

5G: o bom, o mau e o feio

Dr. Roberto Gallo
Diretor Geral - KRYPTUS EED S.A.

gallo@kryptus.com

2021-11-18

Um pouco sobre nossas contribuições e experiência em segurança

- Empresa fundada em 2003, com histórico importante de contribuições ao setor Público, como:
 - Urna Eletrônica do TSE
 - ICP-Brasil, incluindo a Autoridade Certificadora Raiz
 - Comunicações seguras das Forças Armadas
 - Segurança cibernética do Itamaraty
 - Tecnologia para emissão ePassaport brasileiro com a Casa da Moeda
- E grandes clientes no segmento privado no Brasil e em diversas regiões incluindo Américas, Europa, Oriente Médio, África, Ásia.



The background of the slide is a dense, overlapping field of gold coins, likely US one-dollar coins, which are slightly out of focus in the foreground and background, creating a sense of depth. The coins are illuminated from the right, casting soft shadows and highlighting their metallic texture.A small, solid orange horizontal bar is located in the top-left corner of the slide.

A promessa de USD\$13.2 trilhões

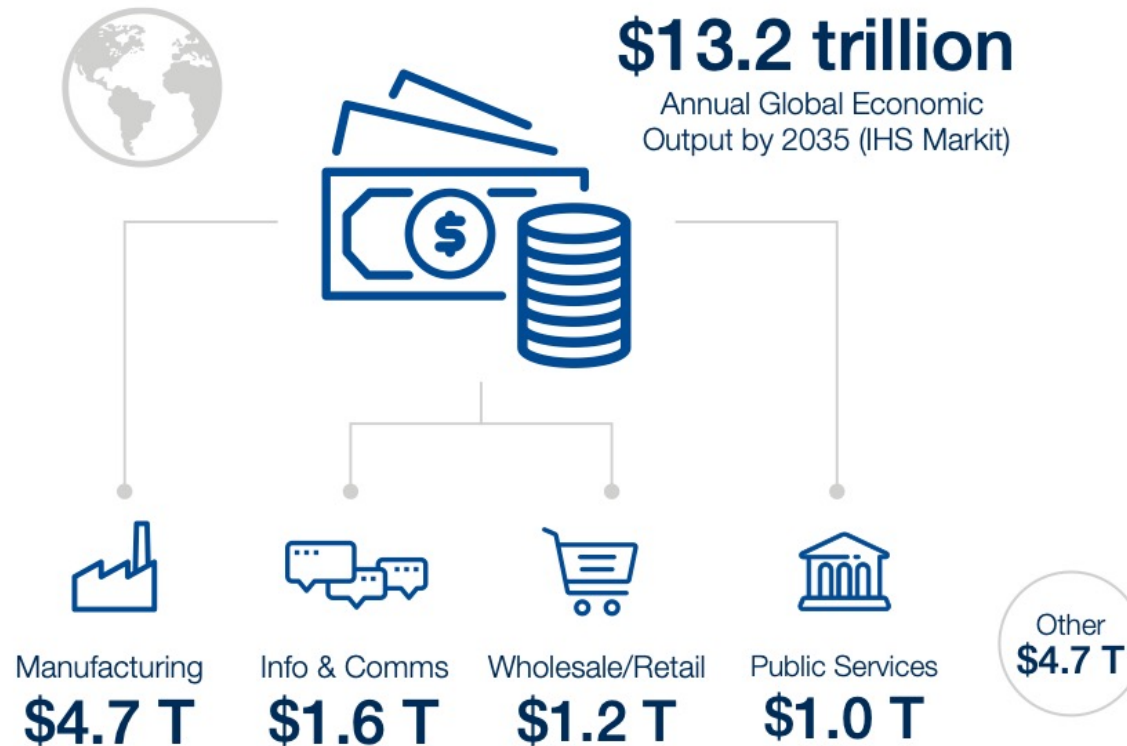
Fonte: https://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf

Economic and social value

http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf

To incentivize them to collaborate on addressing the challenges of widespread 5G deployment, stakeholders must be aware of and aligned on the potential economic and social value of 5G. Intelligent connectivity, enabled by 5G, will be a catalyst for socio-economic growth in the Fourth Industrial Revolution with an estimated **\$13.2 trillion of global economic value reached by 2035** (Figure 2).

Figure 2: Economic and social value



Source: Based on IHS Markit, *The 5G Economy: How 5G will contribute to the global economy*, 2019.

"All the News
That's Fit to Print"

The New York Times.

LATE CITY EDITION

U. S. Weather Bureau Forecast (For the Atlantic):
Cloudy and cool today and tonight.
Misty, fair tomorrow.
Temp. today: 60-65. Tomorrow: 64-69.

VOL. CVII...No. 36,416.

Published by The New York Times Company

NEW YORK, SATURDAY, OCTOBER 8, 1957.

Published by The New York Times Company

FIVE CENTS

SOVIET FIRES EARTH SATELLITE INTO SPACE; IT IS CIRCLING THE GLOBE AT 18,000 M. P. H.; SPHERE TRACKED IN 4 CROSSINGS OVER U. S.

HOFFA IS ELECTED TEAMSTERS' HEAD; WARNS OF BATTLE

Defeats Two Foes 3 to 1
—Says Union Will Fight
"With Every Quota"

Part of the Hoffa address
is printed on Page 6.

By A. H. BARKER
Special to the New York Times.
MIAMI BEACH, Oct. 8.—The
annual—annual International
Brotherhood of Teamsters elect-
ed James R. Hoffa as its presi-
dent today.

He won by a margin of nearly
3 to 1 over the combined vote
of two rivals who campaigned
on pledges to clean up the in-



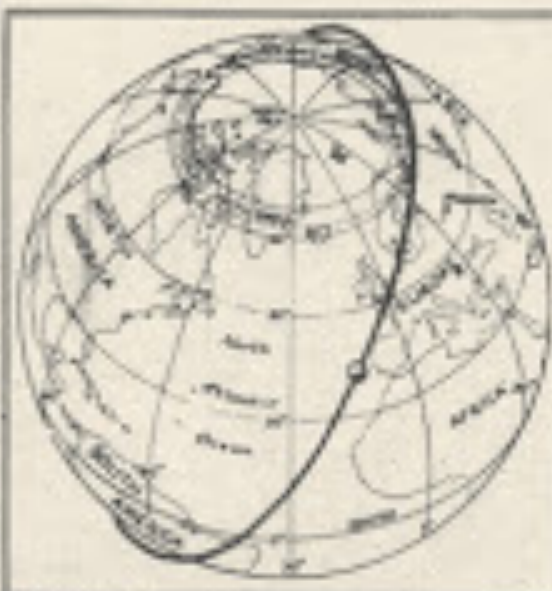
COURSE RECORDED

Navy Picks Up Radio
Signals—4 Report
Sighting Device

By WALTER HELFMAN
Special to the New York Times.
WASHINGTON, Saturday, Oct. 8.—The Naval Research Labo-
ratory announced early today that
it had recorded four crossings
of the Soviet earth satellite
over the United States.

It said that the SAT passed
near Washington. Two cross-
ings were further to the west.
The location of the fourth was
not made available immediately.

It added that tracking would
be continued to an attempt to
pin down the orbit sufficiently
to obtain scientific information
of the type sought by the Inter-
national Geophysical Year.



The New York Times
The approximate orbit of the Russian earth satellite is
shown by black line. The position of the earth will bring
the United States under the orbit of Soviet-made moon.

560 MILES HIGH

Visible With Simple
Binoculars, Moscow
Statement Says

Part of the Soviet statement
appears on Page 1.

By WILLIAM J. BROWNE
Special to the New York Times.
MOSCOW, Saturday, Oct. 8.—
The Soviet Union announced
this morning that it success-
fully launched a man-made
earth satellite into space yester-
day.

The Russians calculated the
satellite's orbit at a maximum
of 560 miles above the earth
and its speed at 18,000 miles an
hour.

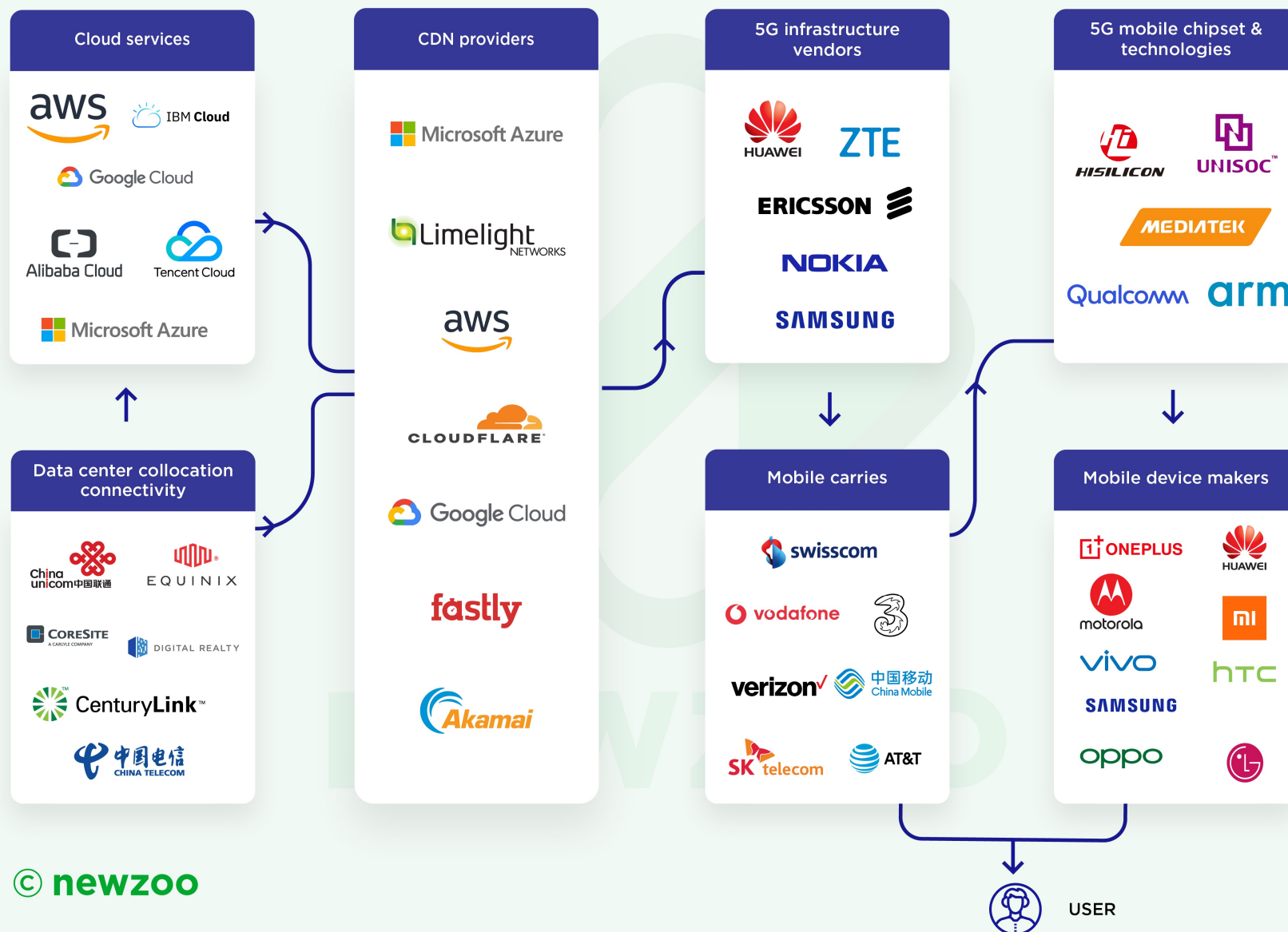
The official Soviet news
agency Tass said the artificial
moon, with a diameter of





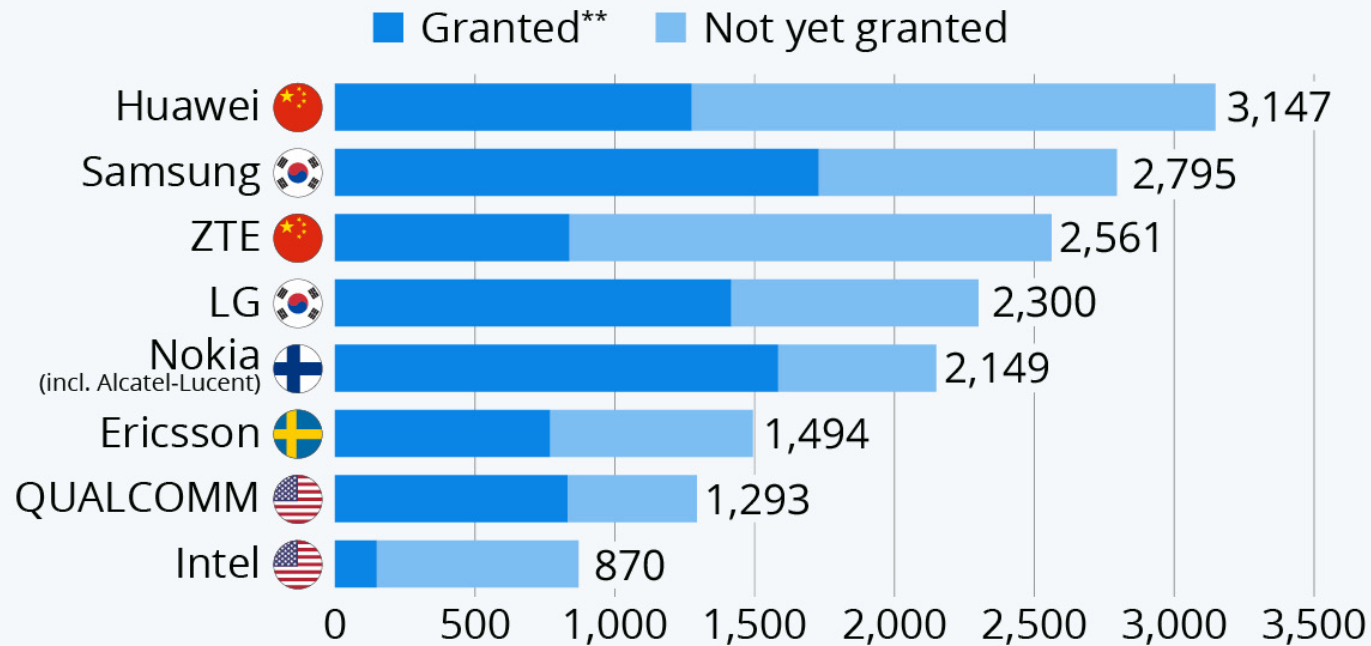
Key Players In 5G

Delivering technology to consumers



Who Is Leading the 5G Patent Race?

Companies which have filed the most patents for 5G technology*

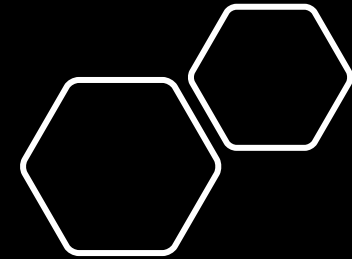


As of February 2020

* 5G SEP patent families, which is a group of patents covering the same technological area

** 5G SEP families with at least one granted patent counted

Source: IPlytics





Edifício Sede da União Africana



A Addis-Abeba, le siège de l'Union africaine espionné par Pékin

Il y a un an, les informaticiens du bâtiment, construit en 2012 par les Chinois, ont découvert que l'intégralité du contenu de ses serveurs était transférée à Shanghai.

Par Joan Tilouine et Ghalia Kadiri • Publié le 26 janvier 2018 à 11h45 - Mis à jour le 27 janvier 2018 à 08h36

🕒 Lecture 5 min.



Le siège de l'Union africaine à Addis-Abeba, capitale éthiopienne. Tiksa Negeri / REUTERS

PUBLICITÉ

ANIMALE
LANÇAMENTO
RIO DE
JANEIRO

AS PEÇAS DE SEDA
QUE VOCÊ AMOU
ESTÃO AQUI

SHOP NOW



Africa

After Allegations of Spying, African Union Renews Huawei Alliance

By Salem Solomon
June 07, 2019 07:05 PM



FILE - Workers prepare a stand for Huawei at the venue of the 21st Century Maritime Silk Road International Expo in Dongguan, Guangdong province, China, Oct. 28, 2015.

1619-2019



US Marks 400th Anniversary of Arrival of First Africans

CHILD MARRIAGE



The Worth of a Girl

SOUTH SUDAN



South Sudan in Focus

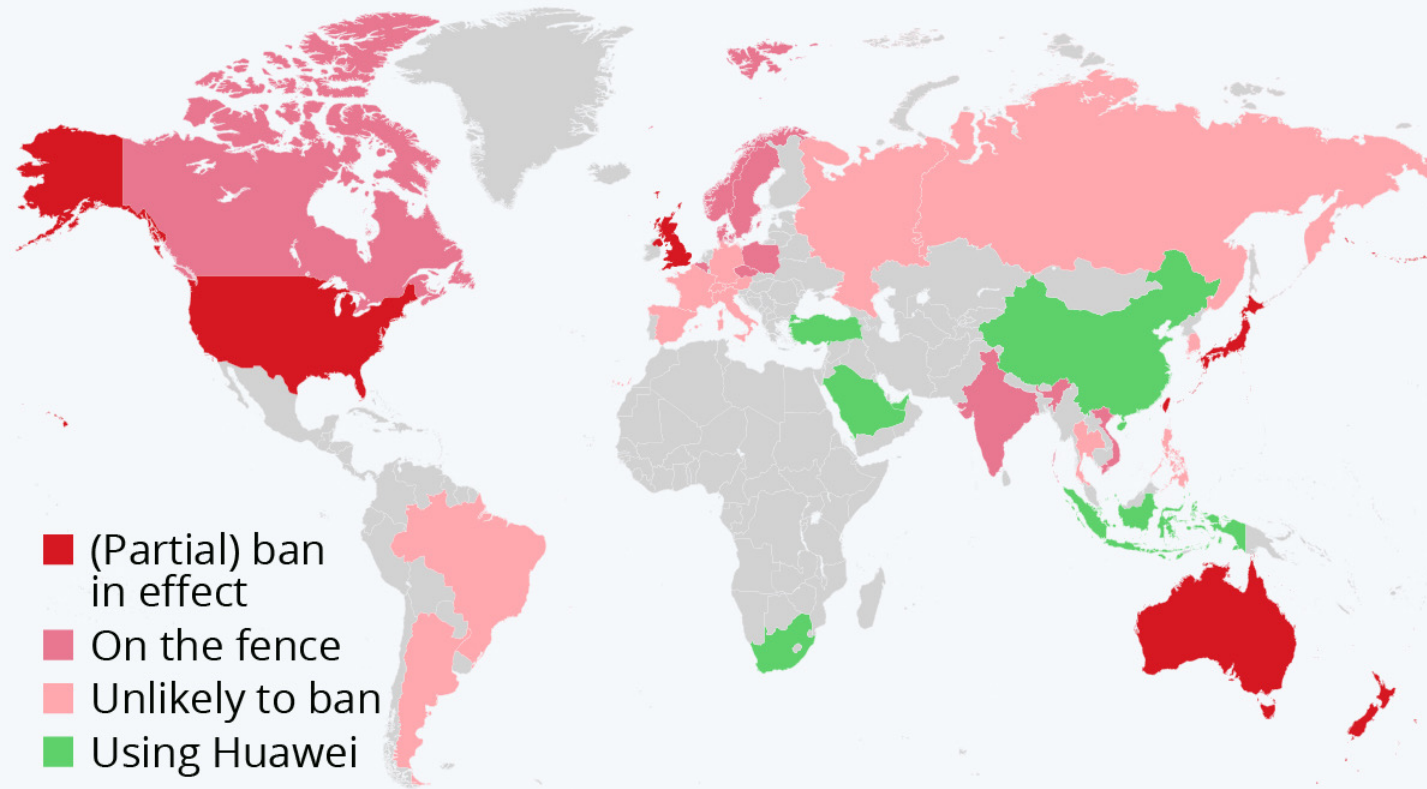
MUSIC TIME IN AFRICA ARCHIVE



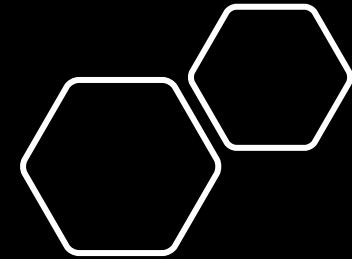
A Journey from Shortwave to

Which Countries Have Banned Huawei?

Countries which have banned or are considering of ban of Huawei products



Sources: Bloomberg, media reports



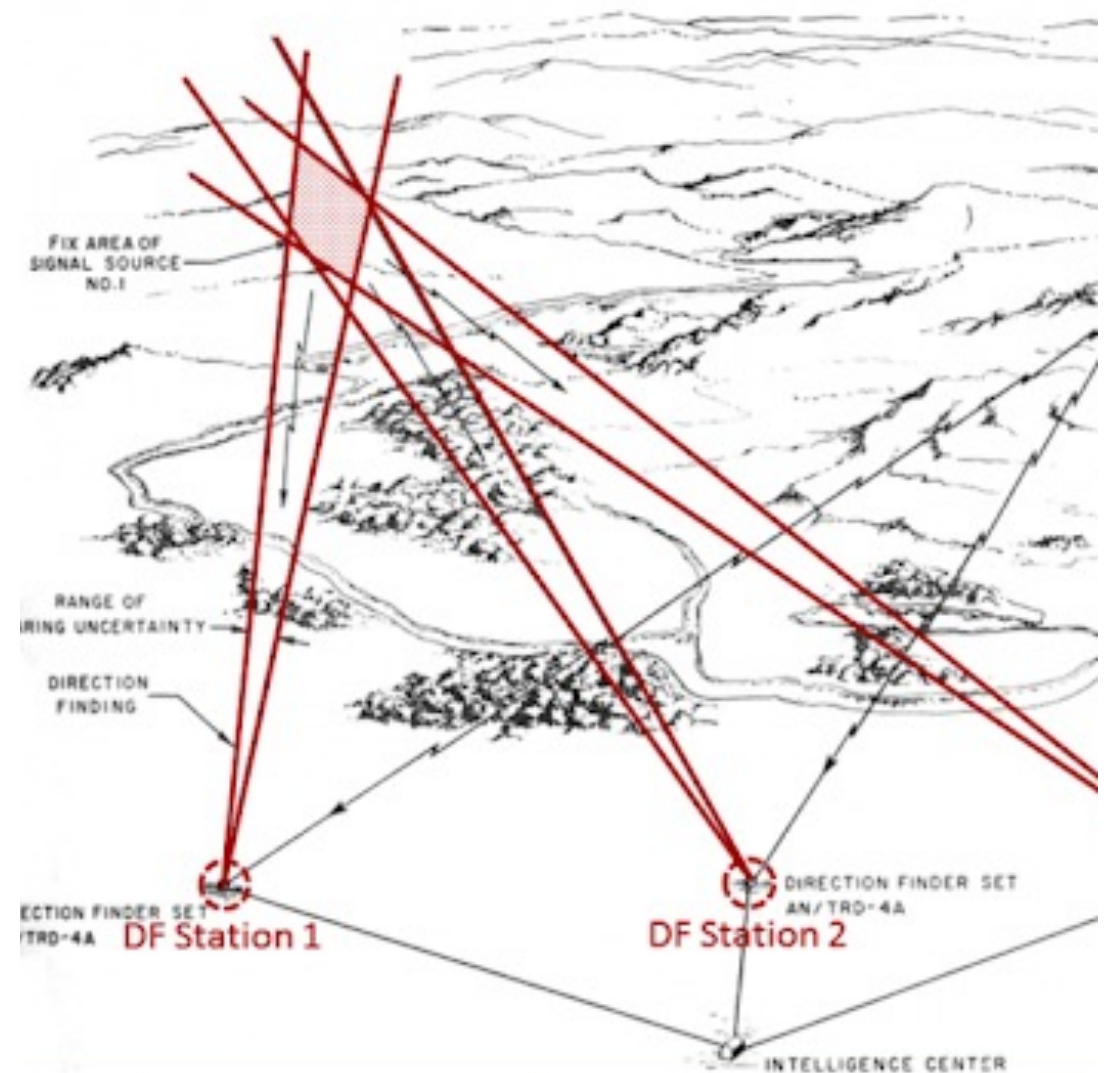
NSA

Secrets Declassified



The History of Traffic Analysis World War I - Vietnam

Signals Intelligence (SIGINT)
Communications Intelligence (COMINT)
World War II, Cold War, Cryptanalysis



National Security

‘The intelligence coup of the century’

For decades, the CIA read the encrypted communications of allies and adversaries.

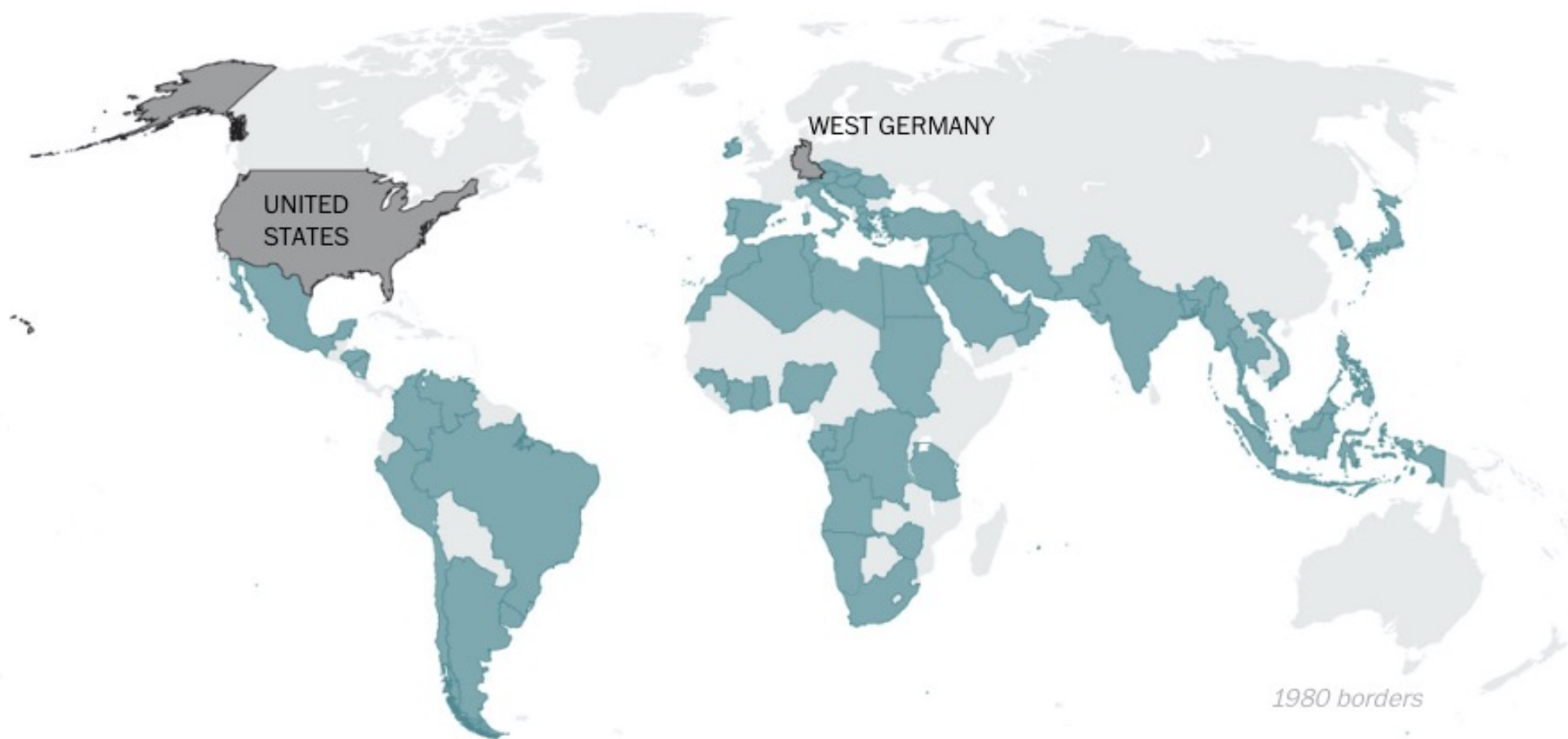
By **Greg Miller** Feb. 11, 2020



United States

Crypto
AG

West Germany



Documents indicate that more than 120 countries used Crypto AG encryption equipment from the 1950s well into the 2000s. The files don't include a comprehensive list but identify at least **62 customers.**

Portal da Transparência

CONTROLADORIA-GERAL DA UNIÃO

Busque por órgão, cidade, CNPJ, servidor...



Sobre o Portal ▾ | Painéis ▾ | Consultas Detalhadas ▾ | Controle social ▾ | Rede de Transparência | Receba Notificações | Aprenda mais ▾

VOCÊ ESTÁ AQUI: INÍCIO » BUSCA

Resultado da busca

crypto AG



31 resultados encontrados para crypto AG

Pessoa Jurídica: EX9300367 - CRYPTO AG

Nome empresarial: **CRYPTO AG**

Documento Pagamento 2017NS000763

Observação do documento: FATURA 425209 - BPV004 - **CRYPTO AG** - REGULARIZACAO FNE OP 143/2015 (FNE)

Favorecido: **CRYPTO AG**

EX9300367 - CRYPTO AG - favorecido(a) do pagamento 2017NS004375

Favorecido: **CRYPTO AG**

Documento Pagamento 2019NS005688

Observação do documento: LIQUIDACAO/PAGAMENTO REFERENTE INVOICE 200118 - CODEMP: S4266 - **CRYPTO AG**: PV49000-2019-00002 - OMC/OMS

Favorecido: **CRYPTO AG**

FILTROS APLICADOS

Utilize as categorias abaixo para refinar o resultado da busca

☐ Despesas ▾

☐ Documentos ▾

☐ Viagens

☐ Receitas públicas

☐ Servidores

☐ Imóveis Funcionais

☐ Sanções ▾

☐ Benefícios ▾

Fundamentos

A impossibilidade de provar que é seguro

Teorema de Rice

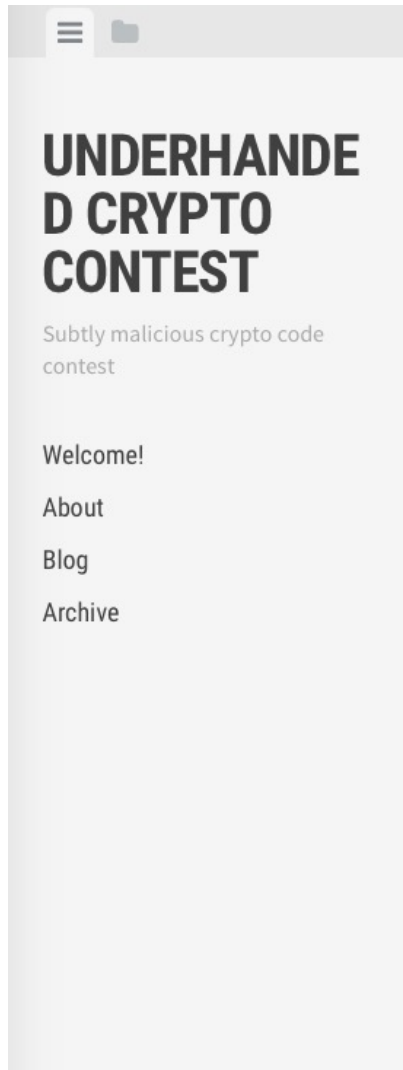
En [teoría de la computación](#), el **teorema de Rice** es un teorema enunciado por [Henry Gordon Rice](#) y luego generalizado junto con [John Myhill](#) y [Norman Shapiro](#) a lo que se conoce como el **teorema de Rice–Shapiro**. Básicamente se puede enunciar el teorema de la siguiente manera:

Dada una propiedad no trivial de las [funciones parciales](#), no es computable determinar si una función arbitraria la posee o no.¹

Aplicaciones [\[editar \]](#)

Las aplicaciones de teorema de Rice son numerosas. La primera aplicación que se nota a simple vista es que no es computable saber si una función arbitraria se detiene para algún valor de entrada (hay al menos una que sí lo hace, y otra que no, por lo que se trata de una propiedad no trivial). Otra aplicación que se puede dar a este teorema es saber que no es computable determinar si un programa es malicioso (que realizará acciones maliciosas como por ejemplo, escribir en cierta zona reservada de memoria, copiarse a sí mismo en otro programa, etc.). Esto no quiere decir que ningún programa malicioso sea detectable, sino que para cualquier procedimiento de detección fiable, siempre se puede definir un programa malicioso que lo burle.

A possibilidade de fazer bugs honestos indiferenciáveis de backdoors



MARCH 8, 2017 by TAYLOR HORNBY

Get Ready for The 2017 Underhanded Crypto Contest

☰ UNCATEGORIZED

💬 LEAVE A COMMENT

The Underhanded Crypto Contest is back, and we can't wait to see all the nifty tricks you'll come up with to put backdoors into cryptography. Last year we wanted to see backdoors that exclusively related to cryptocurrencies, and we didn't get much of a response. So, this year, we're open to *any* kind of crypto backdoor that you can think of.

To give you all a head start, here are a couple of ideas:

1. **Backdooring random number generators.** Surprisingly, we've only ever had one submission for a backdoored random number generator, back in 2014 by Solar Designer. Random number generators are important to almost every aspect of cryptography, so they're a great thing to backdoor. And it's hard to tell when a number is random and when it isn't, so there's lots of room to add an undetectable backdoor.

Tipos de Defeitos e formas de mitigação

Tipo/ Método	Acidental patente	Intencional patente	Acidental oculto	Intencional oculto
Análise em código fonte/projeto				
Análise com código projeto completo				
Acompanhamento de processo, com certificação				
Enquadramento legal com punição exemplar				

Estamos em uma sociedade pós-industrial

Grupos, Nações e Países sempre lutaram por recursos... pedras, fertilizante, petróleo, comida, água.

No ultimo século o maior ativo é conhecimento e tecnologia.

Porém e técnicas para ganhar vantagem neste terreno servem tanto para ações benignas como nocivas:

- Escuta legal
- Espionagem
- Ações de Guerra

Possíveis caminhos

Algumas estratégias...

Entender que a infraestrutura 5G não pode ser confiada e resolver a segurança em camada superior com uso de criptografia e técnicas cibernéticas

Garantir variabilidade onde diferentes ISP's não dependam exclusivamente de um único fornecedor, para aumento de resiliência

Atualizar a criminalização para sabotagem e espionagem explicitando infraestruturas críticas de telecomunicações – nova LSN parece amplamente insuficiente e frágil em comparação com outras democracias;

Ampliar as inspeções técnicas exploratórias nas infraestruturas e tecnologias, nos moldes do Ato 77 da ANATEL;

Multiplicar e ampliar o alcance dos exercícios do tipo “Guardião Cibernético”.



gettyimages®

25 YEARS

Ian Tyas

5G: o bom, o mau e o feio

Obrigado

Dr. Roberto Gallo
Diretor Geral - KRYPTUS EED S.A.

gallo@kryptus.com

2021-11-18

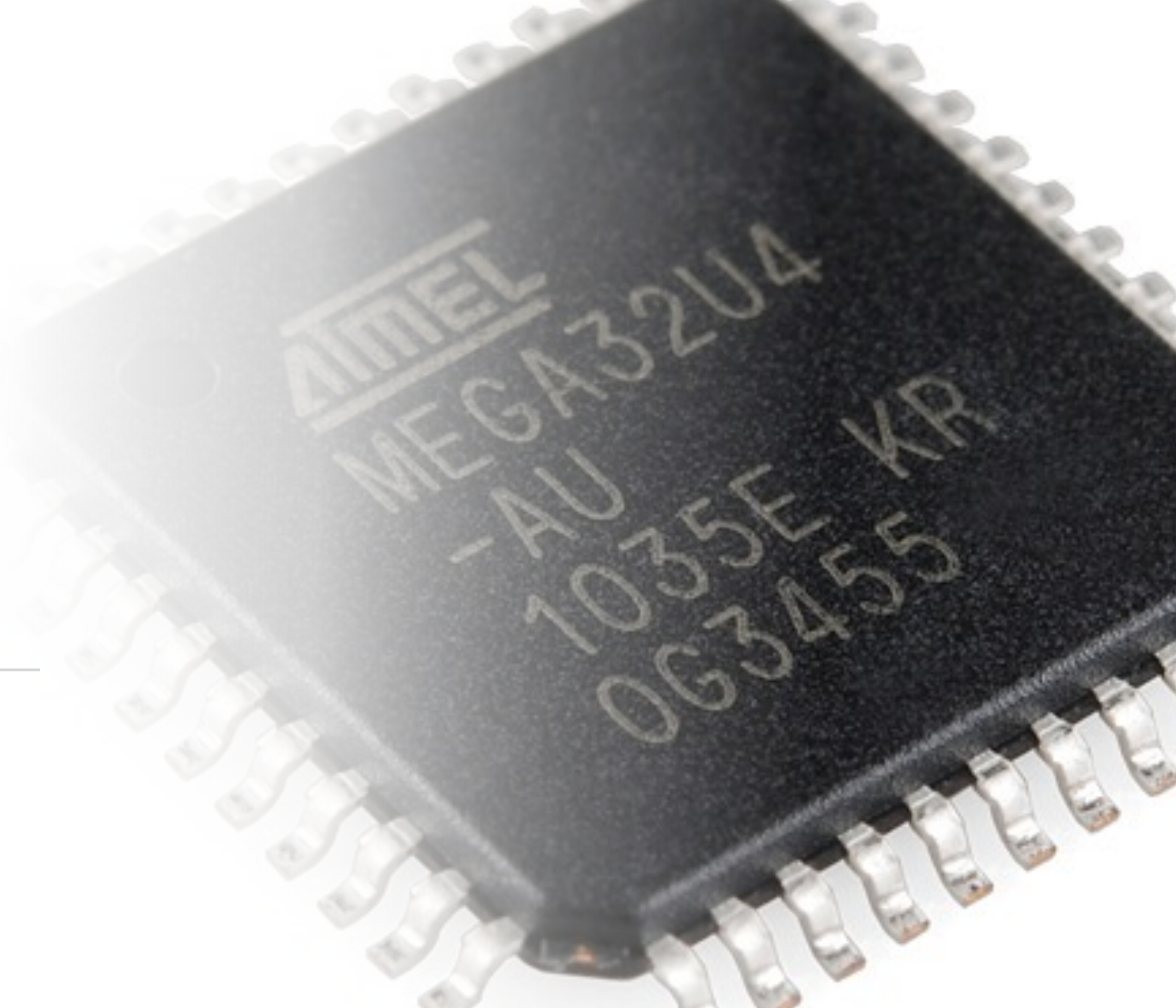


Material extra

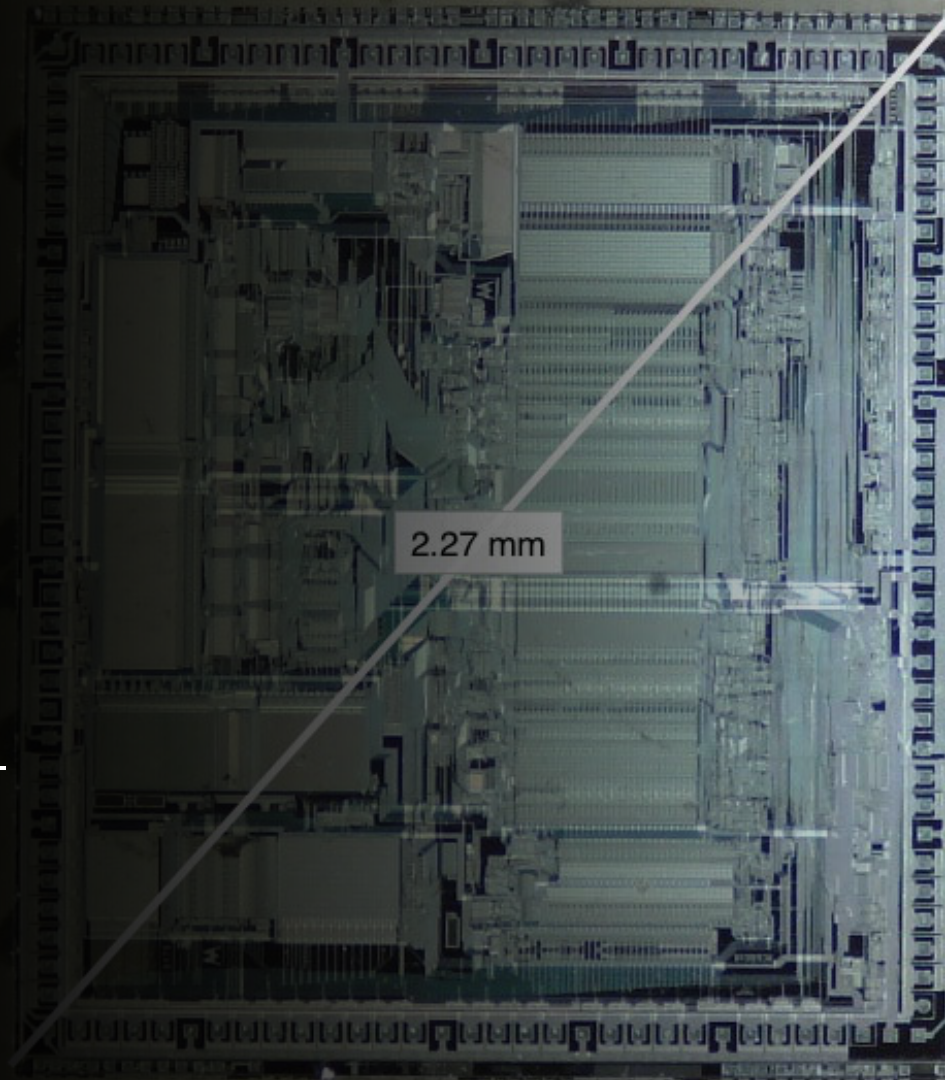
Os limites da verificação



Chips están en
toda parte



Sin la capa
epoxi



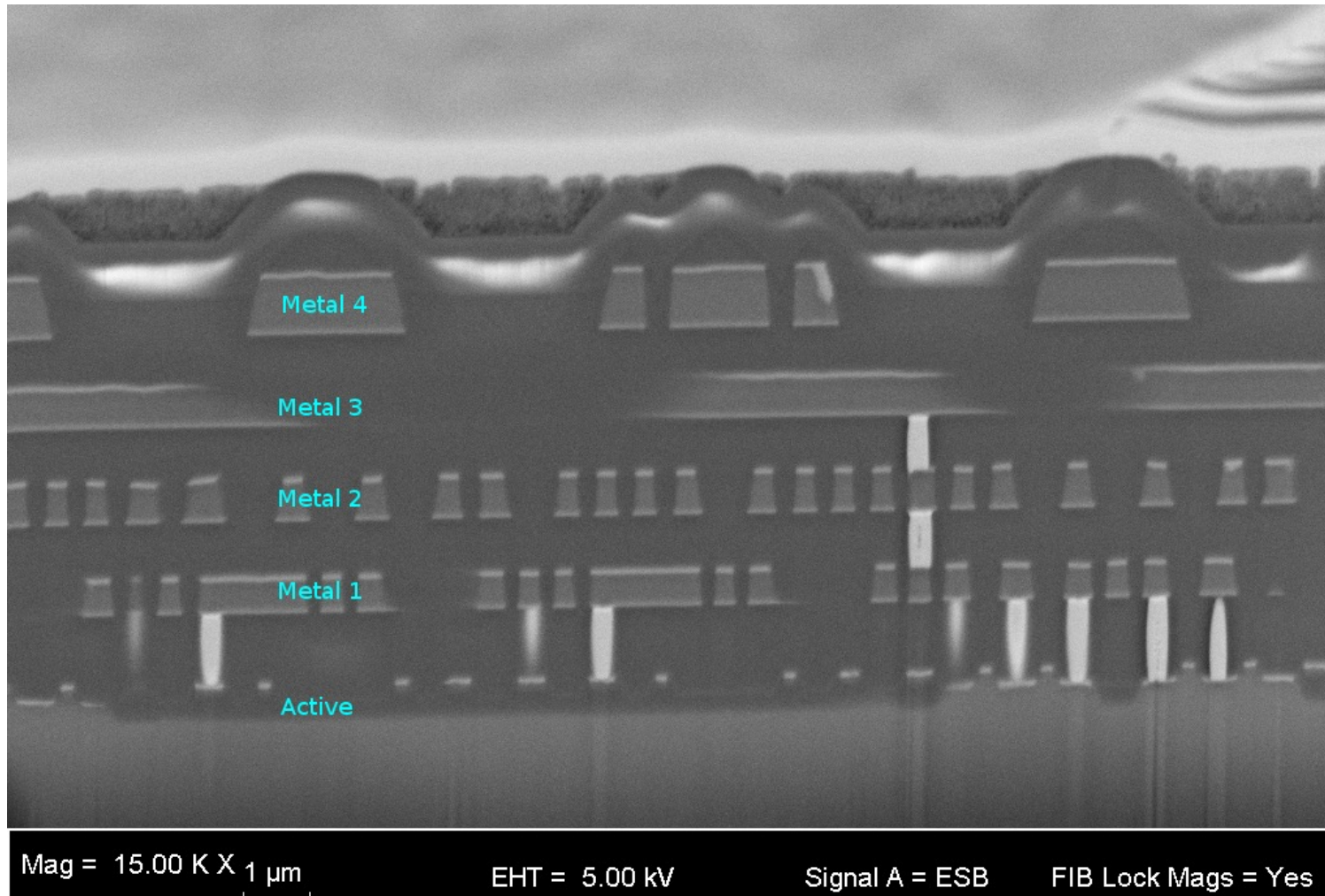
1.00 mm

2014-01-30 12:19

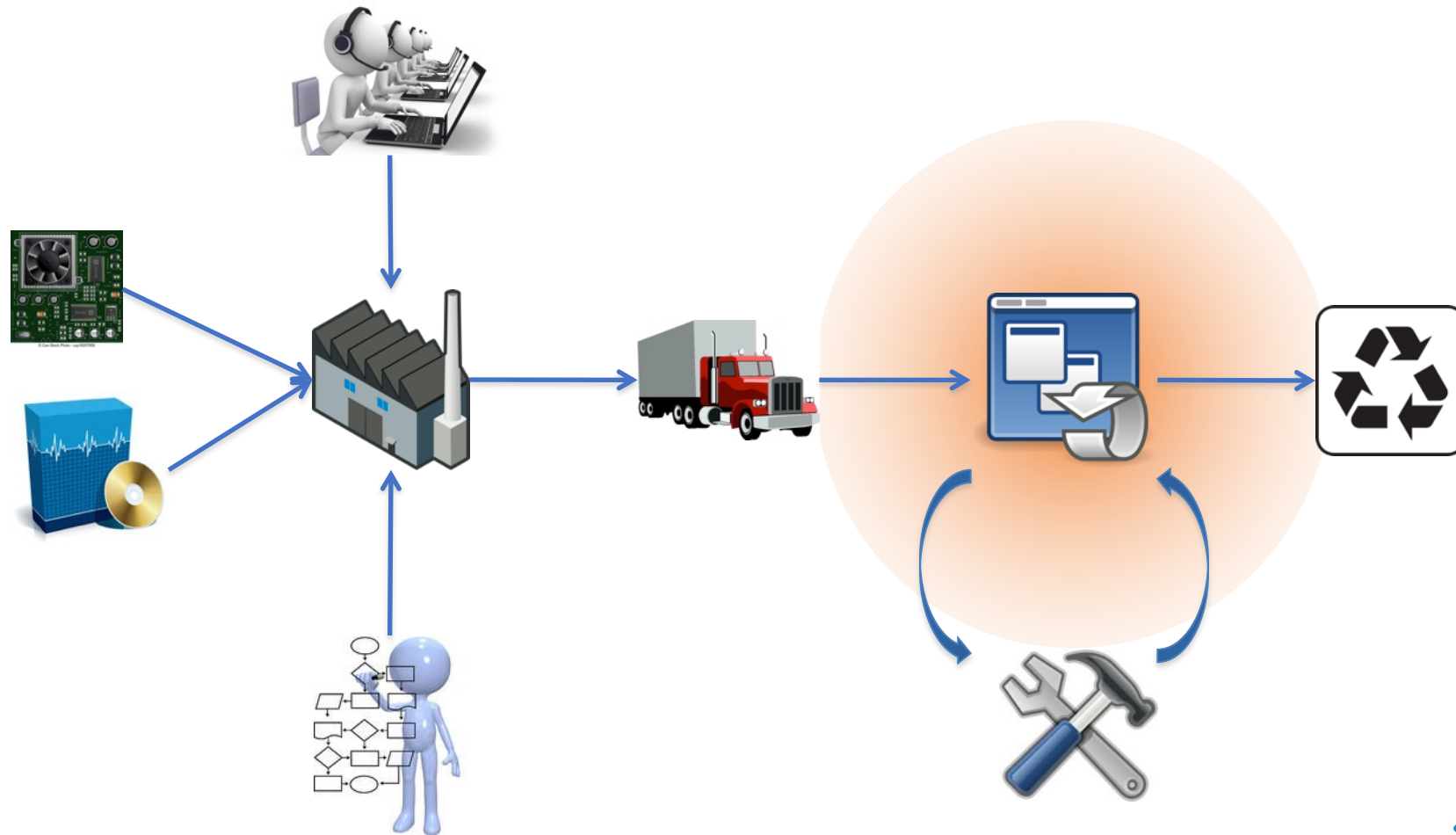


Aumento con microscopio de rayos X

Sección transversal y el FIB

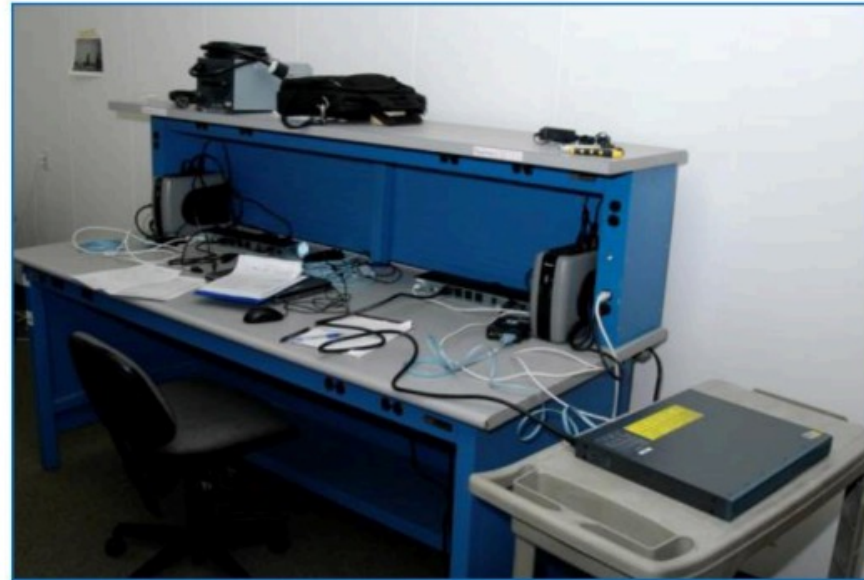


Sabotagens e Ataques de Ciclo de Vida



Cadena logística: NSA “trabajando”

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon



NSA Strategic Partnerships



**Alliances with over 80 Major Global Corporations
Supporting both Missions**

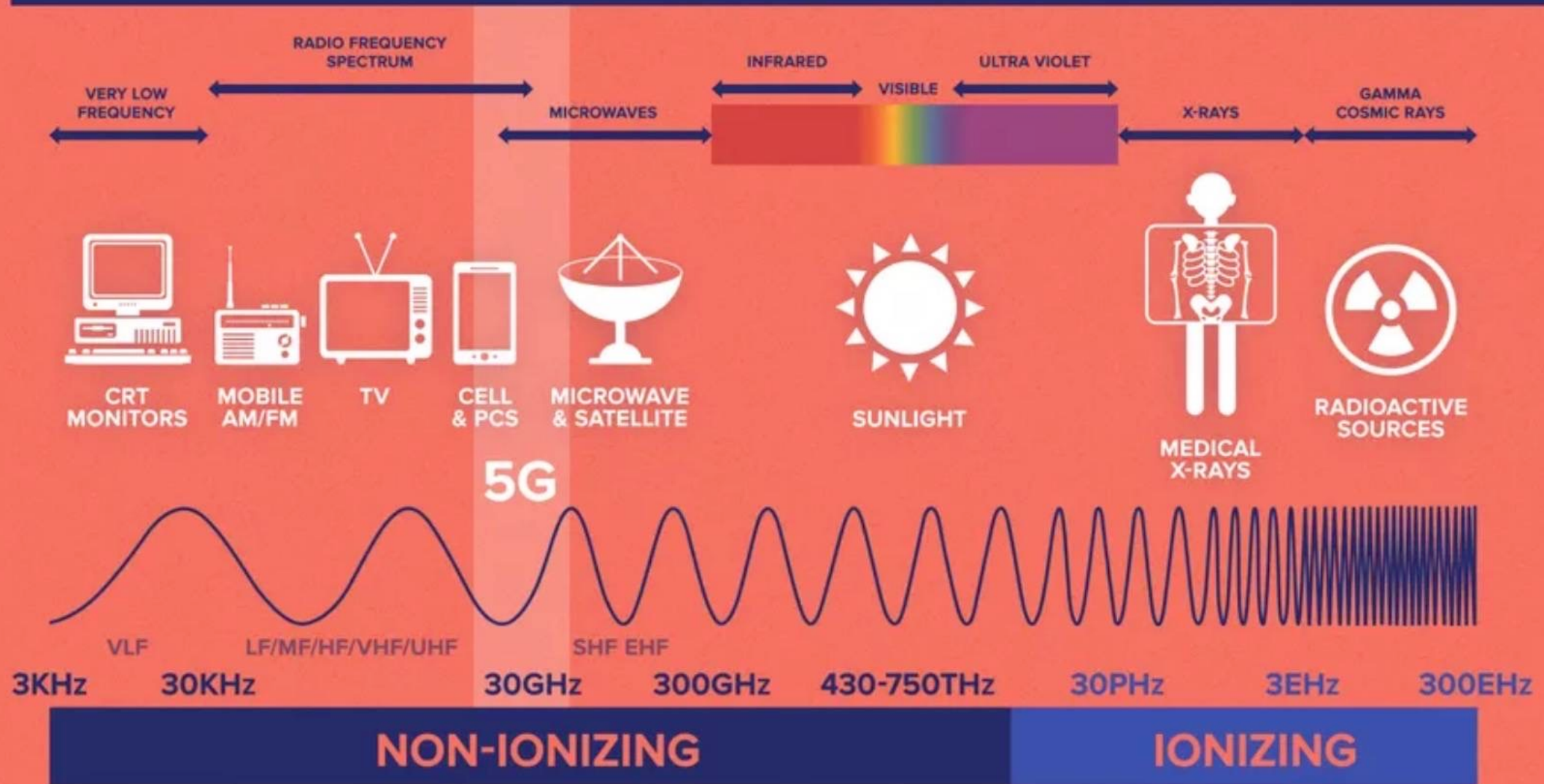
- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms
Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators



Functional driver	Description	Added value	Use cases
Enhanced mobile broadband (eMBB)	Faster connections, higher throughput and greater capacity (up to 10 Gbps)	Allows for an extension in cellular coverage into diverse structures (large venues) and the ability to handle a larger number of devices using high amounts of data	Fixed wireless access service, enhanced in-building broadband service, real-time augmented reality service, real-time virtual and mixed reality service, crowded or dense area service, enhanced digital signage, high-definition cloud gaming, public protection and disaster response services, massive content streaming services, remote surgery and examination
Ultra-reliable low latency communication (uRLLC)	Reduced time for data from device to be uploaded and reach its target (1 ms compared to 50 ms for 4G)	Enables time-sensitive connections wirelessly	Autonomous vehicles, drones and robotic applications, health monitoring systems/telehealth, smart grid and metering, intelligent transportation, factory automation, remote operation, self-driving cars, mission-critical services (security and safety), high-definition real-time gaming
Security	Robust security properties, leading to high reliability and availability	Creates an ultra-reliable connection to support applications where failure is not an option	
Massive machine-type communications (mMTC)	Increased spectral efficiency plus small cell deployment	Allows for a large number of connections to support data-intensive applications	Asset tracking and predictive maintenance, smart cities/buildings/agriculture, internet of energy/utility management, industrial automation, smart logistics (advanced telematics), smart grid and metering, smart consumer wearables, environmental management, intelligent surveillance and video analytics, smart retail
Power efficiency	Efficient power requirements for massive multiple-input, multiple-output (MIMO), small cell implementation	Leads to lower costs and enables massive internet of things	



THE ELECTROMAGNETIC SPECTRUM



O 5G

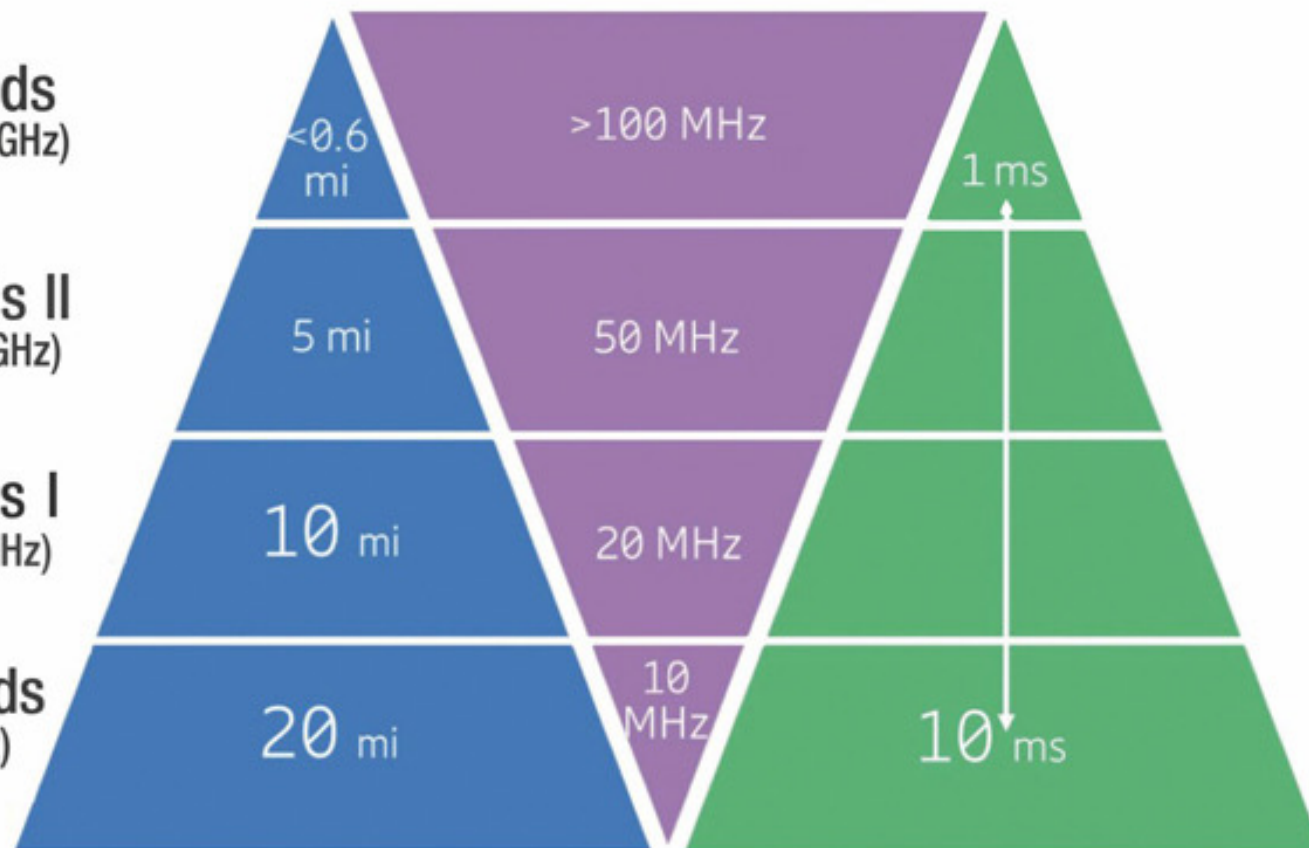
- Padrão criado pela 3GPP para substituir a tecnologia 4G com início de despregue global em 2019;
- Diversas vantagens, a mais proeminente o alto desempenho (10Gpbs);
 - Por comparação, cabos oceânicos mais rápidos do mundo em torno de 100.000Gbps, mas na prática a disponibilidade típica é de segmentos de 100Gps – problemas?
- Competição com ISP's tradicionais para computadores;
- Desempenho adicional advém do uso de frequências EM mais altas, mas que possuem propagação muito menor, então 5G prevê três padrões em um:
 - Baixa (600-700Mhz), que basicamente é o 4G entrega (30-250Mbps);
 - Média (2.5-3.7GHz), com desempenho de 100-900Mbps, alcance de alguns KM;
 - Alta (25-30GHz), com desempenho até 10Gpbs, alcance de metros;

High bands
(24 GHz - 48 GHz)

Mid bands II
(3.5 GHz - 7 GHz)

Mid bands I
(1 GHz - 2.6 GHz)

Low bands
(Sub-1 GHz)



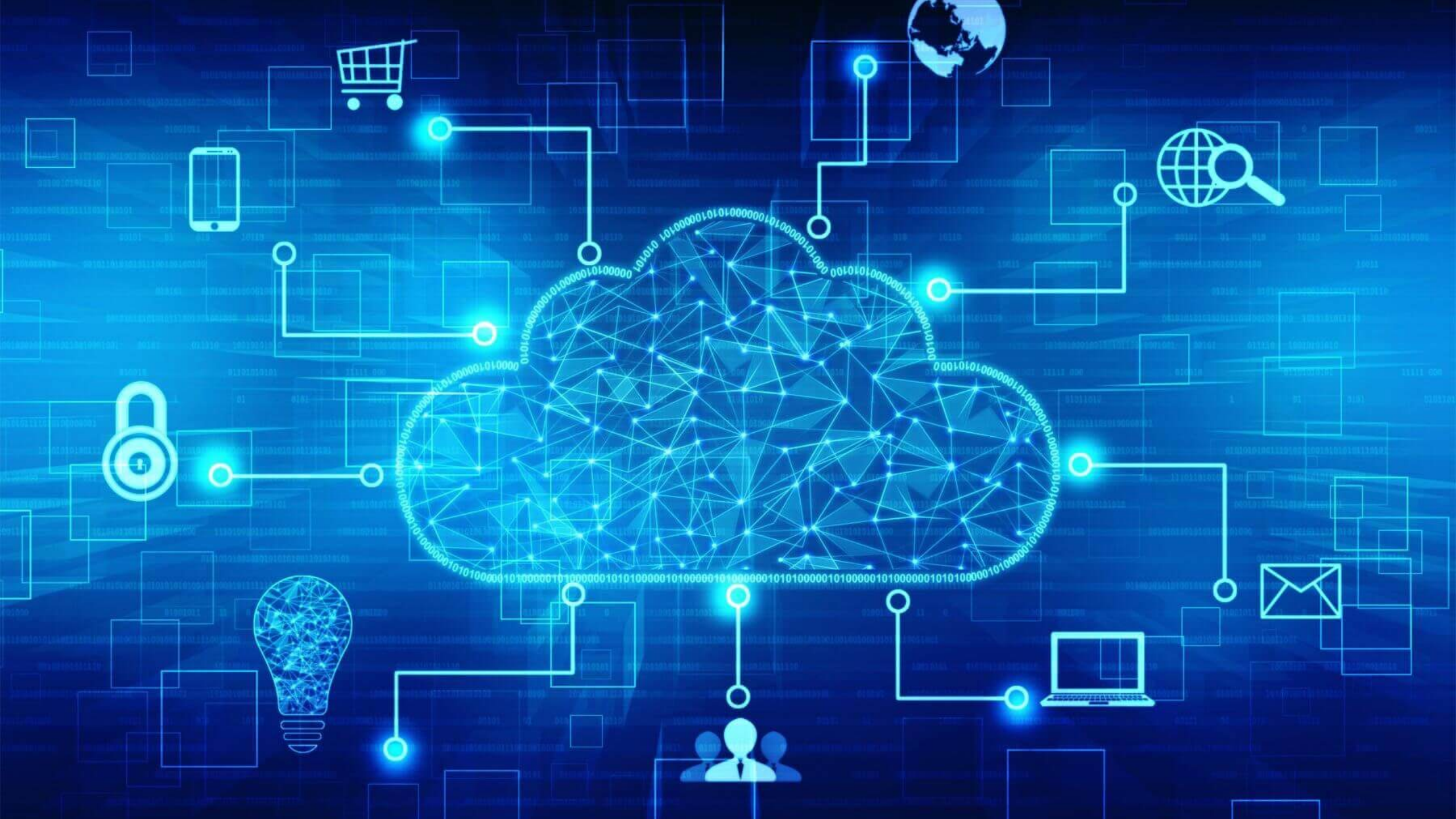
Coverage*

Bandwidth*

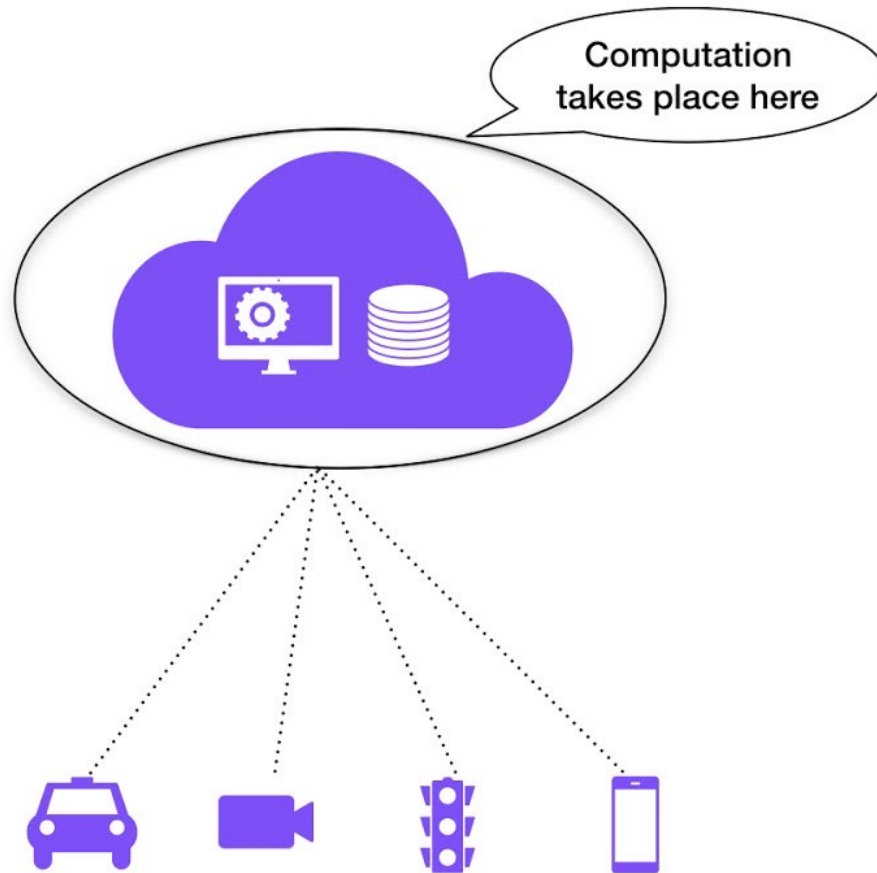
Latency*

High capacity
hotspot/ dense
urban

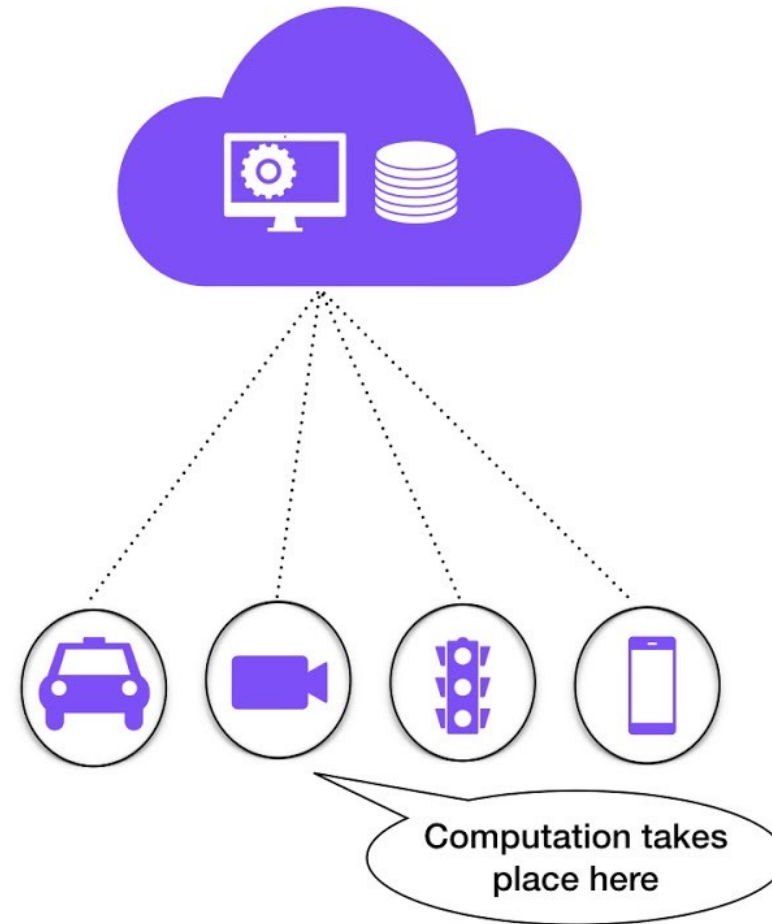
Moderate
capacity
Wide area/
outside-in
coverage



Cloud Computing



Edge Computing







KANGDUO

KANGDUO



Portal da Transparência

CONTROLADORIA-GERAL DA UNIÃO

Busque por órgão, cidade, CNPJ, servidor...



[Sobre o Portal](#) | [Painéis](#) | [Consultas Detalhadas](#) | [Controle social](#) | [Rede de Transparência](#) | [Receba Notificações](#) | [Aprenda mais](#)

VOCÊ ESTÁ AQUI: INÍCIO » DESPESAS » CONSULTA » DOCUMENTOS DE EXECUÇÃO DA DESPESA PÚBLICA » DOCUMENTO

Detalhamento do documento de Pagamento

ORIGEM DOS DADOS

Nº do documento

2019NS005688

Data

03/12/2019

Descrição

NOTA DE LANÇAMENTO DE SISTEMA (NS)

Fase

PAGAMENTO

Tipo de documento

NÃO SE APLICA

Valor do documento

-

Observação do documento

LIQUIDACAO/PAGAMENTO REFERENTE INVOICE 200118 - CODEMP: S4266 - CRYPTO AG: PV49000-2019-00002 - OMC/OMS/OMD: 49000 - MSG DE AUT DE PAGAMENTO: R-132143Z/NOV/2019 DE COMTIM - 2019OP002116.

DADOS DO FAVORECIDO

CPF/CNPJ/Outros

EX9300367

Nome

CRYPTO AG

DADOS DO ÓRGÃO PAGADOR

Órgão Superior

52000

MINISTÉRIO DA DEFESA

Órgão / Entidade Vinculada

52131

COMANDO DA MARINHA

Unidade Gestora

770100

COMISSAO NAVAL BRASILEIRA NA
EUROPA - LONDRES

Gestão

00001

TESOURO NACIONAL





Russo-Georgian War



Russian Hybrid Tactics in Georgia

Niklas Nilsson

SILK ROAD PAPER
January 2018



Central Asia- Caucasus Institute
Silk Road Studies Program

