ICS cybersecurity and media (mis)information. The media's role and how it influences perceptions

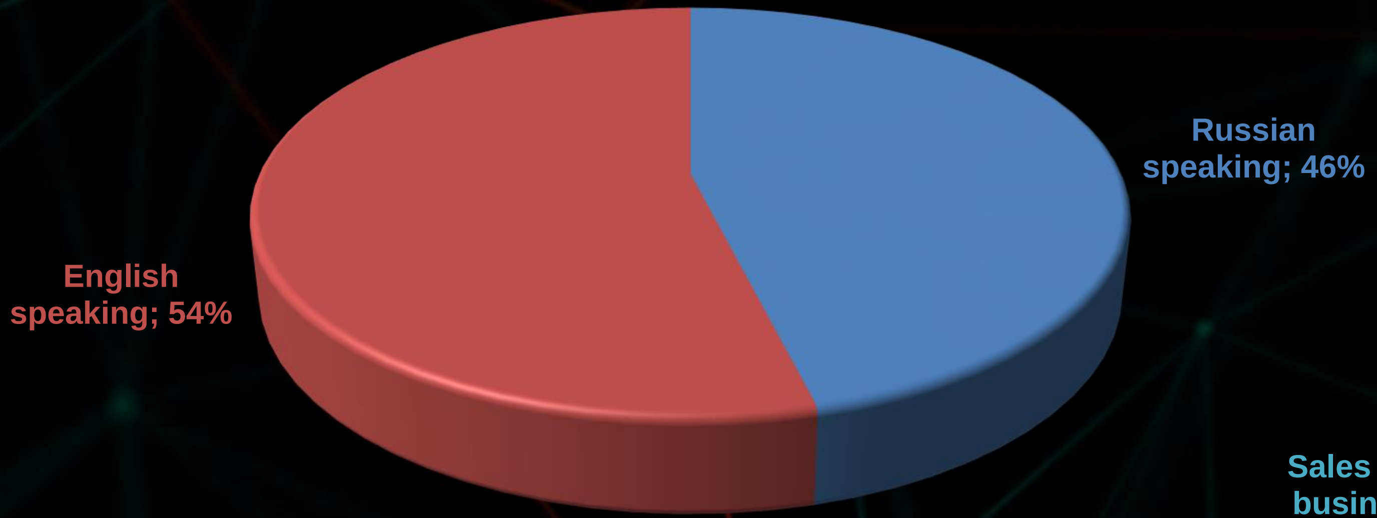
Yuliya Dashchenko
Kaspersky Lab ICS CERT

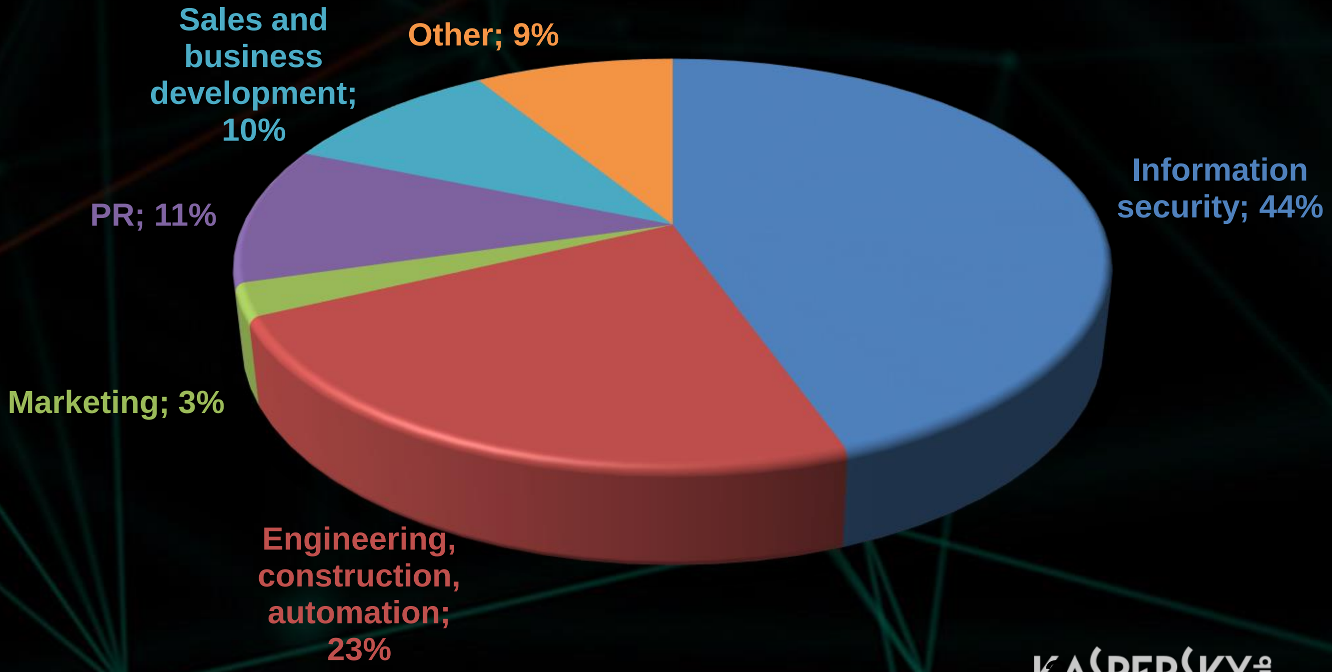
Vladimir Dashchenko
Kaspersky Lab ICS CERT

Intro

- Why did we start this research?
- How does information from the mass media/open sources influence public opinion in terms of ICS Security?
- How much do people trust information from the mass media/open sources and what affects their trust?

The survey



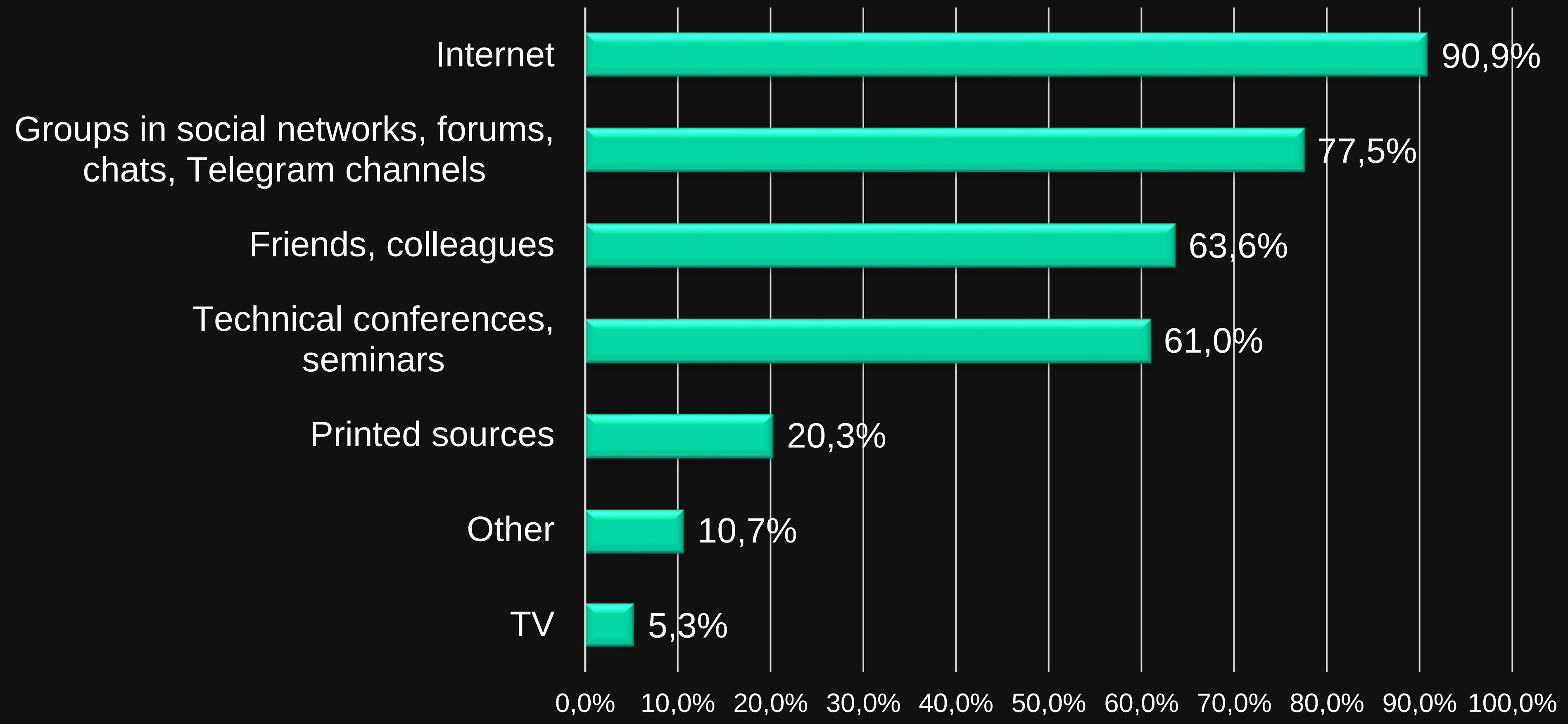


Total: 193 respondents

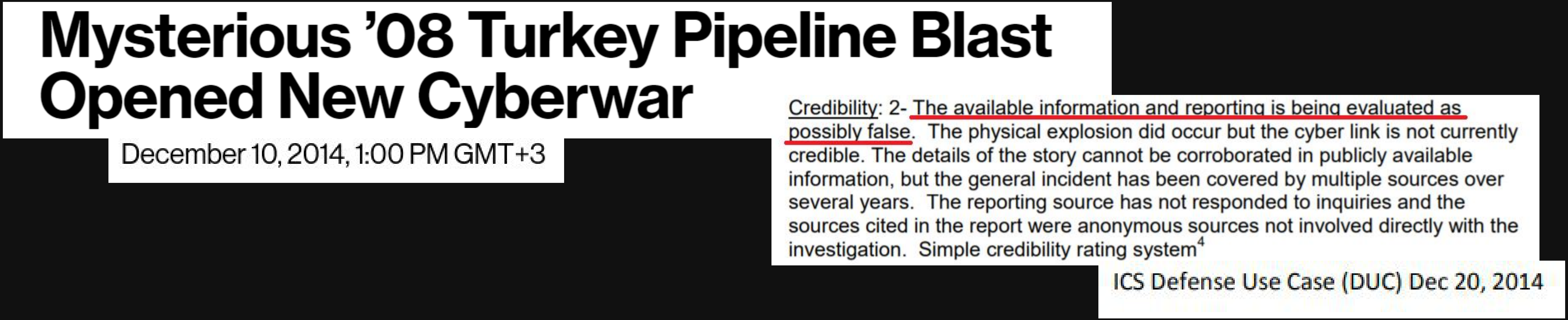
Good things about media and open-source information

- Raising awareness
- Highlighting cybersecurity problems and helping to solv them
- Pushing the development of regulatory frameworks

Sources of information



Headline Kung-Fu

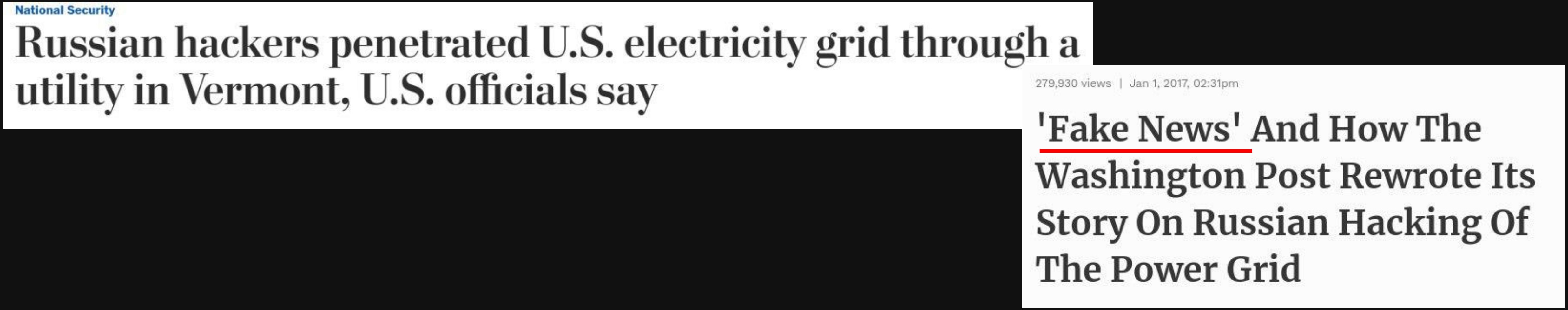


Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar

December 10, 2014, 1:00 PM GMT+3

Credibility: 2- The available information and reporting is being evaluated as possibly false. The physical explosion did occur but the cyber link is not currently credible. The details of the story cannot be corroborated in publicly available information, but the general incident has been covered by multiple sources over several years. The reporting source has not responded to inquiries and the sources cited in the report were anonymous sources not involved directly with the investigation. Simple credibility rating system[4]

ICS Defense Use Case (DUC) Dec 20, 2014



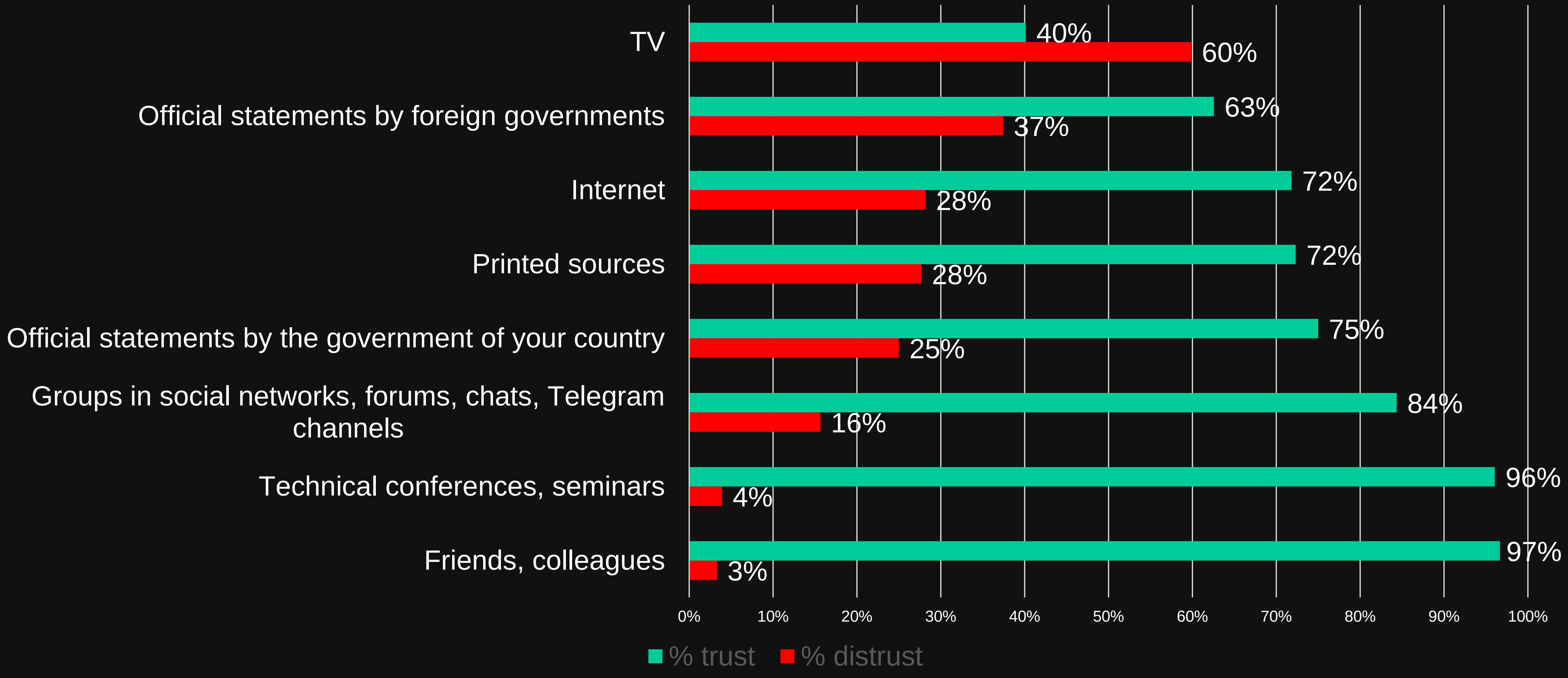
National Security

Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say

279,930 views | Jan 1, 2017, 02:31pm

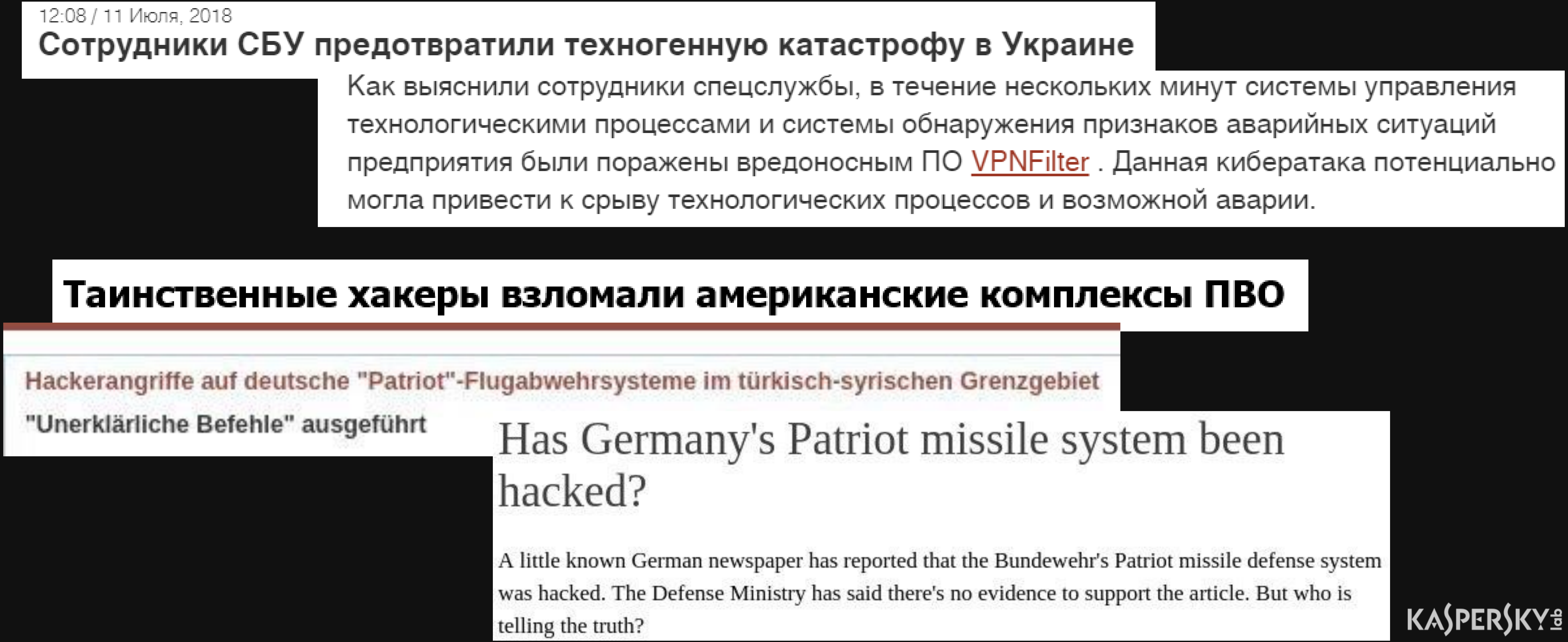
'Fake News' And How The Washington Post Rewrote Its Story On Russian Hacking Of The Power Grid

Level of trust in sources



Exaggeration!

- Main goal – attract the audience! And it changes the sense sometimes
- Headlines do not reflect the reality



12:08 / 11 Июля, 2018

Сотрудники СБУ предотвратили техногенную катастрофу в Украине

Как выяснили сотрудники спецслужбы, в течение нескольких минут системы управления технологическими процессами и системы обнаружения признаков аварийных ситуаций предприятия были поражены вредоносным ПО VPNFilter . Данная кибератака потенциально могла привести к срыву технологических процессов и возможной аварии.

Таинственные хакеры взломали американские комплексы ПВО

Hackerangriffe auf deutsche "Patriot"-Flugabwehrsysteme im türkisch-syrischen Grenzgebiet

"Unerklärliche Befehle" ausgeführt

Has Germany's Patriot missile system been hacked?

A little known German newspaper has reported that the Bundewehr's Patriot missile defense system was hacked. The Defense Ministry has said there's no evidence to support the article. But who is telling the truth?

Top trends, problems and fears

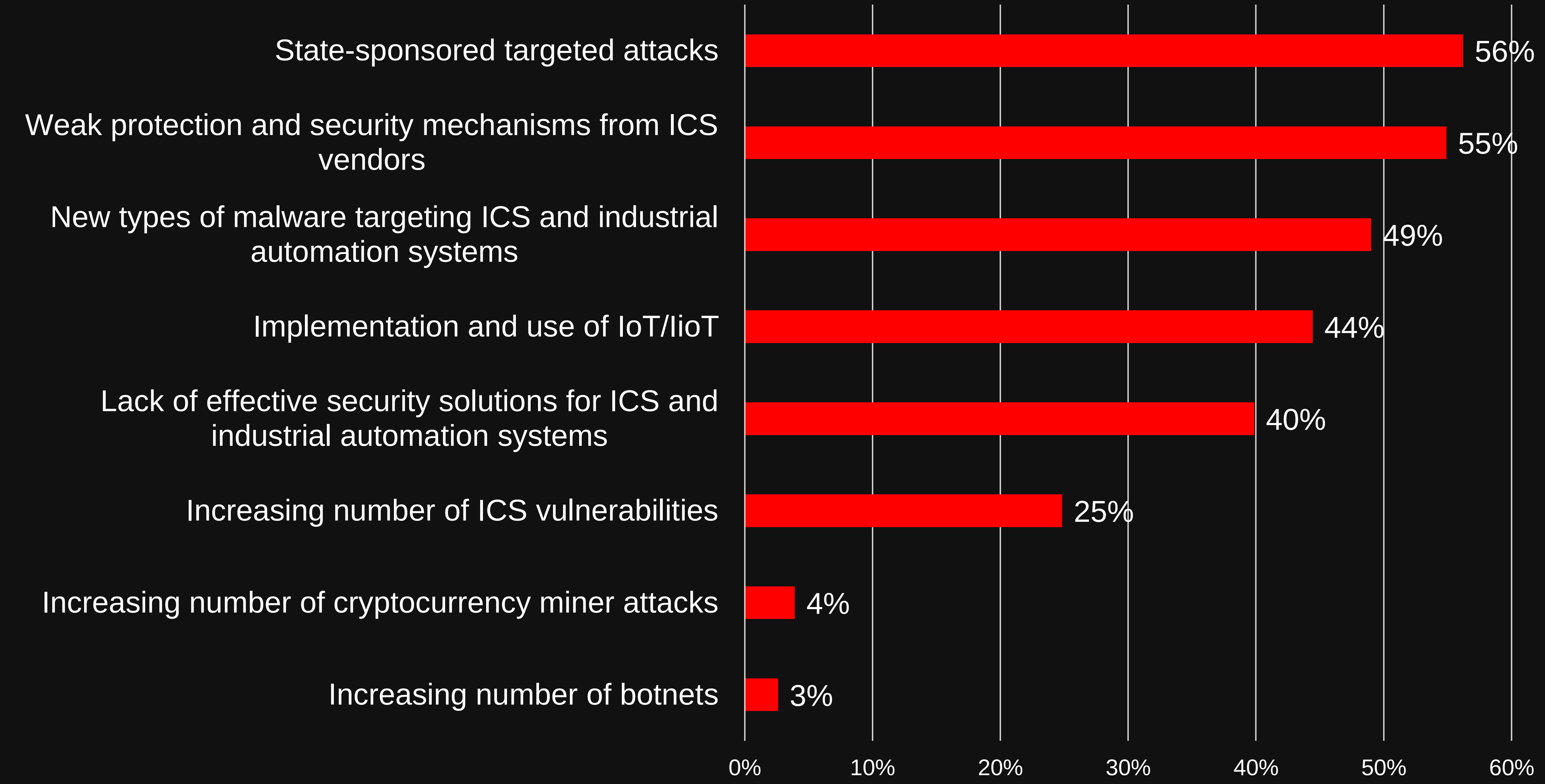
IoT/IIoT

ers

Stat

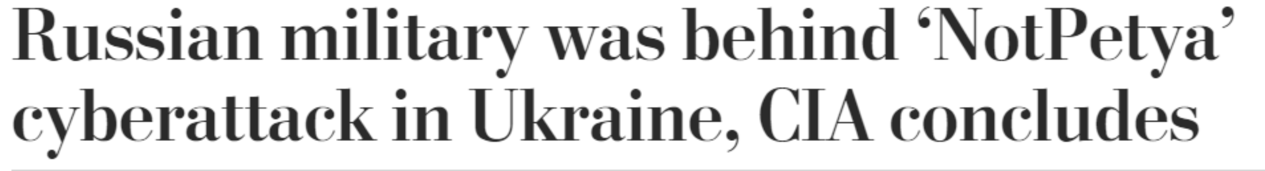
cks

Real problems

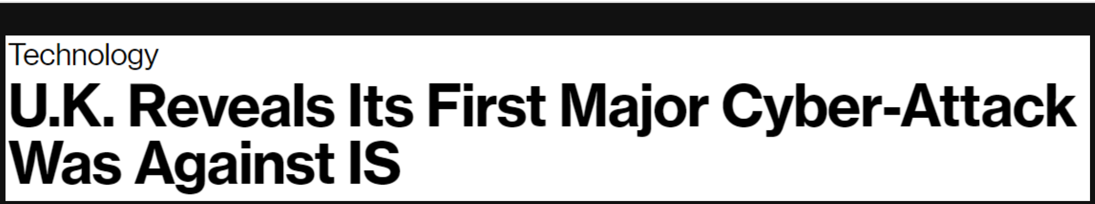


KASPERSKY lab

Way too much politics in the cyberspace

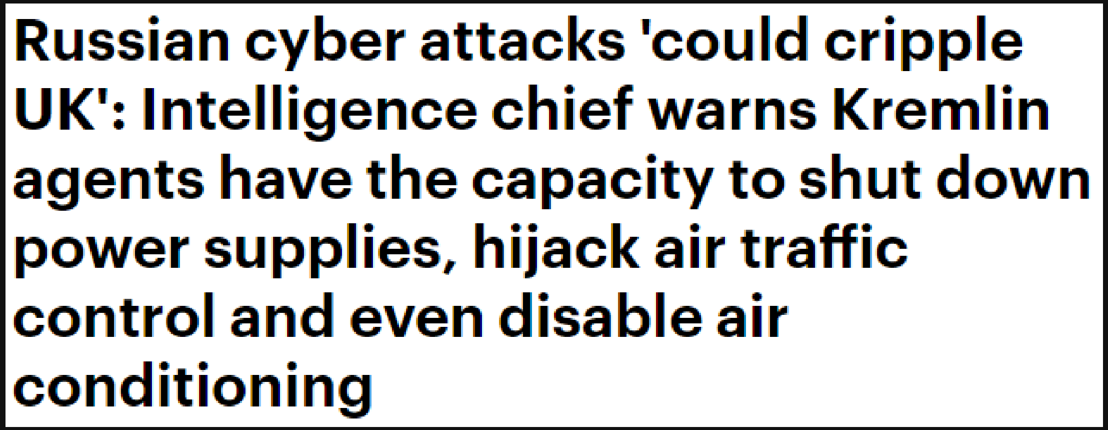


Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes

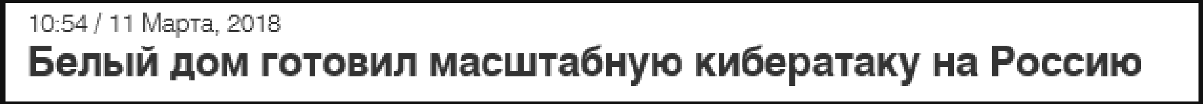


Technology

U.K. Reveals Its First Major Cyber-Attack Was Against IS

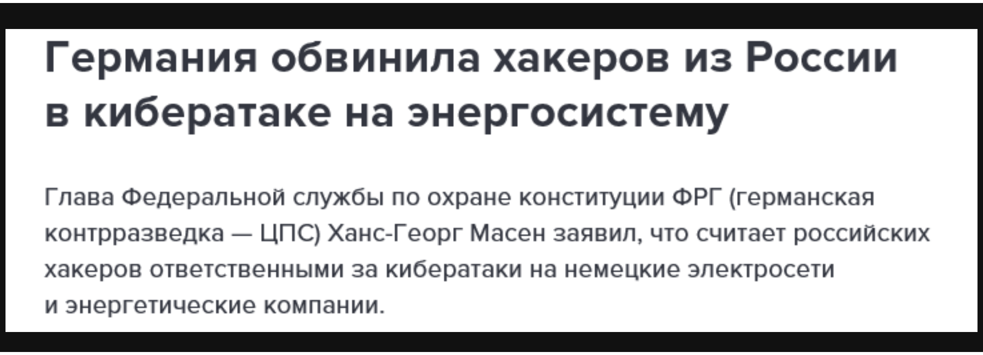


Russian cyber attacks 'could cripple UK': Intelligence chief warns Kremlin agents have the capacity to shut down power supplies, hijack air traffic control and even disable air conditioning



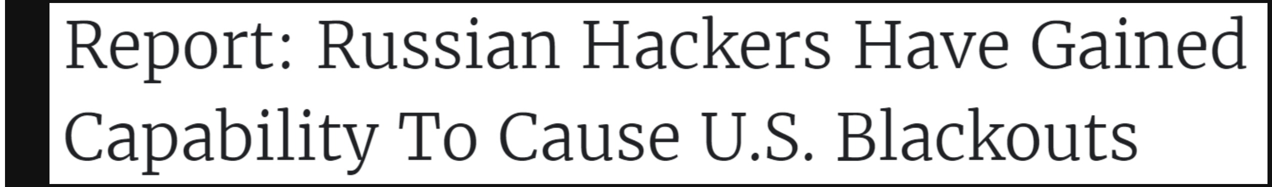
10:54 / 11 Марта, 2018

Белый дом готовил масштабную кибератаку на Россию

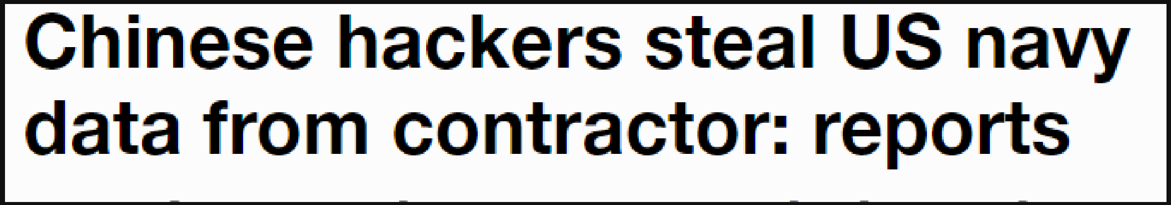


Германия обвинила хакеров из России в кибератаке на энергосистему

Глава Федеральной службы по охране конституции ФРГ (германская контрразведка — ЦПС) Ханс-Георг Масен заявил, что считает российских хакеров ответственными за кибератаки на немецкие электросети и энергетические компании.



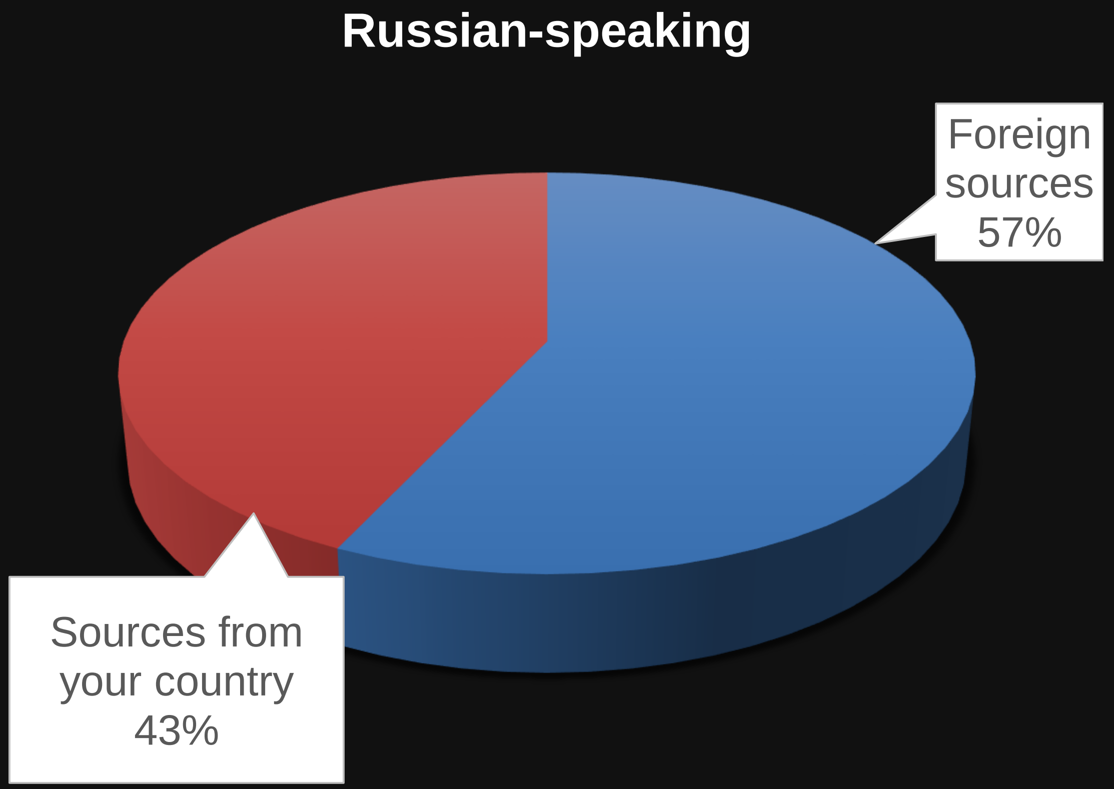
Report: Russian Hackers Have Gained Capability To Cause U.S. Blackouts

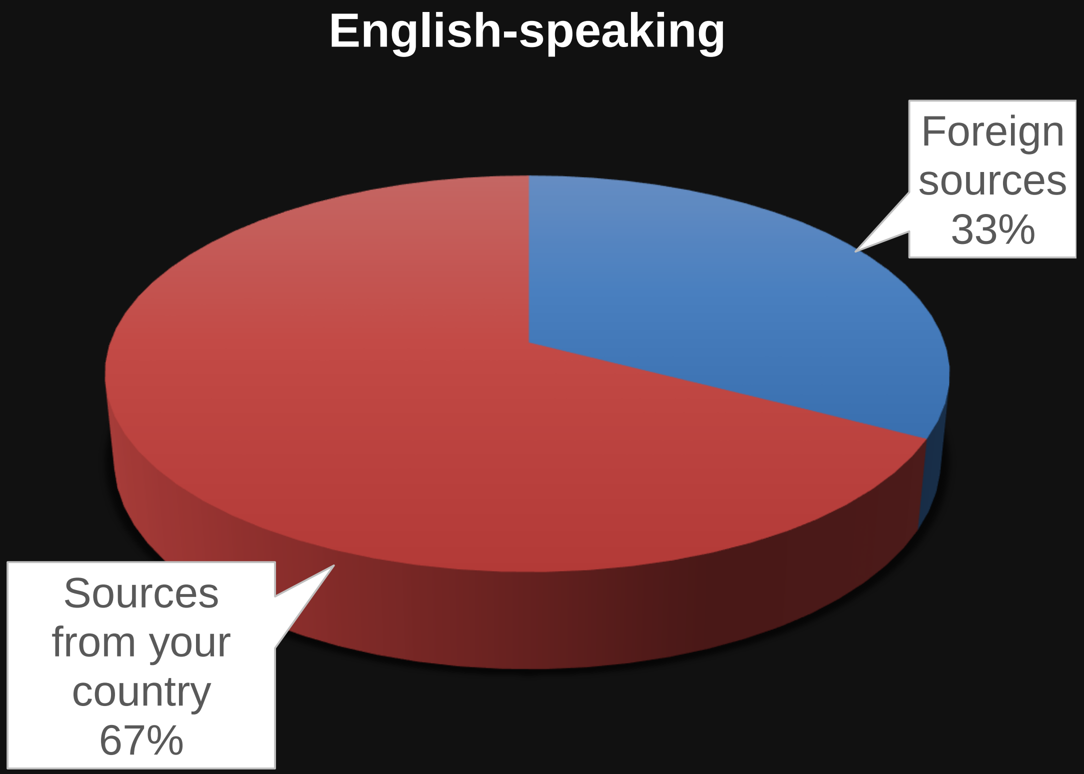


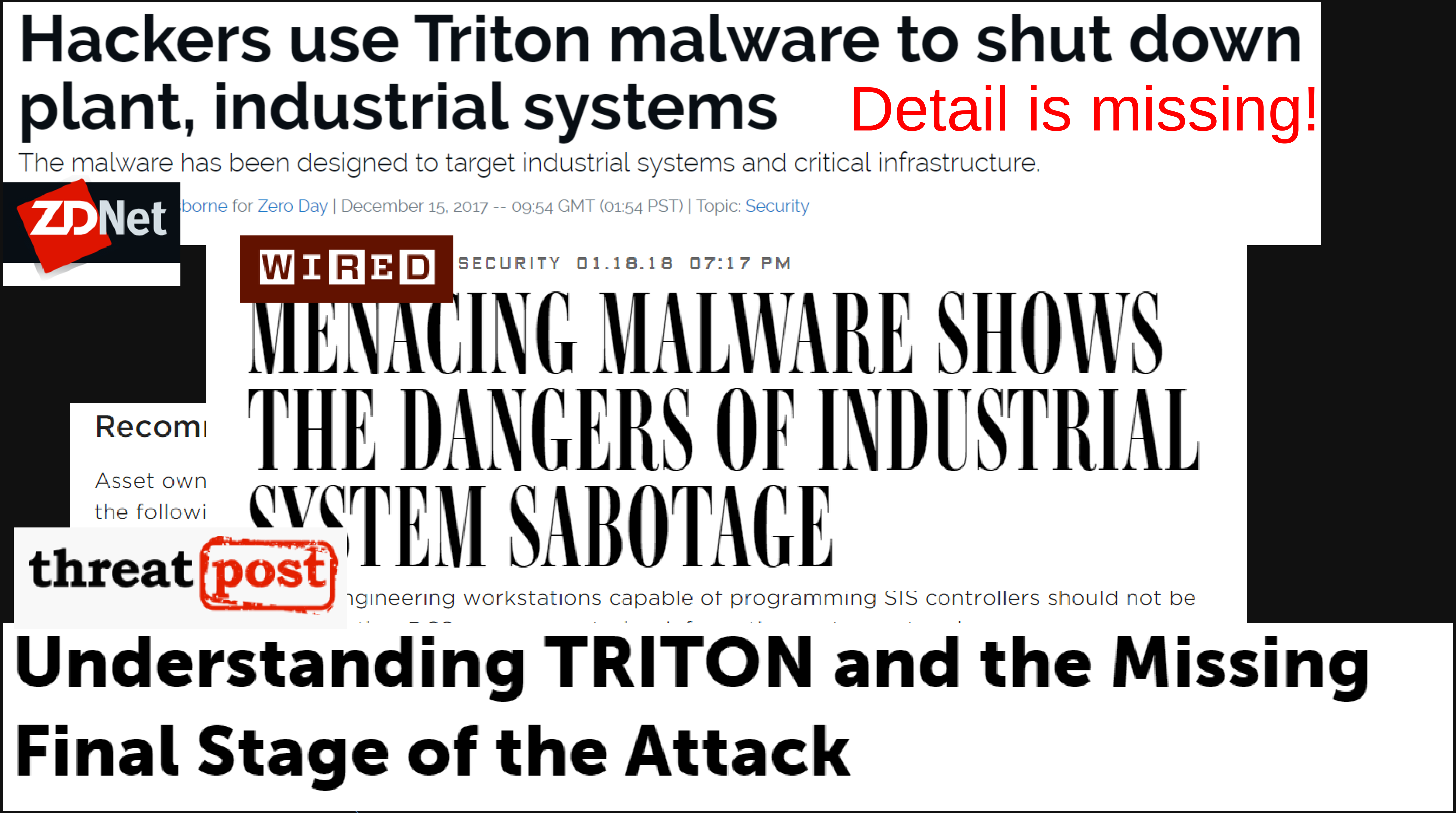
Chinese hackers steal US navy data from contractor: reports

- yet another instrument of political propaganda
- a weapon in information wars between countries
- news + general political tensions -> negative attitude towards "hostile" countries among ordinary people

Priority of trust: local sources VS foreign sources







Hackers use Triton malware to shut down plant, industrial systems

Detail is missing!

The malware has been designed to target industrial systems and critical infrastructure.

borne for Zero Day | December 15, 2017 -- 09:54 GMT (01:54 PST) | Topic: Security

SECURITY 01.18.18 07:17 PM

MENACING MALWARE SHOWS THE DANGERS OF INDUSTRIAL SYSTEM SABOTAGE

Recomm

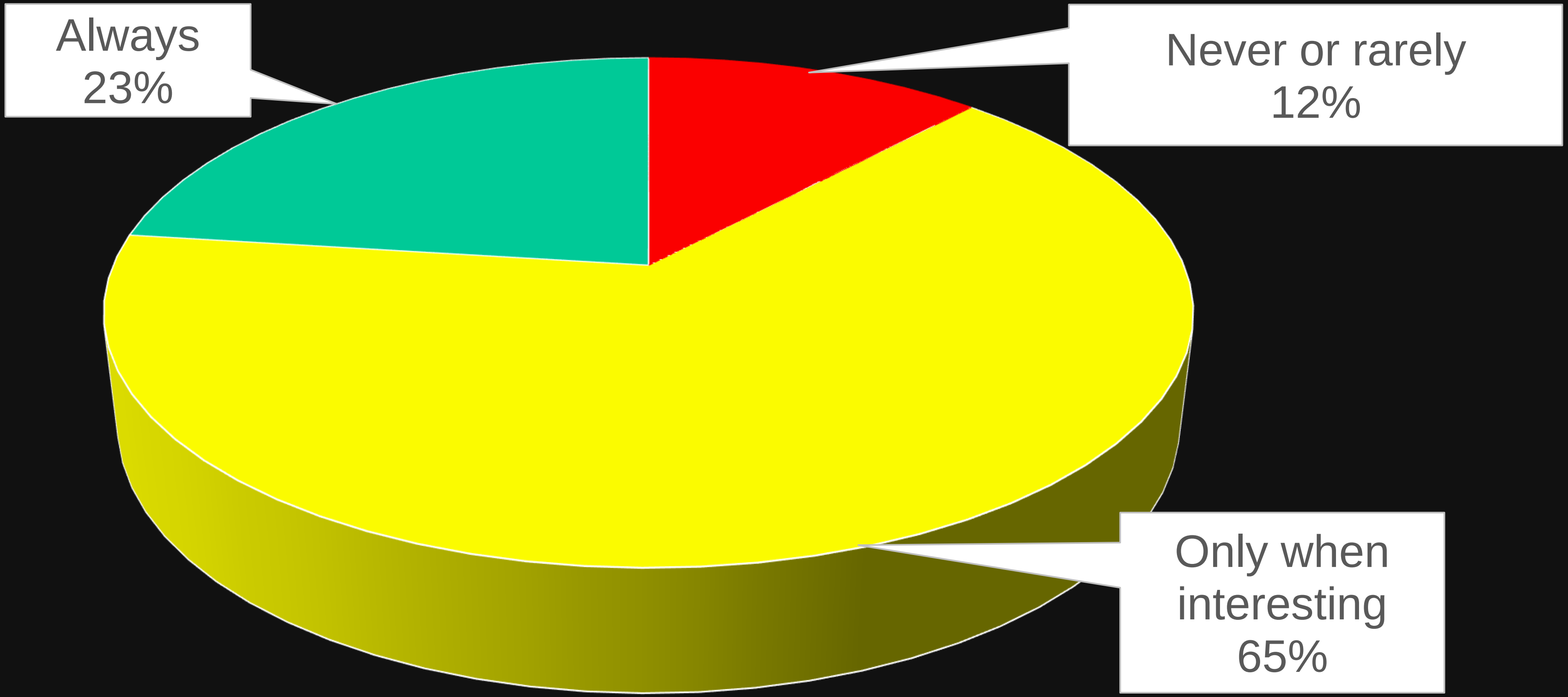
Asset own

the followi

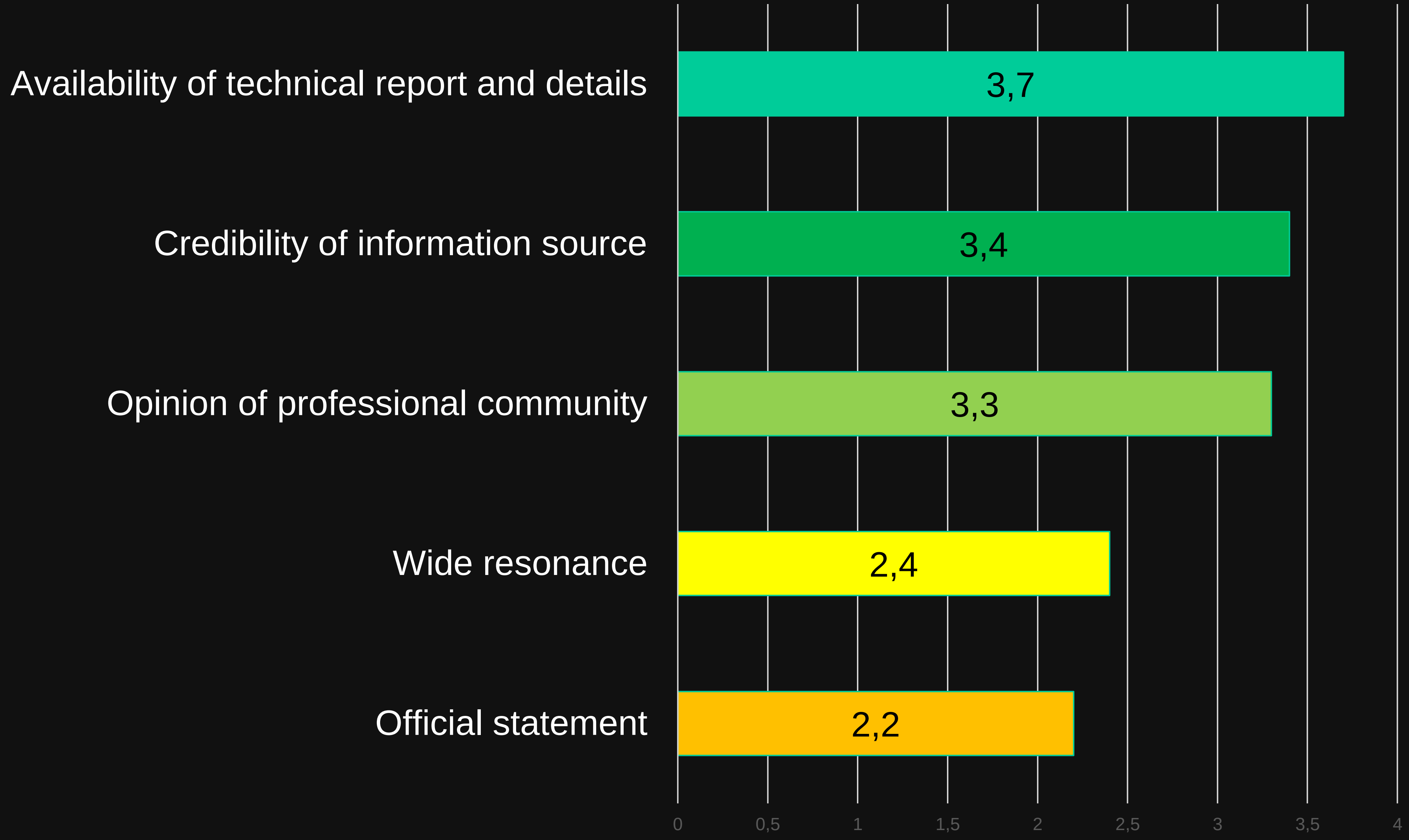
ngineering workstations capable of programming SIS controllers should not be

Understanding TRITON and the Missing Final Stage of the Attack

Does the source matter?



Trust factors



Where’s the truth?

Methodology of trust measurement

Metric	Metric value	Numerical value	Metric	Metric value	Numerical value
Source authority	High Medium Low	1 0,8 0,5	Community opinion	Confirmed Discredit None	1 0,5 0
Technical details	High Medium Low None	1 0,8 0,5 0	Official statement	Confirmed None	1 0
Evidence	High Medium Low Unproven	1 0,8 0,5 0,2	Media resonance	High Medium Low	1 0,8 0,5

Trust formula

$$\text{Score} = K_1 * \text{Authority} + K_2 * (\text{TechDetails} + \text{Evidence})/2 + K_3 * \text{ComOpinion} + K_4 * \text{OfStatement} + K_5 * \text{Resonance}6$$

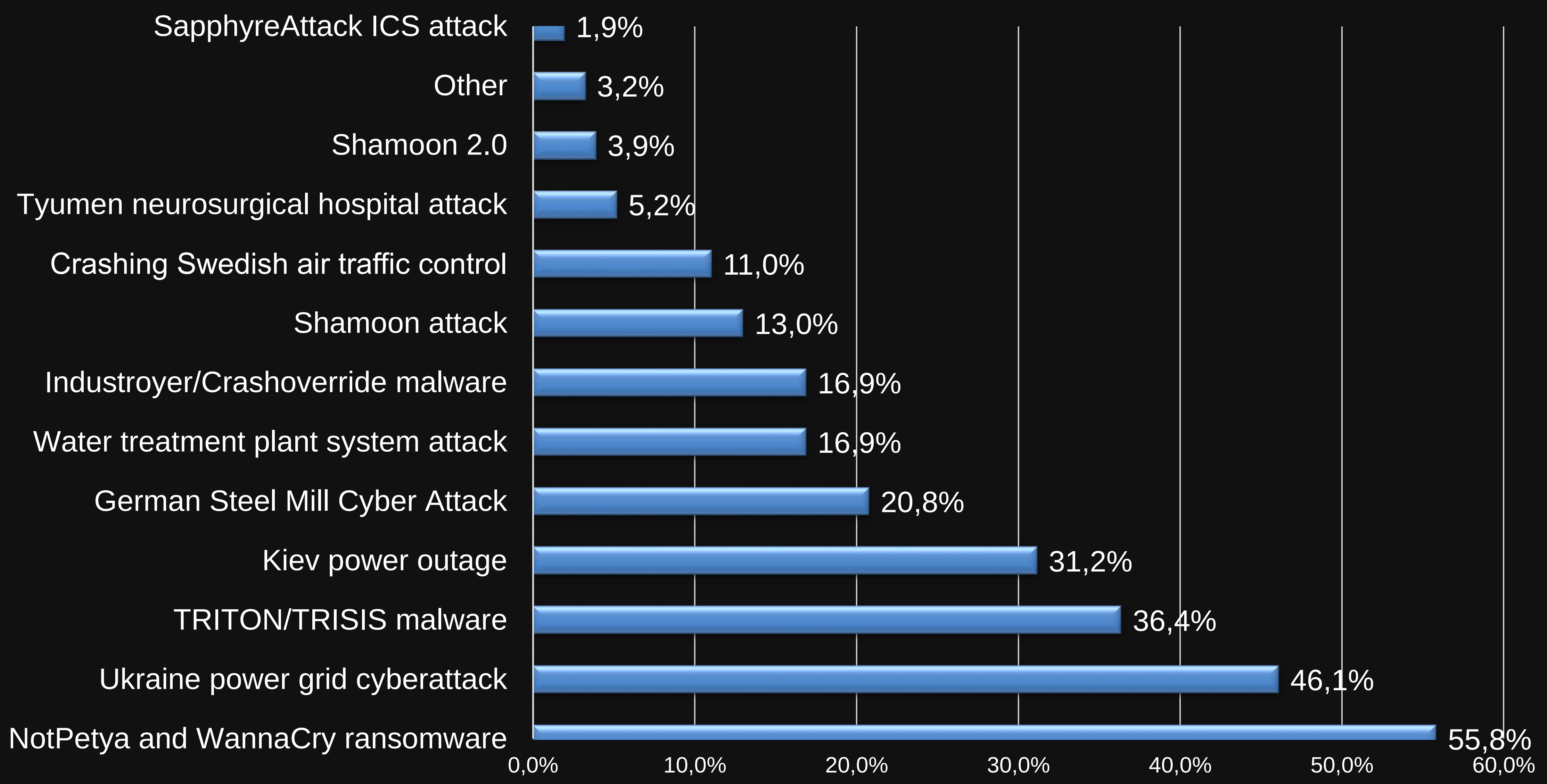
where Ki – trust factors

Metric	Trust factor	Metric	Trust factor
Source authority	2,2	Community opinion	2,1
Technical details	2,5	Official statement	1,6
Evidence		Media resonance	1,6

Trust level	Low	Medium	High
Score	0 – 4,9	5 – 6,9	7 – 10

Let’s measure!

Highest-profile incidents



Applying the methodology

Incident	Authority	TechDetails	Evidence	ComOpinion	OfStatement	Resonance	Score
Ukraine power grid cyberattack	1	1	1	1	1	1	**10**
Kiev power outage	0,8	0,5	0,5	1	1	1	**8,31**
Shamoon 2.0	1	1	1	1	1	0,5	**9,2**
Crashing Swedish air traffic control	0,5	0	0	0,5	1	0,8	**4,48**

Conclusion

- Open source information influences perceptions. Not only in a good way
- Only trust the technical facts
- Always look for the primary source
- Cyber-hygiene VS Trends
- Highest level of responsibility for our content

Hall of thanks

- Anton Shipulin
- Daniil Tameev
- Ekaterina Odnostorontseva
- PR team
- Kaspersky Lab ICS CERT team

Let’s talk!

Yuliya Dashchenko
Yuliya.Dashchenko@kaspersky.com

Vladimir Dashchenko
Vladimir.Dashchenko@kaspersky.com

ics-cert.kaspersky.ru
www.kaspersky.com