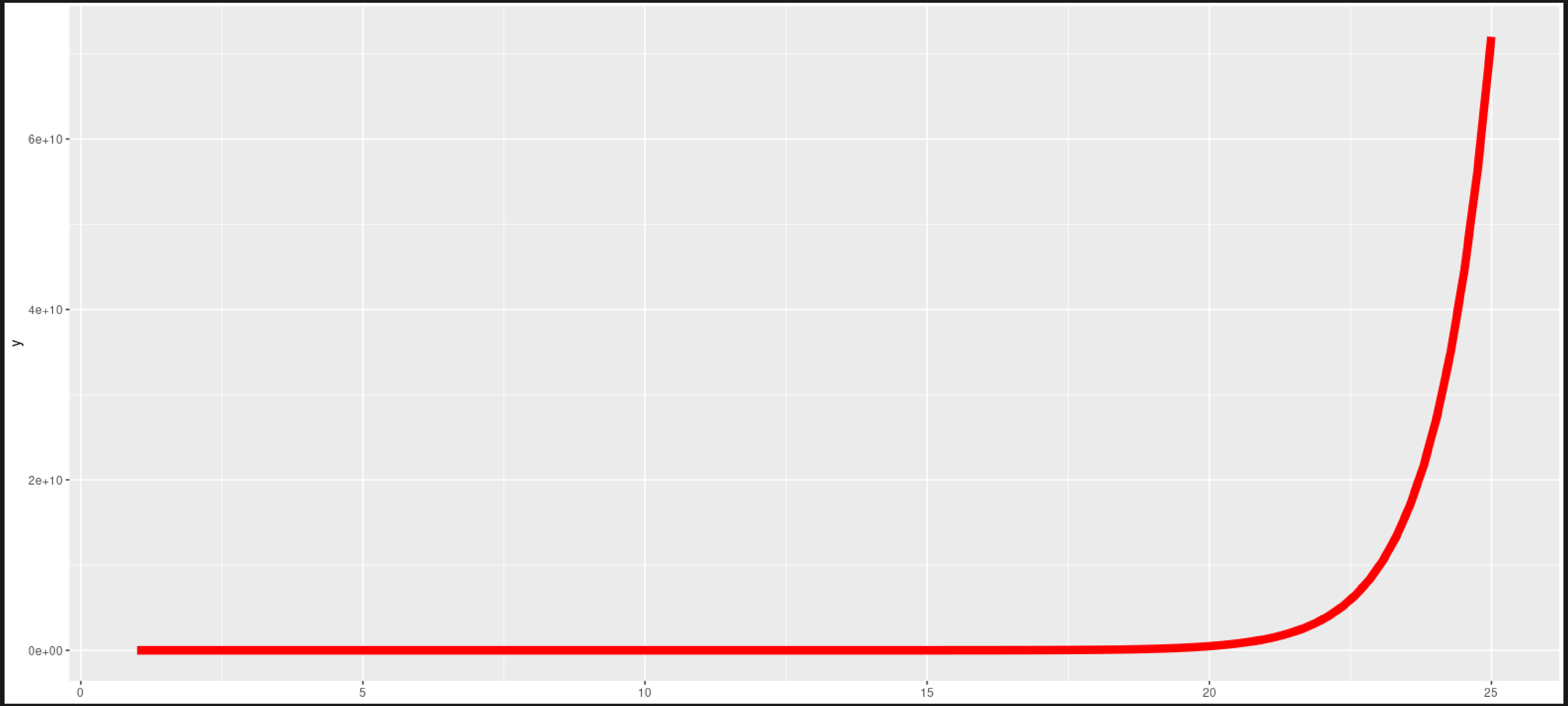
EXPONENTIAL FUNCTION

„Well-known“ since COVID-19…



EXPONENTIAL FUNCTION

„Well-known“ since COVID-19…



Pure exponential growth has no limiting factors.

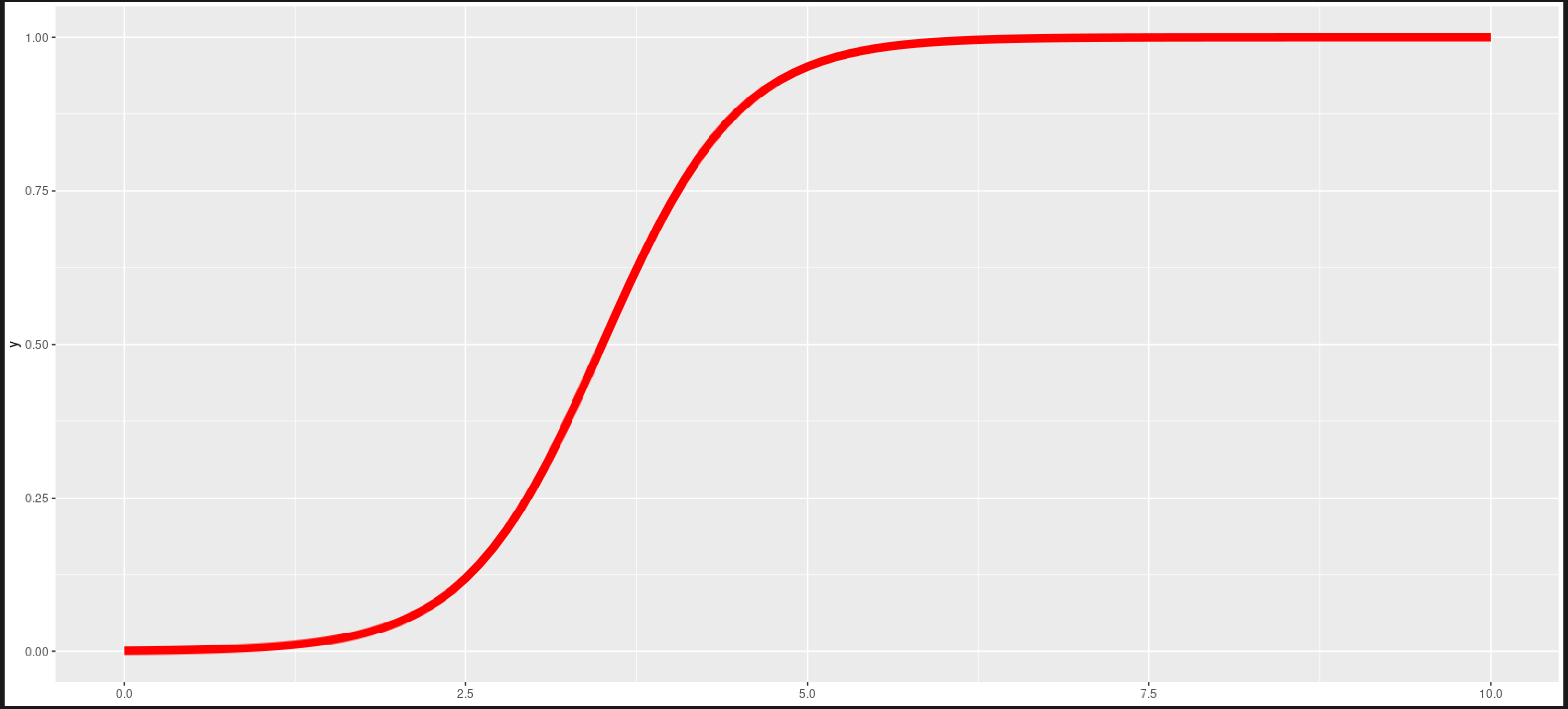
LOGISTICS FUNCTION

LOGISTICS FUNCTION

„Limitless“ growth with limits looks like this:

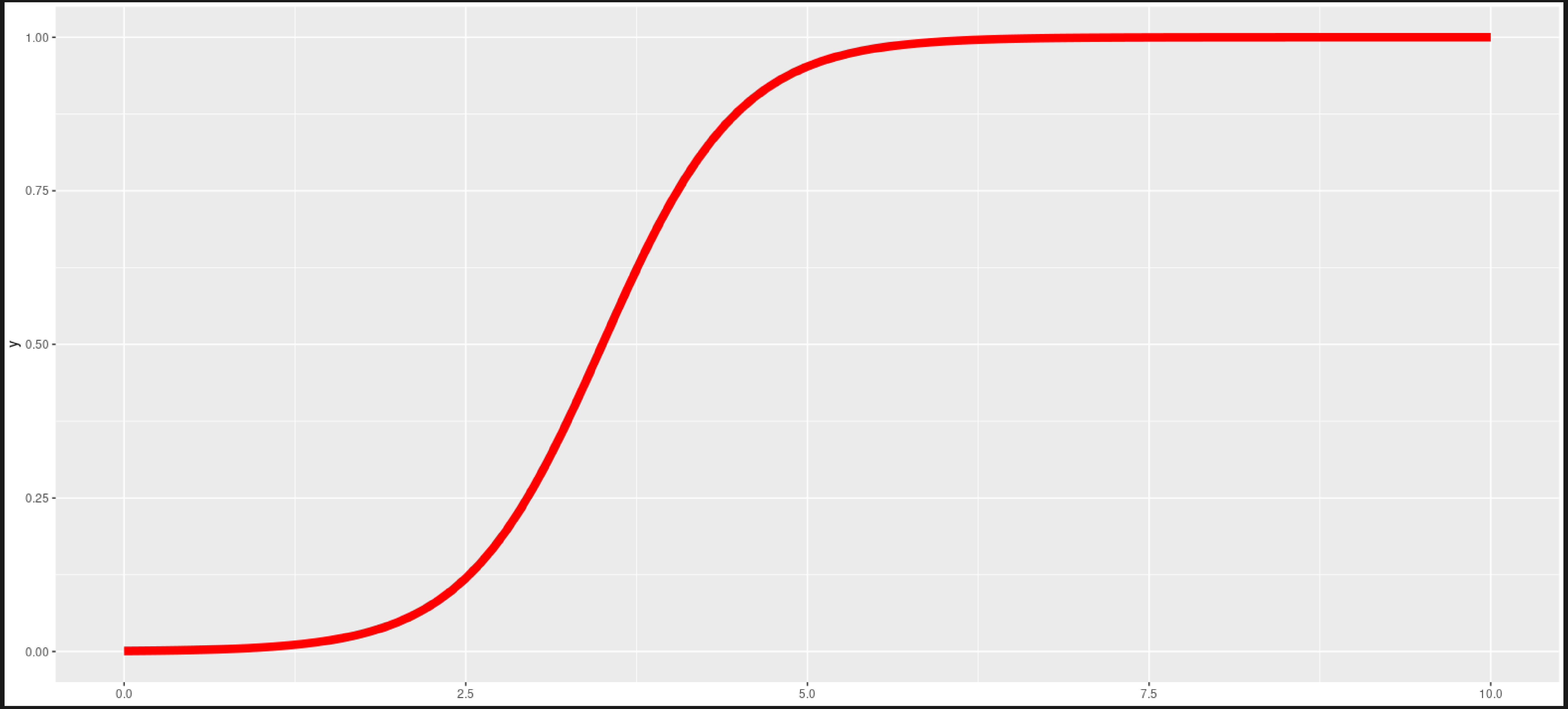
LOGISTICS FUNCTION

„Limitless“ growth with limits looks like this:



LOGISTICS FUNCTION

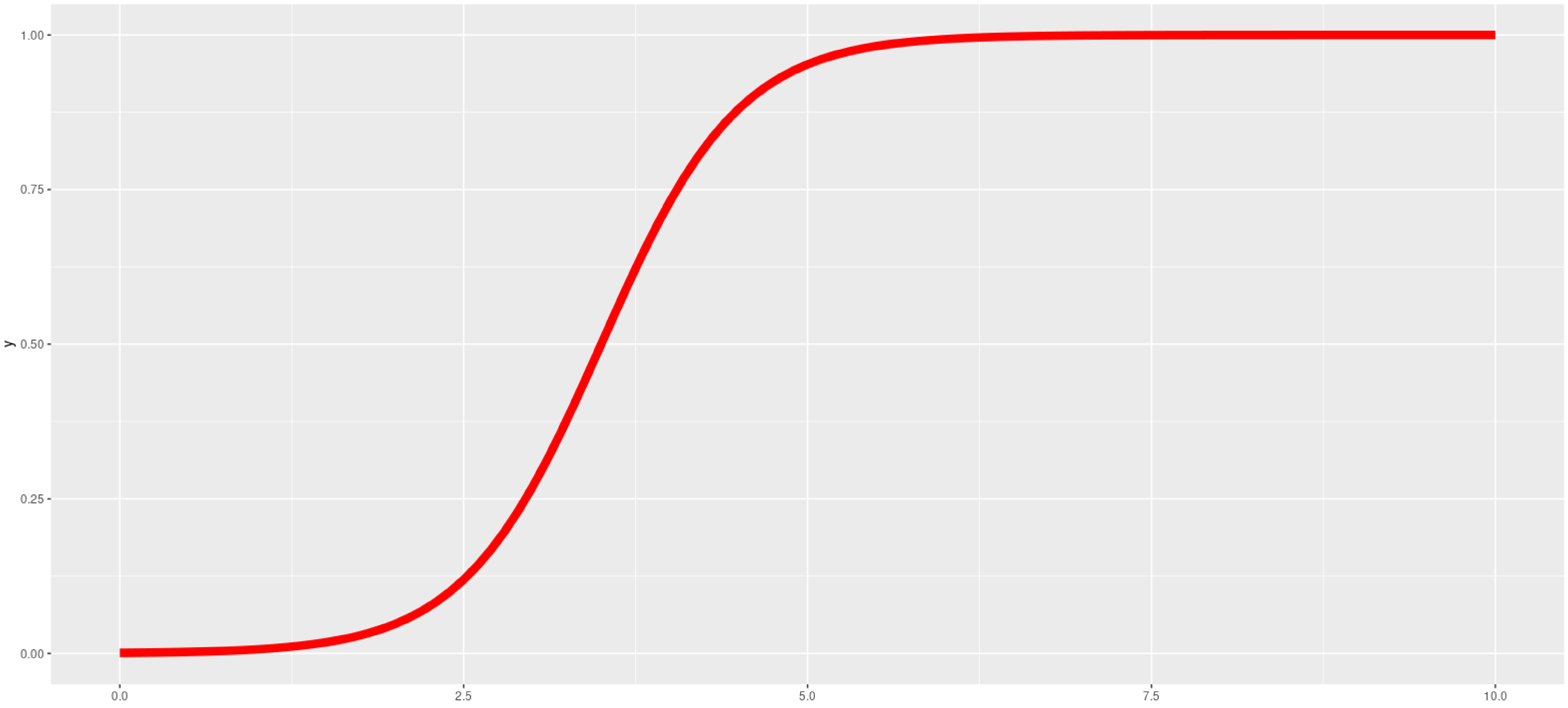
„Limitless“ growth with limits looks like this:



Economists and investors hate this function and often ignore it.

LOGISTICS FUNCTION

„Limitless“ growth with limits looks like this:



Economists and investors hate this function and often ignore it.

(Moore's Law has not yet encountered „hard“ limits…)

ENTER THE HUMAN MIND

ENTER THE HUMAN MIND

BACK TO COMPLEXITY

BACK TO COMPLEXITY

Complexity „just happens“ (subjectively)…

BACK TO COMPLEXITY

Complexity „just happens“ (subjectively)…

…but is is created because of limitations.

ENTER THE MACHINE'S MIND

ENTER THE MACHINE'S MIND

int, float, char, boolean, String

ENTER THE MACHINE'S MIND

int, float, char, boolean, String

int, long, short, char, long long, float, double, bool, void *

ENTER THE MACHINE'S MIND

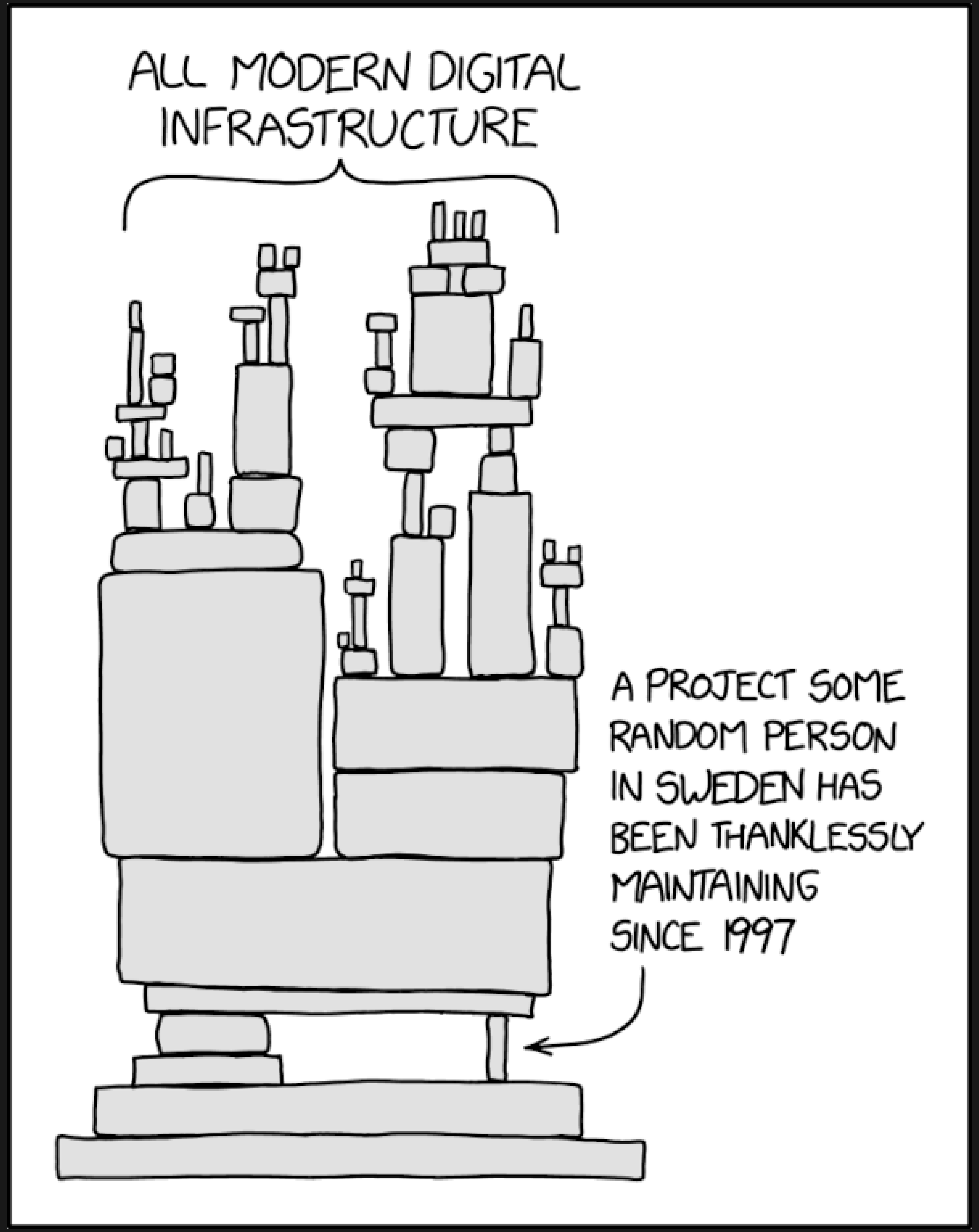
int, float, char, boolean, String

int, long, short, char, long long, float, double, bool, void *

Machines „think“ differently.

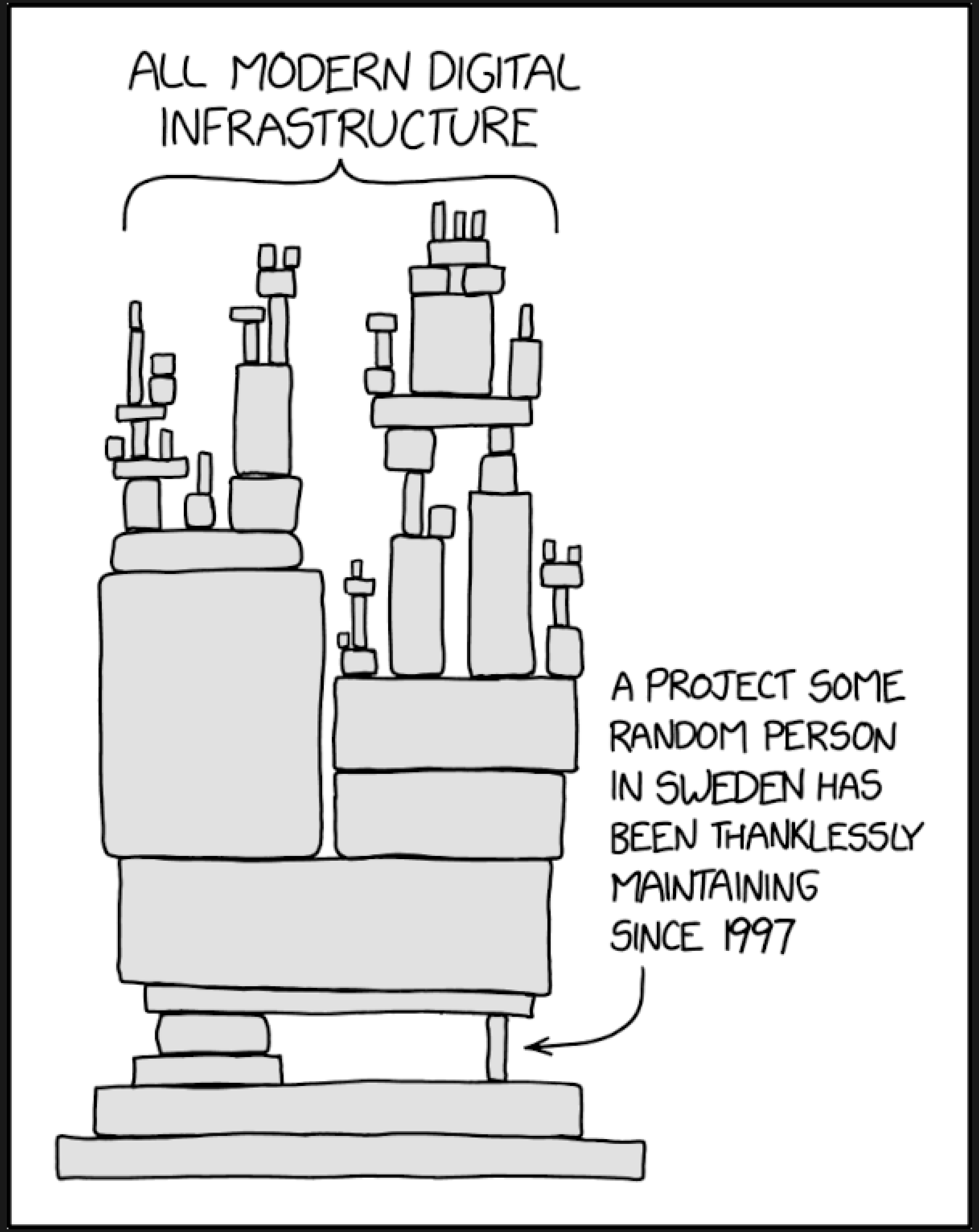
COMPLEXITY

COMPLEXITY


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN SWEDEN HAS BEEN THANKLESSLY MAINTAINING SINCE 1997

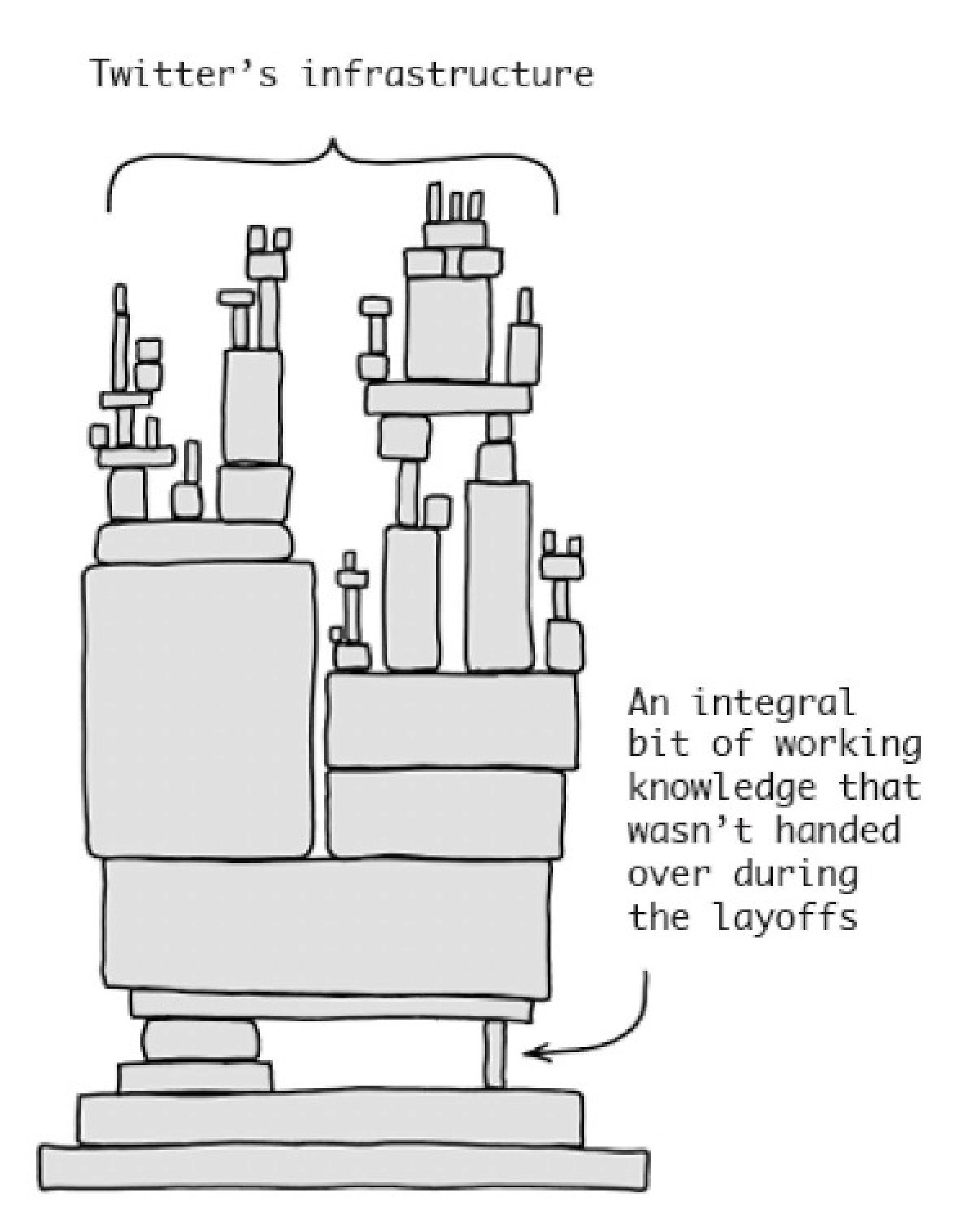
COMPLEXITY

Yes, it's curl / libcurl!


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN SWEDEN HAS BEEN THANKLESSLY MAINTAINING SINCE 1997

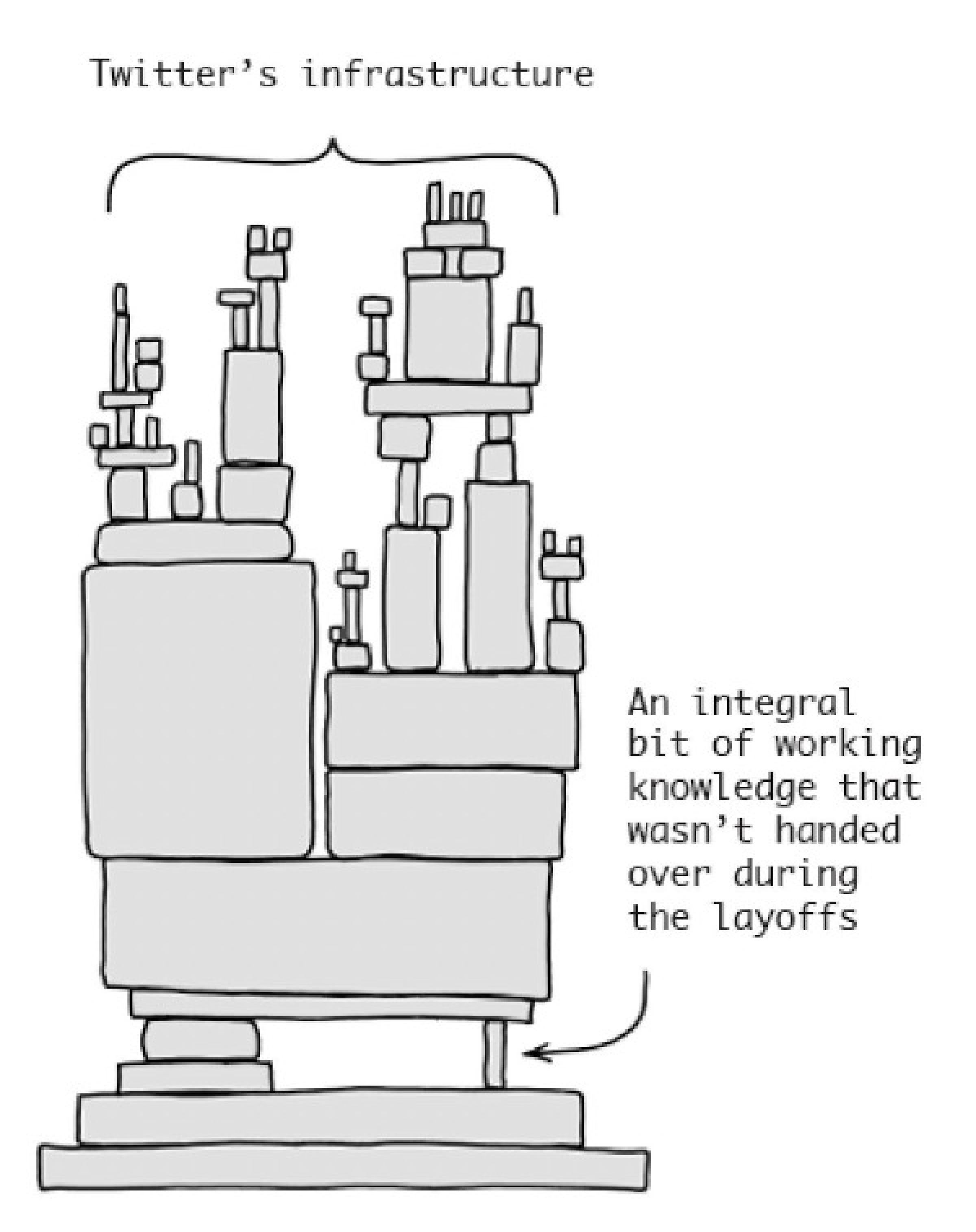
COMPLEXITY

COMPLEXITY


Twitter's infrastructure
An integral bit of working knowledge that wasn't handed over during the layoffs

COMPLEXITY

Could be any other (tech) company!


Twitter's infrastructure
An integral bit of working knowledge that wasn't handed over during the layoffs

WHY DOES THIS HAPPEN?

WHY DOES THIS HAPPEN?

Developer
Npm packages
Project

LIBRARIES ARE GREAT!

LIBRARIES ARE GREAT!

One does not simply walk into Mordor with one's own libcrypto.

LIBRARIES ARE GREAT!

One does not simply walk into Mordor with one's own libcrypto.

With great package managers comes great responsibility!

LIBRARIES ARE GREAT!

One does not simply walk into Mordor with one's own libcrypto.

With great package managers comes great responsibility!

Selection of components vary from conservative to 50 packages per second.

COMPLEXITY RELOADED

COMPLEXITY RELOADED

Complexity is not exclusively tied to software development.

COMPLEXITY RELOADED

Complexity is not exclusively tied to software development.

Data Loss Prevention (DLP) means you know **all data** of your organisation.

COMPLEXITY RELOADED

Complexity is not exclusively tied to software development.

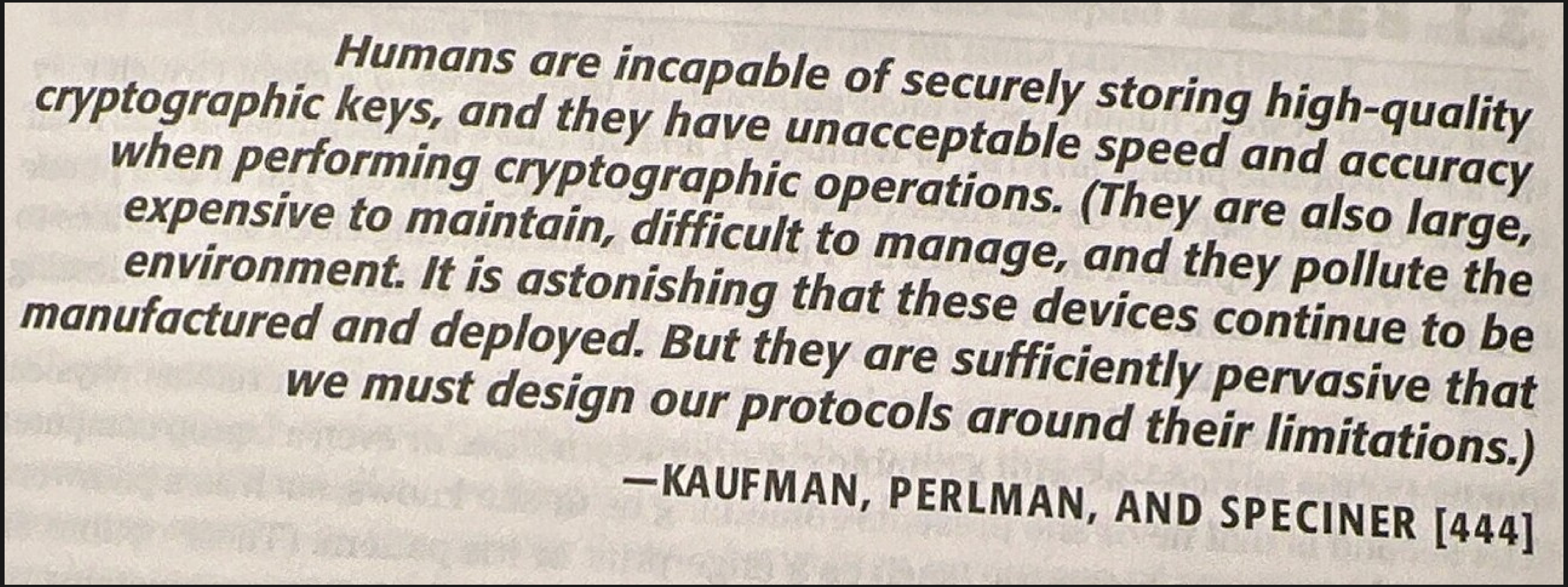
Data Loss Prevention (DLP) means you know **all data** of your organisation.

Do you?

INFORMATION TECHNOLOGY

Source: Network Security: Private Communication in a Public World

INFORMATION TECHNOLOGY

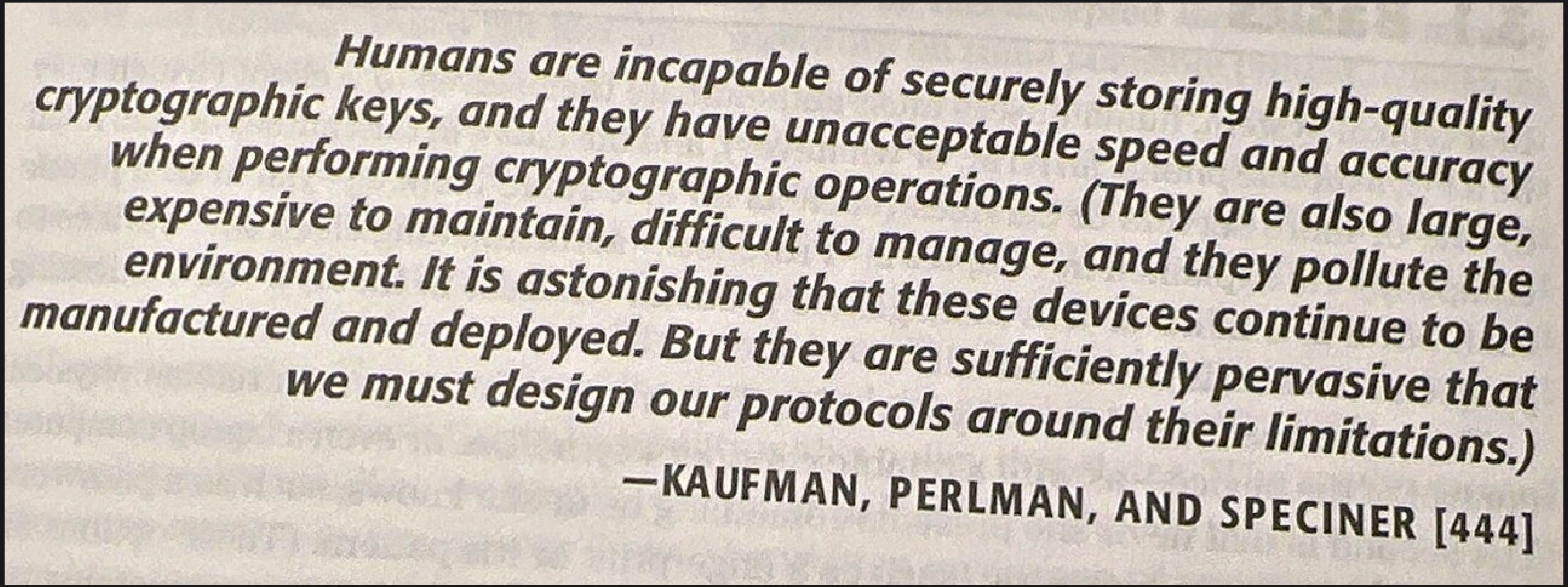


Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)

—KAUFMAN, PERLMAN, AND SPECINER [444]

Source: Network Security: Private Communication in a Public World

INFORMATION TECHNOLOGY



> *Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)*
>
> —KAUFMAN, PERLMAN, AND SPECINER [444]

IT has to deal with complexity. And humans!

Source: Network Security: Private Communication in a Public World

KEEP IT SIMPLE(, STUPID) (KISS)

KEEP IT SIMPLE(, STUPID) (KISS)

Origin in Lockheed Skunk Works (U-2, SR-71)…

KEEP IT SIMPLE(, STUPID) (KISS)

Origin in Lockheed Skunk Works (U-2, SR-71)…

…or the 1938 issue of the Minneapolis Star.

KEEP IT SIMPLE(, STUPID) (KISS)

Origin in Lockheed Skunk Works (U-2, SR-71)…

…or the 1938 issue of the Minneapolis Star.

Often cited, not self-evident, hard to implement, always misunderstood.

KEEP IT SIMPLE (2)

KEEP IT SIMPLE (2)

You can have complex objects, but…

KEEP IT SIMPLE (2)

You can have complex objects, but…

…these objects must be easy to fix (in the „field“ = „in production“).

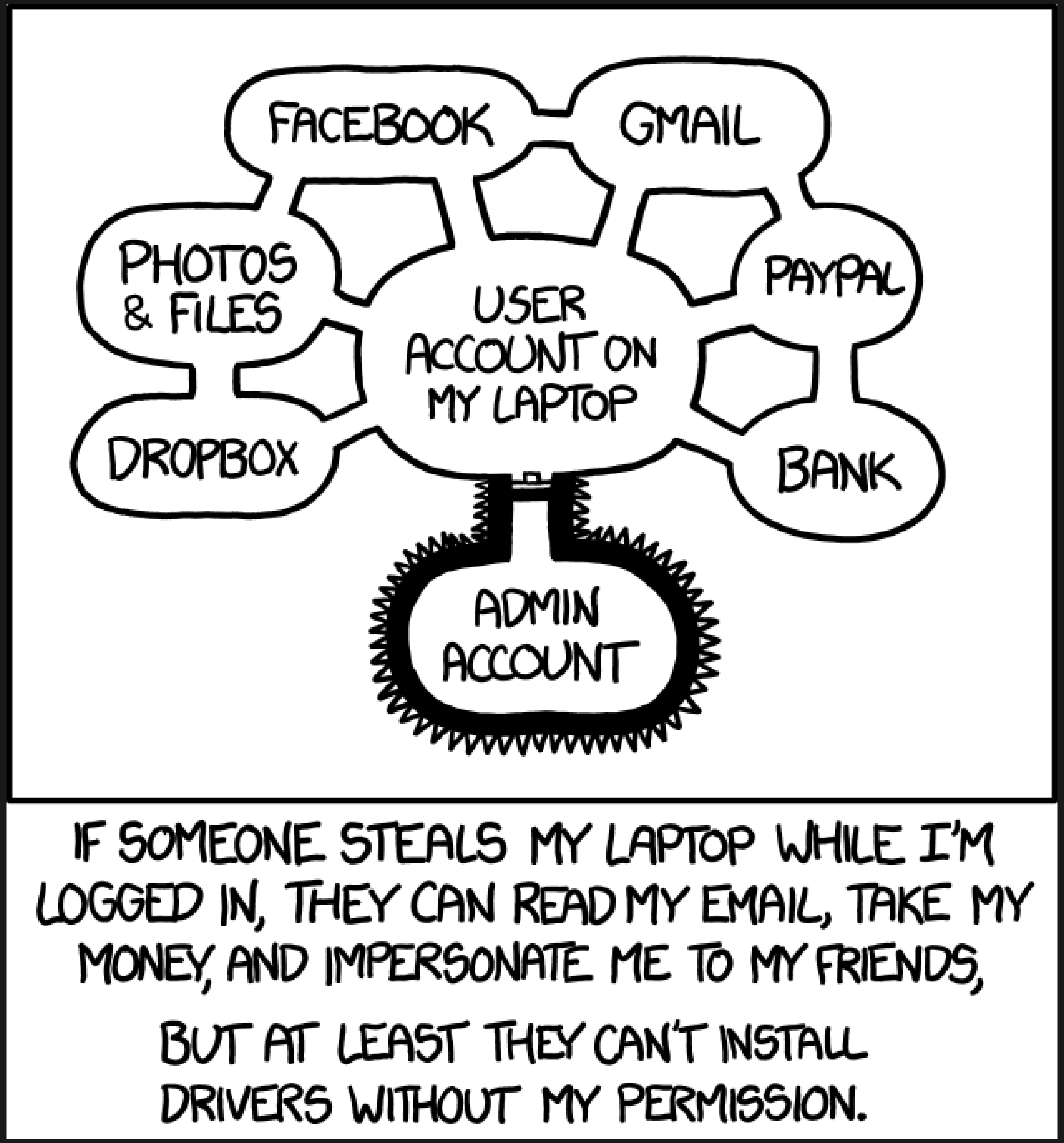
KEEP IT SIMPLE (2)

You can have complex objects, but…

…these objects must be easy to fix (in the „field“ = „in production“).

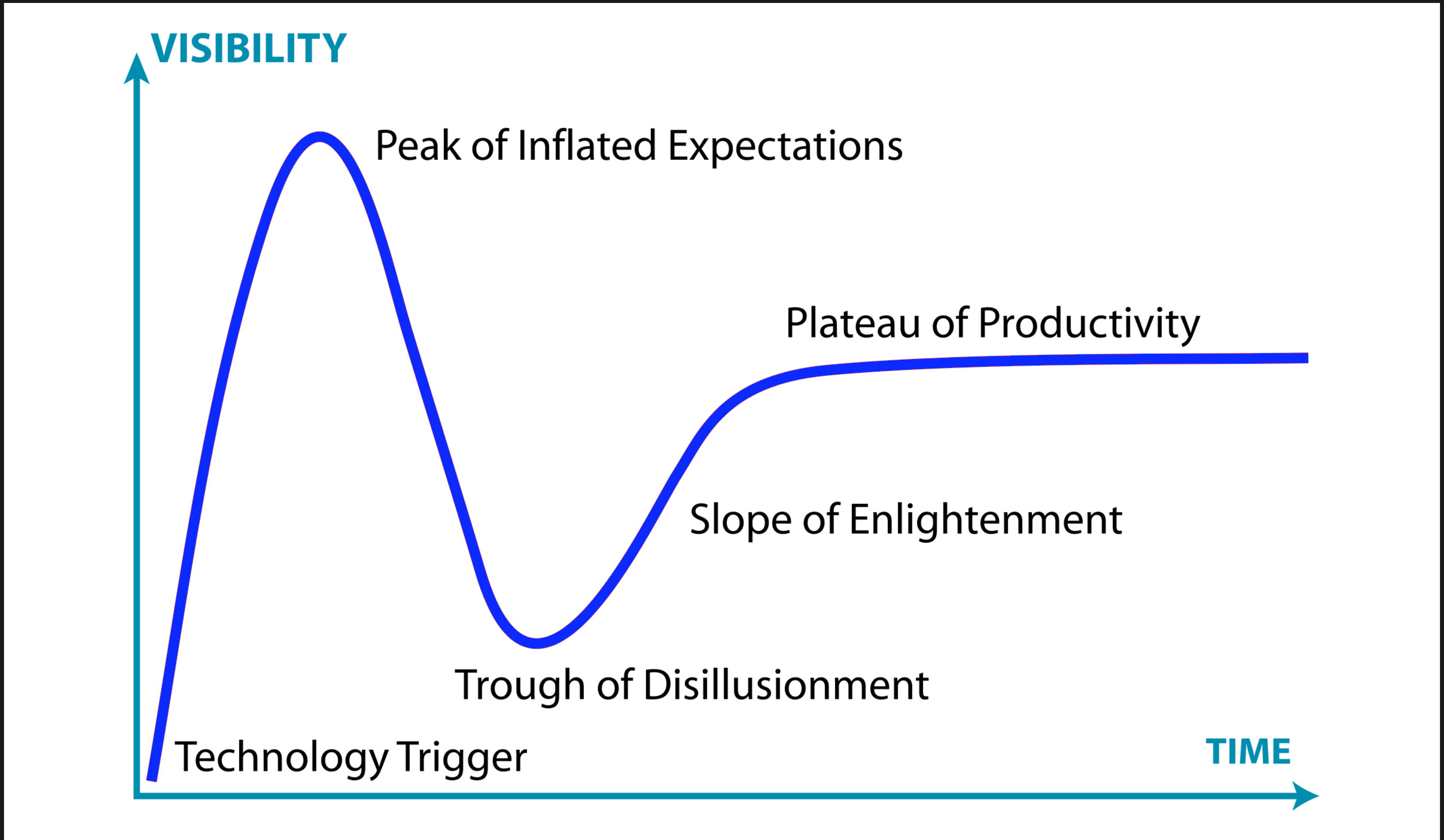
„Make everything as simple as possible, but not simpler.“ (Albert E.)

INFORMATION SECURITY

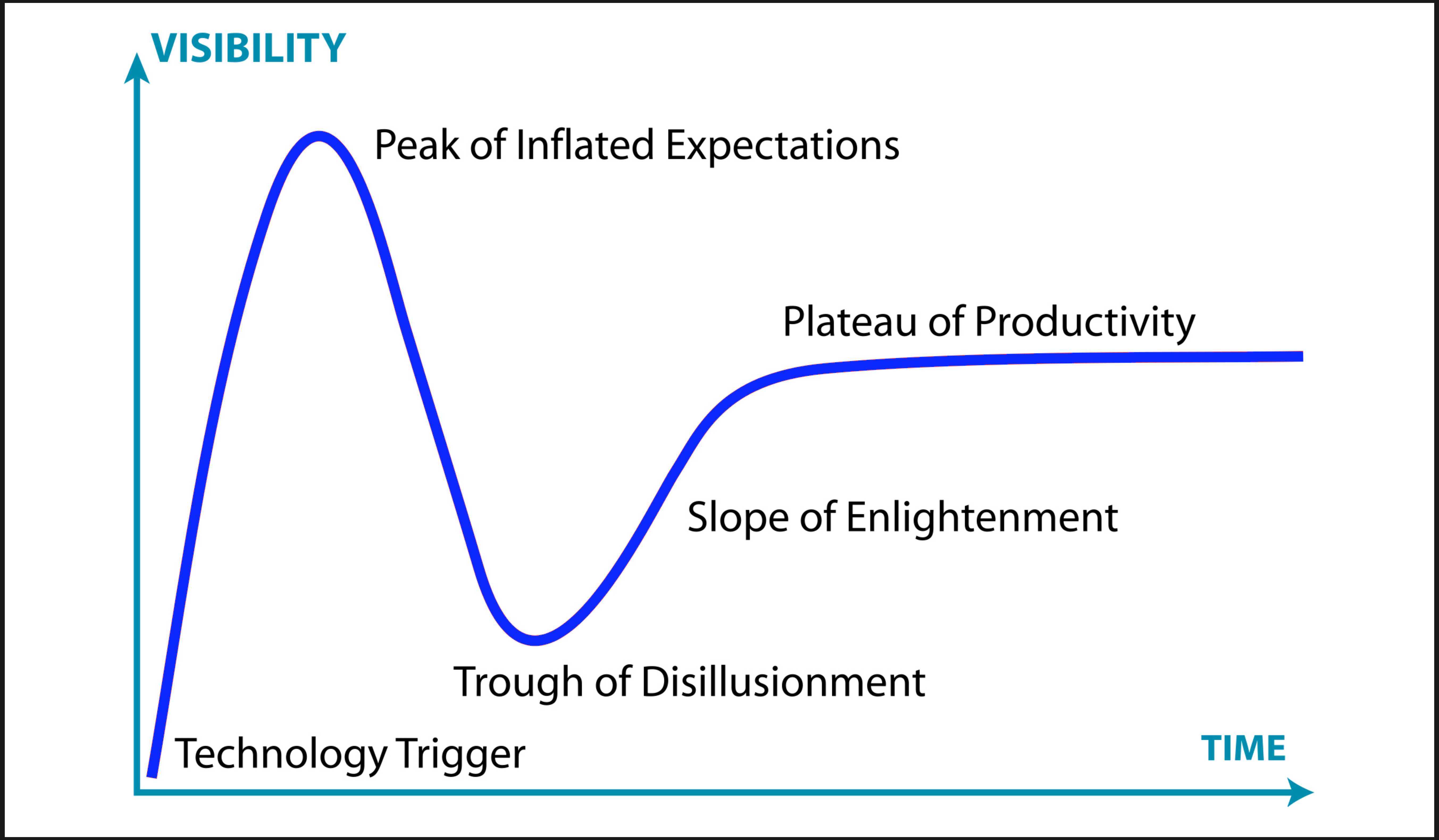

FACEBOOK
GMAIL
PHOTOS & FILES
USER ACCOUNT ON MY LAPTOP
PAYPAL
DROPBOX
BANK
ADMIN ACCOUNT
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Source: xkcd Authorization

HYPE, TRENDS, FASHION STATEMENTS

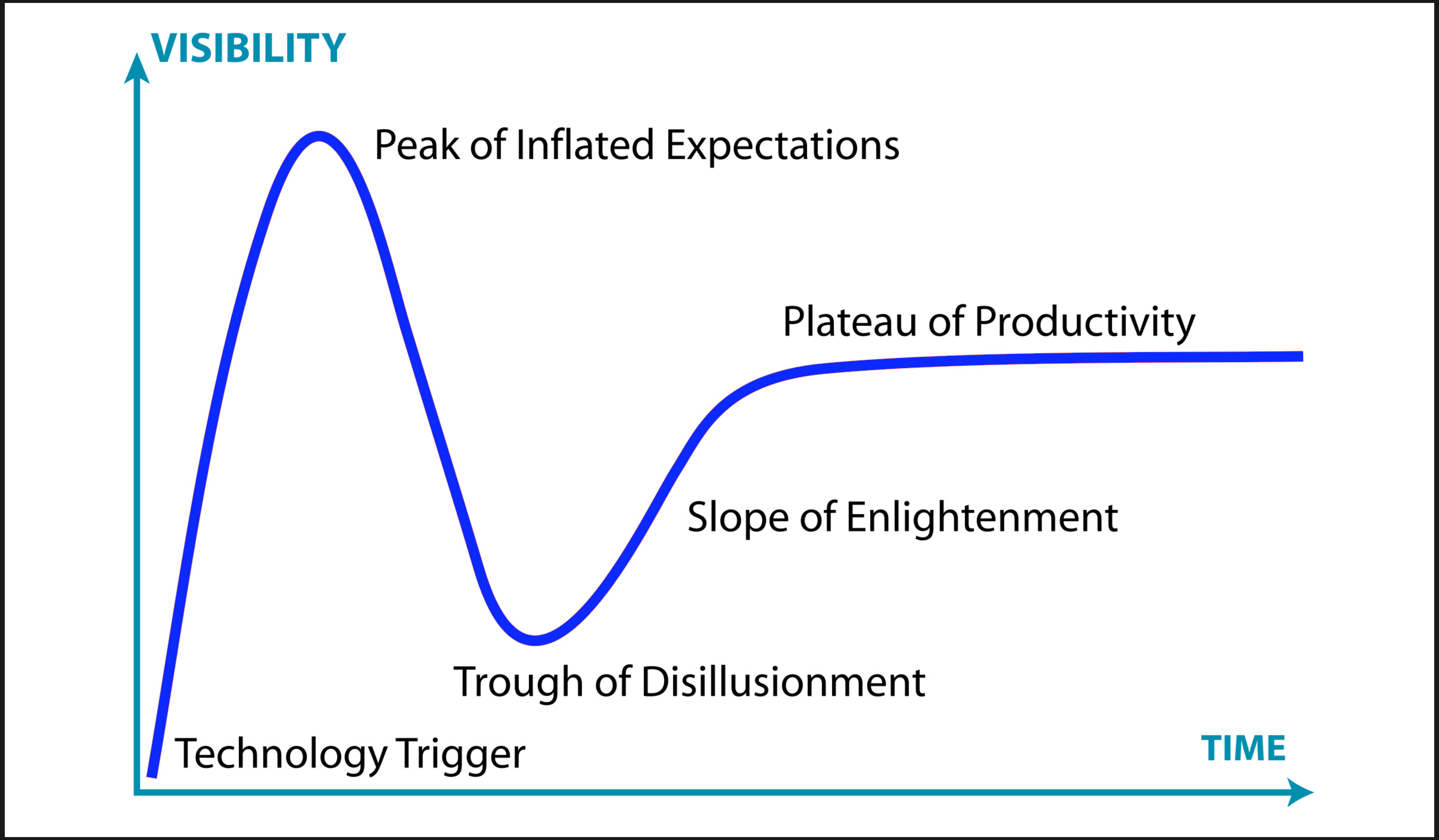


HYPE, TRENDS, FASHION STATEMENTS



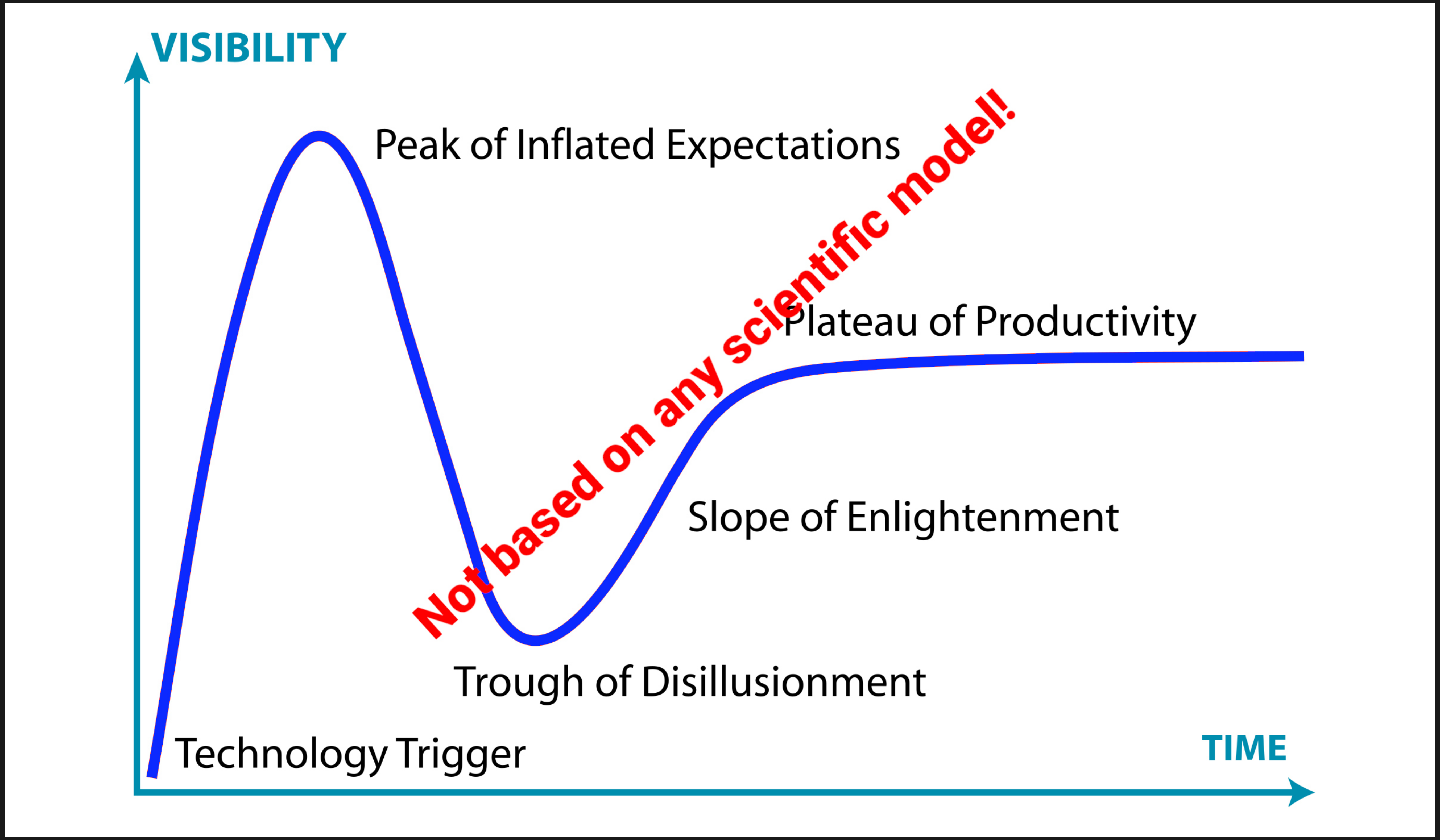
HYPE, TRENDS, FASHION STATEMENTS

This feels familiar.



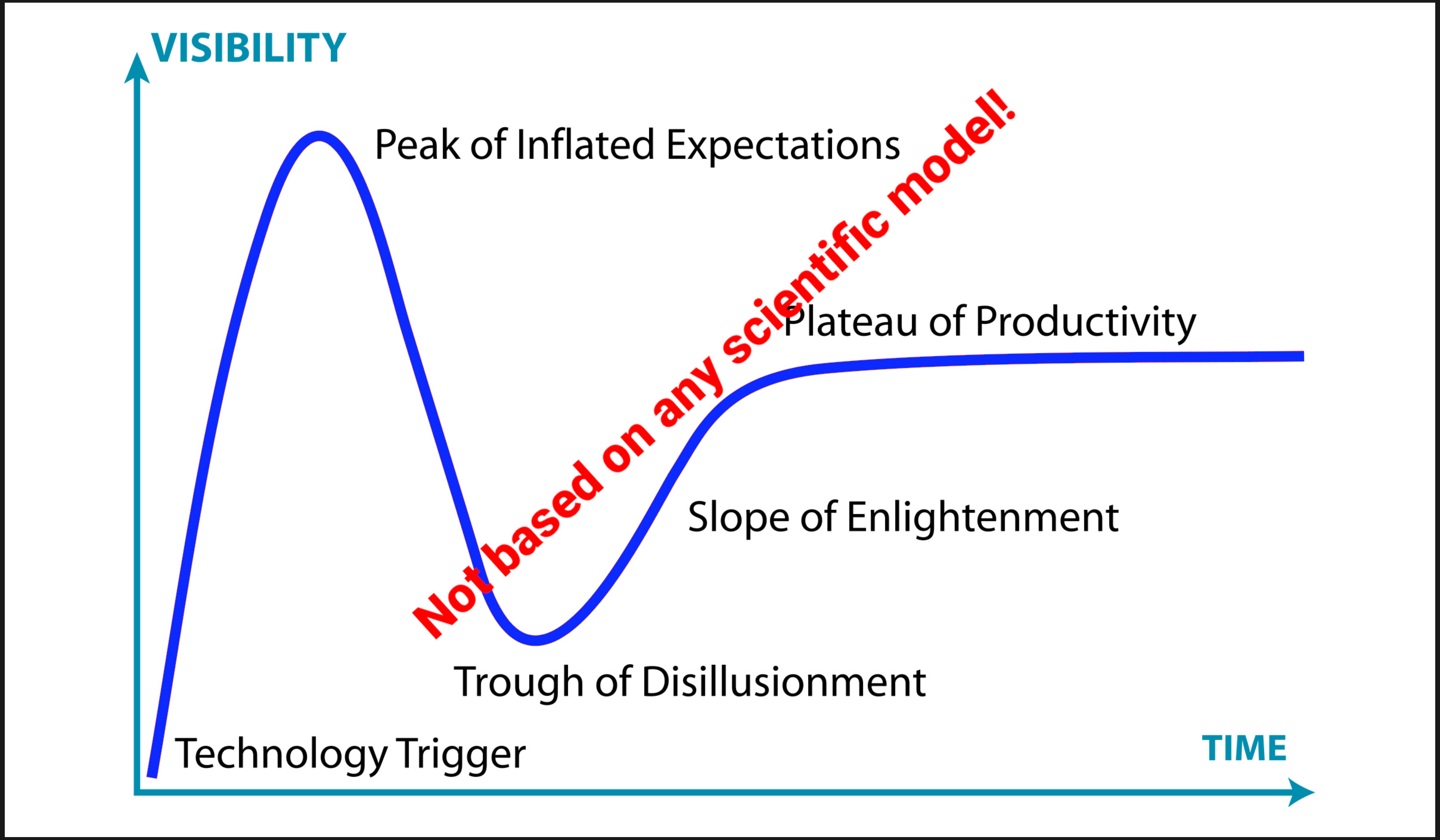
PROBLEM

PROBLEM


VISIBILITY
Peak of Inflated Expectations
Not based on any scientific model!
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

PROBLEM

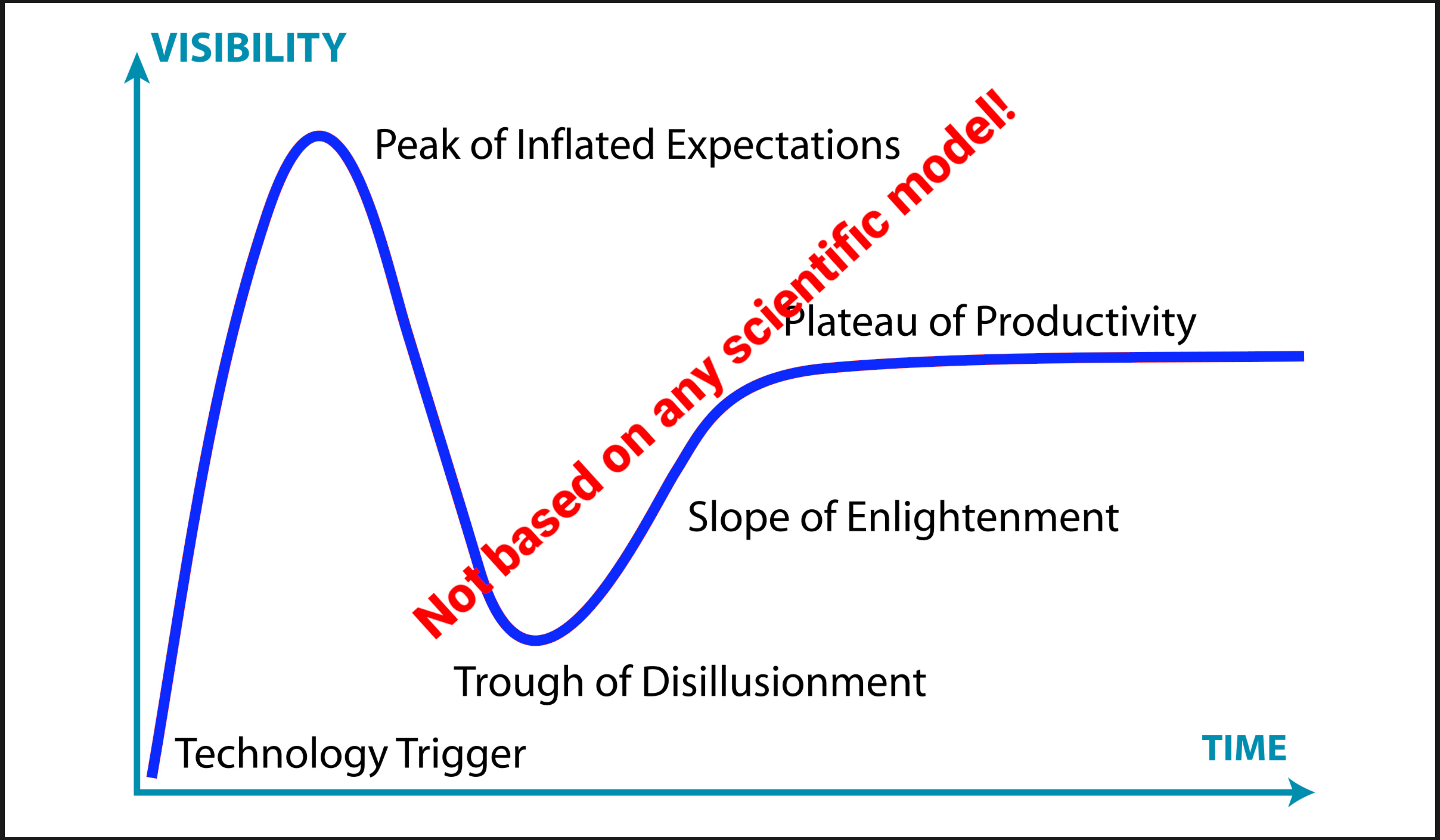
That's not a model. It's just a drawing.


VISIBILITY
Peak of Inflated Expectations
Not based on any scientific model!
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

PROBLEM

That's not a model. It's just a drawing.

Thinking like this is the cause for serious issues in IT (security)!


VISIBILITY
Peak of Inflated Expectations
Not based on any scientific model!
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢
- How do you measure (lack of / increased) security? 🔎

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢
- How do you measure (lack of / increased) security? 🔎
- Can you assess all your data and systems? ⚖

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢
- How do you measure (lack of / increased) security? 🔎
- Can you assess all your data and systems? ⚖
- Can you tolerate a false positive rate of 0.0005? 🛎

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢
- How do you measure (lack of / increased) security? 🔎
- Can you assess all your data and systems? ⚖
- Can you tolerate a false positive rate of 0.0005? 🛎
- (No, because 1e6 events/month mean 16,6 alerts/day.)

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣ ☢
- How do you measure (lack of / increased) security? 🔎
- Can you assess all your data and systems? ⚖
- Can you tolerate a false positive rate of 0.0005? 🛎
- (No, because 1e6 events/month mean 16,6 alerts/day.)
- Can you name relevant indicators of compromise? 🔥

HOW DO YOU SELECT IT SECURITY SOLUTIONS?

- There is a need for ${SOMETHING}.
- Need usually means unsolved problems or hazards. 🧯 ☣️ ☢️
- How do you measure (lack of / increased) security? 🔎
- Can you assess all your data and systems? ⚖️
- Can you tolerate a false positive rate of 0.0005? 🛎️
- (No, because 1e6 events/month mean 16,6 alerts/day.)
- Can you name relevant indicators of compromise? 🔥
- „Hello, world!“ – Complexity is back. 🥳

WHAT ACTUALLY HAPPENS

WHAT ACTUALLY HAPPENS

1. Ask the IT department, maybe get an answer.

WHAT ACTUALLY HAPPENS

1. Ask the IT department, maybe get an answer.
2. Check the budget.

WHAT ACTUALLY HAPPENS

1. Ask the IT department, maybe get an answer.
2. Check the budget.
3. Ask companies with a good PR department for their products.
   (If you don't know them, you cannot ask them, hence PR.)

WHAT ACTUALLY HAPPENS

1. Ask the IT department, maybe get an answer.
2. Check the budget.
3. Ask companies with a good PR department for their products.
   (If you don't know them, you cannot ask them, hence PR.)
4. Spend money for a compromise between budget, blame, and risk.

WHAT ACTUALLY HAPPENS

1. Ask the IT department, maybe get an answer.
2. Check the budget.
3. Ask companies with a good PR department for their products.
   (If you don't know them, you cannot ask them, hence PR.)
4. Spend money for a compromise between budget, blame, and risk.

„In IT security, the products with the best PR usually wins.“

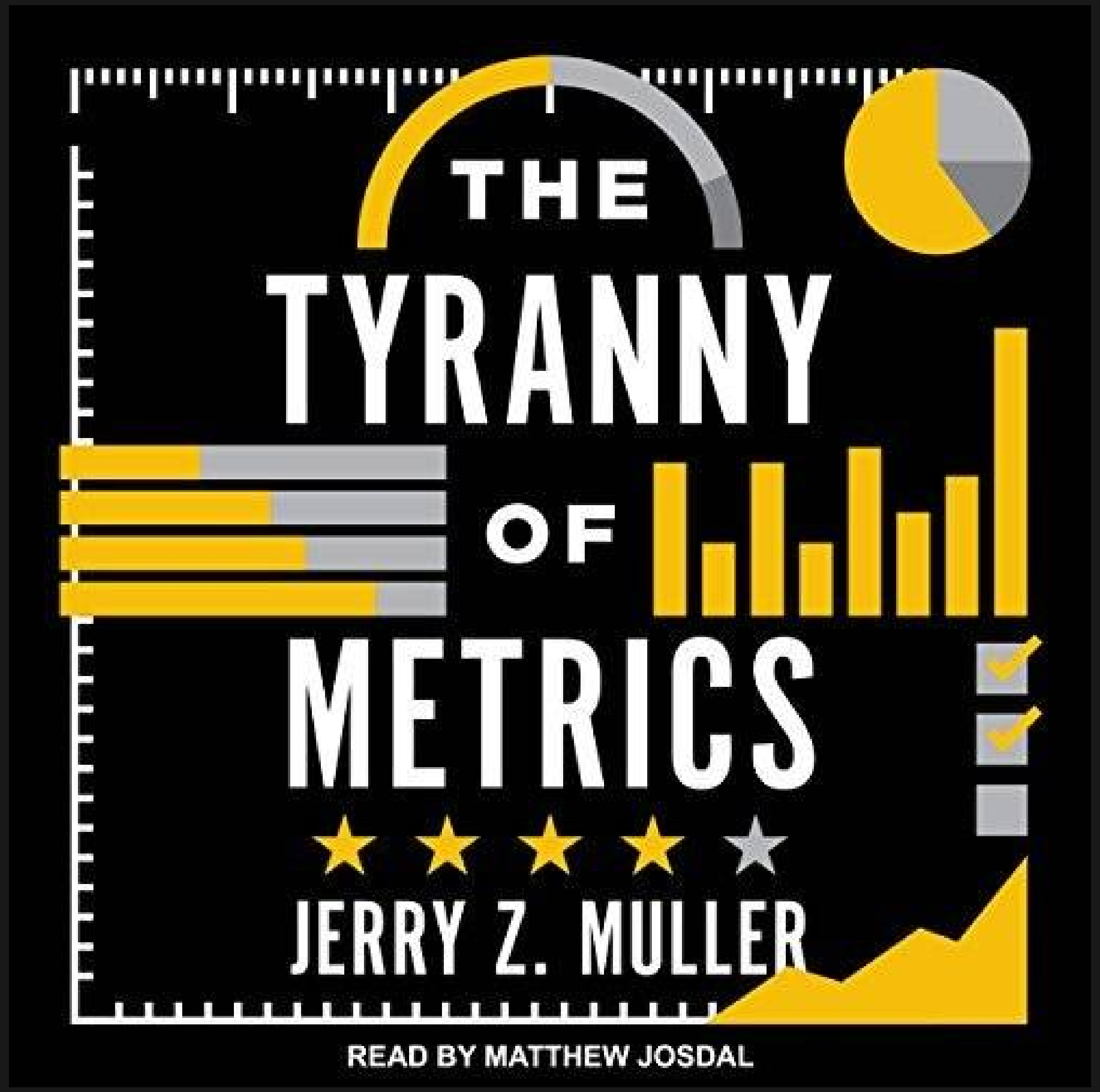
THE JOY OF METRICS

THE JOY OF METRICS

It is good practice to measure something. Or to pretend, at least.

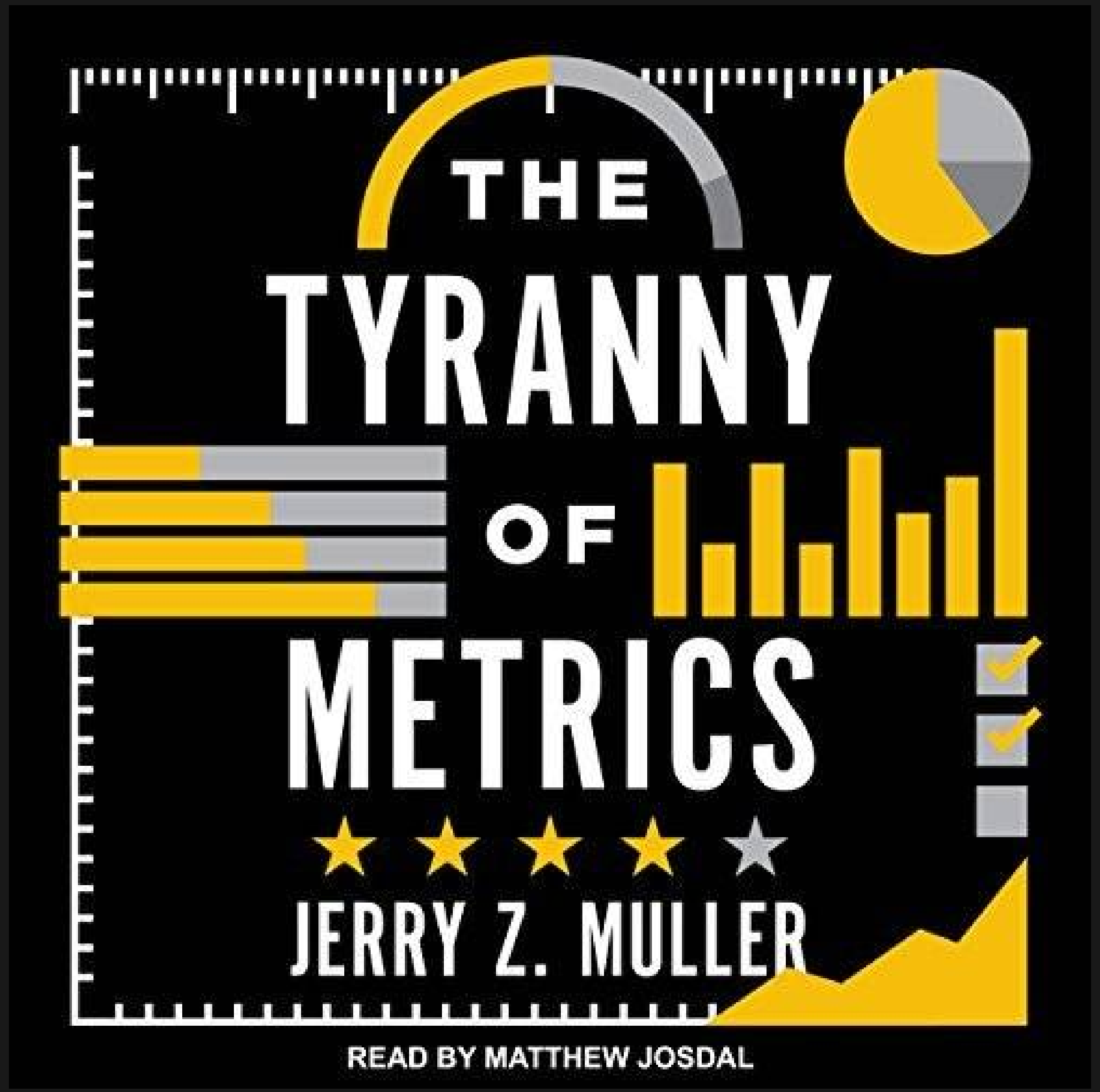
THE JOY OF METRICS

It is good practice to measure something. Or to pretend, at least.



THE JOY OF METRICS

It is good practice to measure something. Or to pretend, at least.



Quantification has become a cult - procedure without meaning.

WHAT ABOUT COMPLEXITY?

WHAT ABOUT COMPLEXITY?

Source: Schrödinger’s cat gets a reality check

WHAT ABOUT COMPLEXITY?

We can deal with complexity in software (mostly).

Source: Schrödinger’s cat gets a reality check

WHAT ABOUT COMPLEXITY?

We can deal with complexity in software (mostly).

We cannot deal with complexity in black boxes!

Source: Schrödinger’s cat gets a reality check

METRICS: THE CHECKLIST

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?
5. To what purposes will the measurements be put?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?
5. To what purposes will the measurements be put?
6. To whom will the information be made transparent?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?
5. To what purposes will the measurements be put?
6. To whom will the information be made transparent?
7. What are the costs of aquiring the metrics?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?
5. To what purposes will the measurements be put?
6. To whom will the information be made transparent?
7. What are the costs of aquiring the metrics?
8. Why does your organisation demand performance metrics?

Source: The Tyranny of Metrics

METRICS: THE CHECKLIST

1. What kind of information are you thinking of measuring?
2. How useful is the information?
3. How useful are more metrics?
4. What are the costs of not relying upon standardized measurement?
5. To what purposes will the measurements be put?
6. To whom will the information be made transparent?
7. What are the costs of aquiring the metrics?
8. Why does your organisation demand performance metrics?
9. How and by whom are the measures of performance developed?

Source: The Tyranny of Metrics

HELPFUL HINTS

HELPFUL HINTS

- Reanalyze Big Data.

HELPFUL HINTS

- Reanalyze Big Data.
- Define and apply sensible metrics.

HELPFUL HINTS

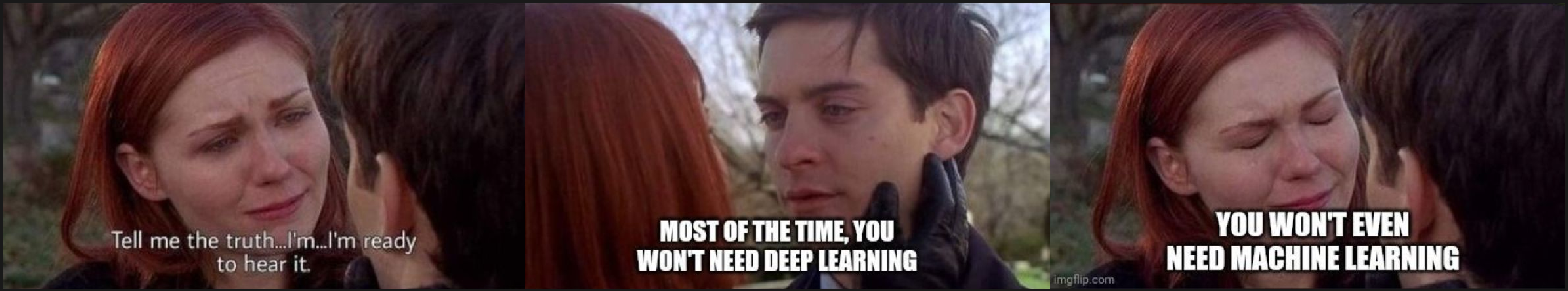
- Reanalyze Big Data.
- Define and apply sensible metrics.
- Refactor everything - reduce complexity in your organisation.

HELPFUL HINTS

- Reanalyze Big Data.
- Define and apply sensible metrics.
- Refactor everything - reduce complexity in your organisation.
- What does SIEM mean for you?

HELPFUL HINTS

- Reanalyze Big Data.
- Define and apply sensible metrics.
- Refactor everything - reduce complexity in your organisation.
- What does SIEM mean for you?


Tell me the truth...I'm...I'm ready to hear it.
MOST OF THE TIME, YOU WON'T NEED DEEP LEARNING
YOU WON'T EVEN NEED MACHINE LEARNING
imgflip.com

QUESTIONS?

Source: N-Body Simulation with 131072 bodies

WHOAMI

- 🆔 René „Lynx“ Pfeiffer
- ℹ Senior Systems Administrator
- ℹ DeepSec In-Depth Security Conference organisation team
- ☢ Study of theoretical physics
- 🕸 Internet user since 1992
- ⌛ 30+ years of experience with software development, computing platforms, and systems administration

CONTACT

- Email: *rpfeiffer@deepsec.net*
- PGP/GPG: `0x8531093E6E4037AF`
- Mobile: `+43.676.5626390` (Signal available)
- GSMK Cryptophone™: +807.94905059
- Threema: `7U6X9E5W`

ABOUT THE AUTHOR

René „Lynx“ Pfeiffer was born in the year of Atari's founding and the release of the game Pong. Since his early youth he started taking things apart to see how they work. He couldn't even pass construction sites without looking for electrical wires that might seem interesting. The interest in computing began when his grandfather bought him a 4-bit microcontroller with 256 byte RAM and a 4096 byte operating system, forcing him to learn Texas Instruments TMS 1600 assembler before any other programming language.

After finishing school he went to university in order to study physics. He then collected experiences with a C64, a C128, two Commodore Amigas, DEC's Ultrix, OpenVMS and finally GNU/Linux on a PC in 1997. He is using Linux since this day and still likes to take things apart und put them together again. Freedom of tinkering brought him close to the Free Software movement, where he puts some effort into the right to understand how things work – which he still does.

René is a senior systems administrator, a lecturer at the University of Applied Sciences Technikum Wien and FH Burgenland, and a senior security consultant. He uses all the skills in order to develop security architectures, maintain/improve IT infrastructure, test applications, and to analyse security-related attributes of applications, networks (wired/wireless, components), (cryptographic algorithms), protocols, servers, cloud platforms, and more indicators of modern life.