12

Fundamental Cyber Security Problems

Boris Taratine

and

Ganna Pogrebna

first published on cyberbitsetc.org

ACE CSR Winter School

December 14-16, 2020

in association with
National Cyber Security Centre

Setting the Challenge

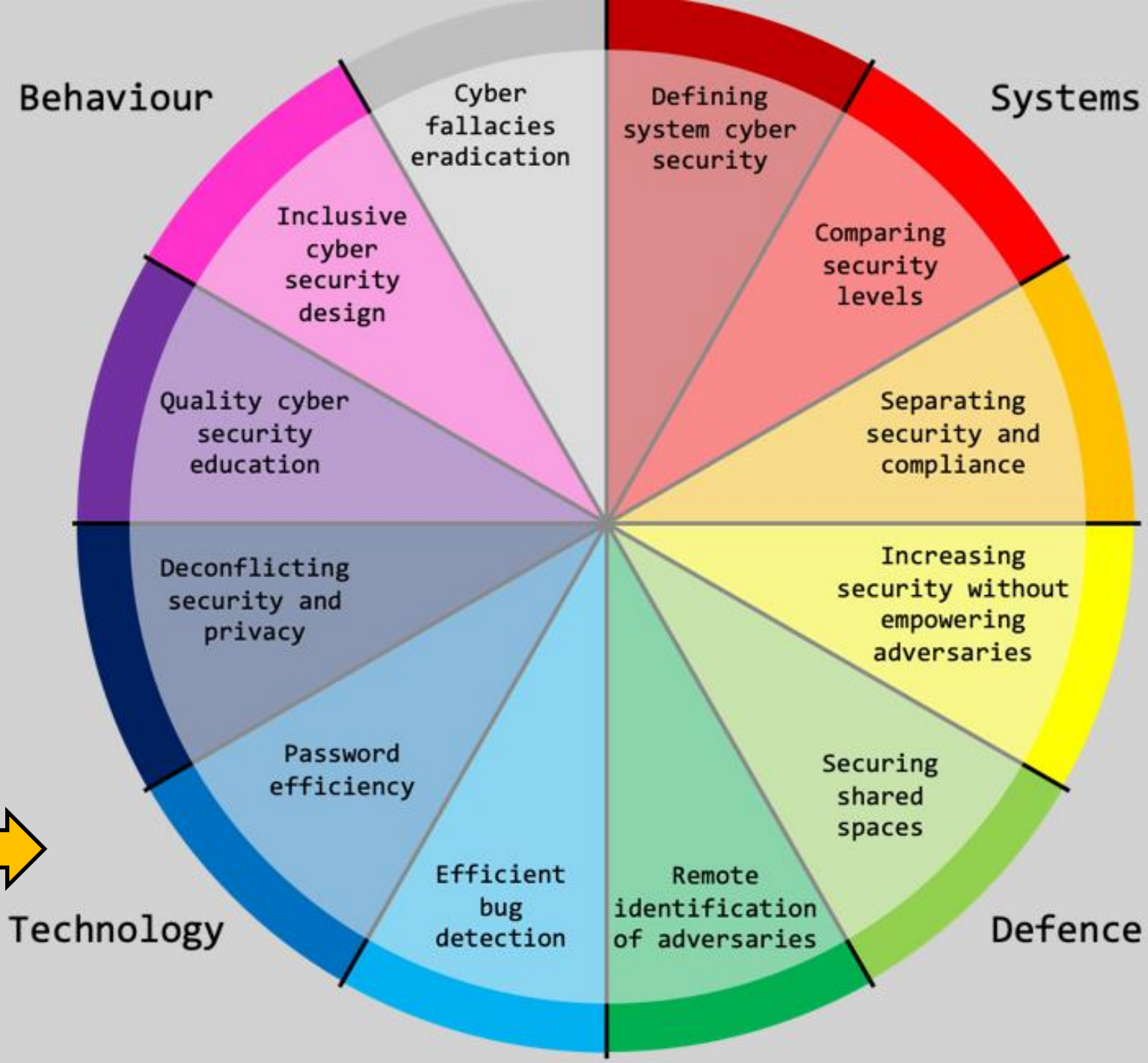
- For many centuries, the progress of humanity was fostered by setting up important goals for the future – the **major challenges** faced by the humankind
- Such goal-setting is important not only at the global level, but also **zooming in** on individual domains
- In 1900, David Hilbert presented a set of important problems in mathematics - these problems **outlined the roadmap** for many years and some of them still remain **unresolved**
- In 2015, the UN set up 17 goals to reach a "better" world by 2030 with no poverty or hunger, tackle climate change, etc. - yet, **none** of these goals target cyber space

Fundamental Cyber Security and Cyber Defence Problems

12 fundamental problems organised in **4 clusters**

- the ticking clock of the future cyber security

Our challenge for you



System Problems

1. How to consistently define the security of a system and the methods to demonstrate it?

Defining system cyber security: While many definitions exist, coming up with a universal set of necessary and sufficient characteristics of what constitutes as secure system is a fundamental challenge of the future.

System Problems

2. How to compare the relative security of two systems?

Comparing security levels: We know very little about how to conduct the relative comparisons between several systems in terms of their cyber security, that yet to be defined too.

System Problems

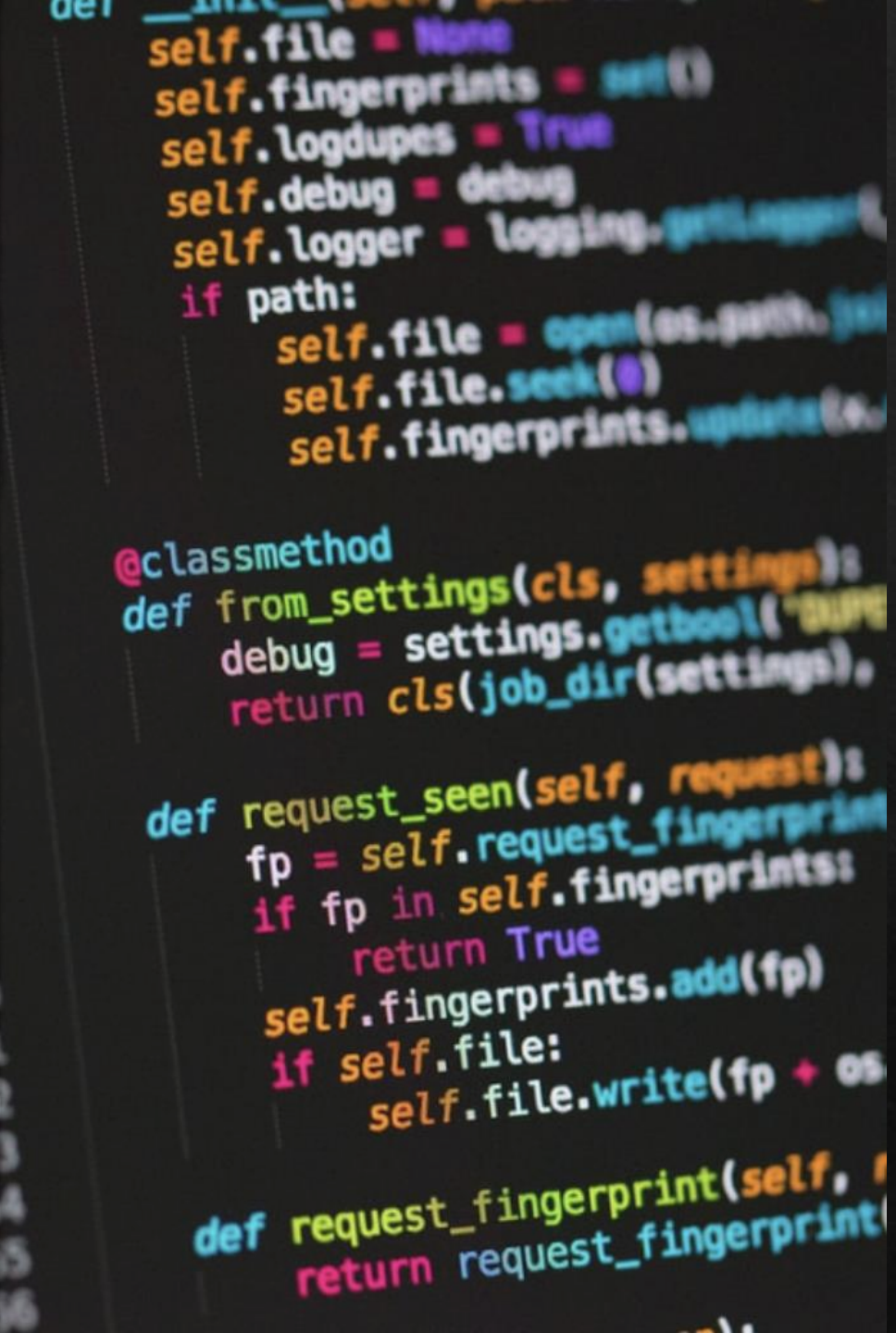
3. What is the relationship between the security of a system and its compliance to an arbitrarily chosen cyber security framework?

Separating security and compliance: Organizations make their systems compliant with various cyber security frameworks. Yet, the number of cyber security breaches increase year by year suggesting that compliance does not increase systems' security.

Defence Problems

4. How to strengthen the security of a system without increasing strength of its adversary?

Increasing security without empowering adversaries: Advances in cyber security become known to the cybercriminals almost immediately. Therefore, increased security often makes adversaries stronger. One of the main challenges is to find ways in which security can be achieved without raising the adversarial competence.



Defence Problems

5. How to identify and prevent the adversary's code from running on shared hardware / environment?

Securing shared spaces: In a shared environment, the possibility does not equal zero because the hardware does not have a moral imperative to tell the “good” and “bad” apart and the software that offers separation cannot be proven perfect. This makes the question of safety of shared environments opened.

Defence Problems

6. How to remotely tell apart the legit user of a remote system and an adversary who remotely controls the system when this system is compromised?

Remote identification of adversaries: Even the ever-popular so-called “zero-trust” does not consider this problem or offers a reliable solution.

Technology Problems

7. How to identify and eliminate finite number of all bugs in the arbitrary program code?

Efficient bug detection: Vulnerabilities may remain dormant for years even in open source code. Exploitable vulnerability is an often cause for successful compromise. Eradicating the bugs will eradicate the large class of attacks.

Technology Problems

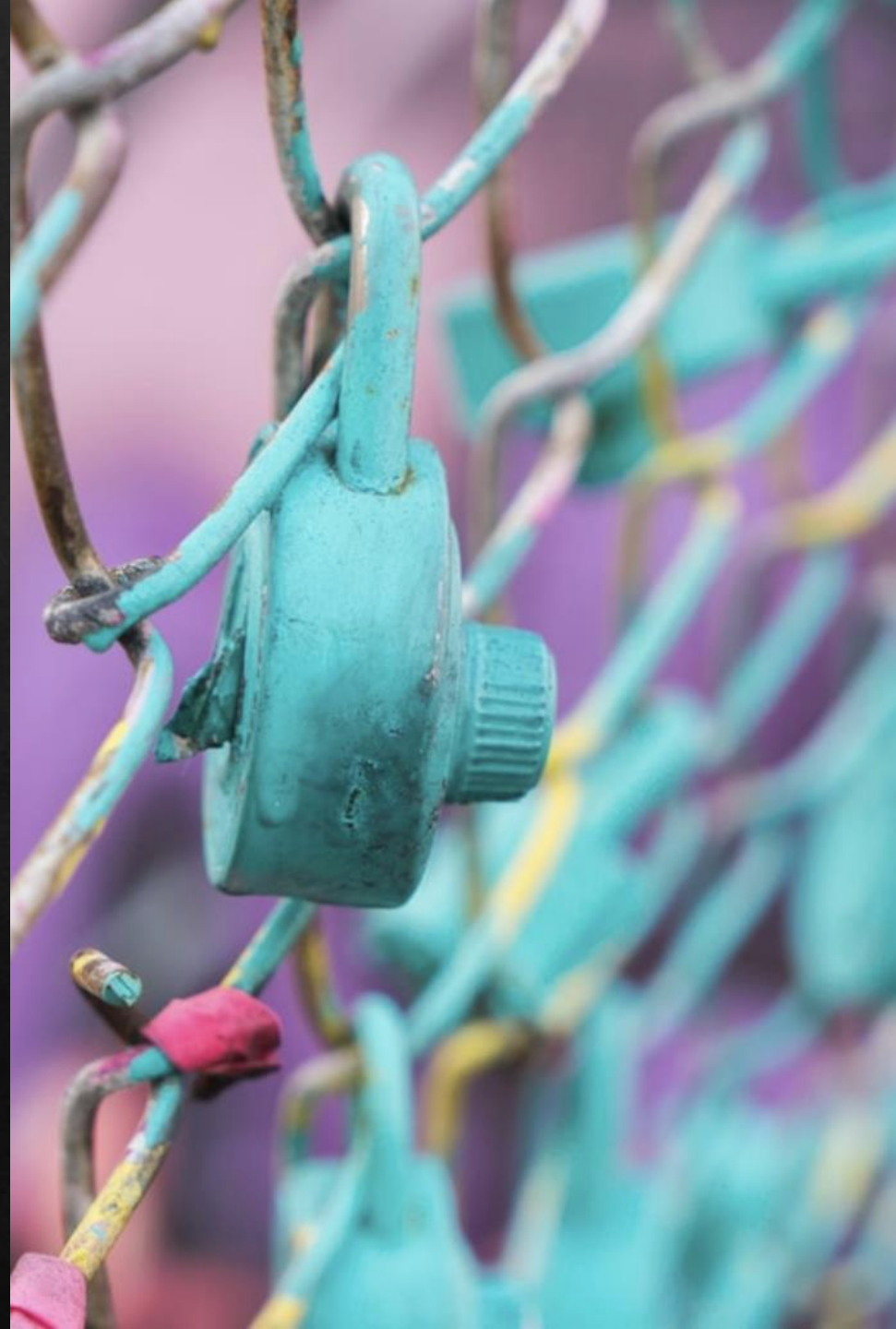
8. How to compare the strength of two passwords against a non-brute force compromise?

Password efficiency: A random adversary facing a random user would unlikely make a successful guess should the password be not in the top popular passwords list. Finding the balance between the password strength and its appropriateness for various environments is an important problem for the future because a “something you know” factor would likely be in use for long.

Technology Problems

9. How to deconflict security and privacy?

Deconflicting security and privacy: Security is often achieved at the expense of privacy. Yet, is it really necessary to invade someone's privacy to make the system or an environment safer? Understanding whether and what can offer a solution to this problem is a key question.



Behavioural Problems

10. How to educate users to recognize, detect and avoid cyber security threats?

Quality cyber security education: Many of cyber security measures concentrate on improving technology. Yet, it is also necessary to improve human understanding of cyber threats and educate people to deal with these threats more effectively.

Behavioural Problems

11. How do we make sure that security systems are understood by all users?

Inclusive cyber security design: Cyber security measures are often not accessible to an average user as they are often too complex. Providing simple and accurate explanations to sophisticated cyber rationales is necessary for building inclusive cyber security systems.

Behavioural Problems

12. How to eradicate justification of the security measures by narrative fallacies?

Cyber fallacies eradication: Many arguments in cyber security are built on logical fallacies. For example, “zero trust” cyber security is built on “never trust always verify” principle, which is impossible in principle due to the fact that a security system ultimately needs to trust something/someone. Avoiding such contradictions is necessary to prevent flaws in system design.

Our Study:

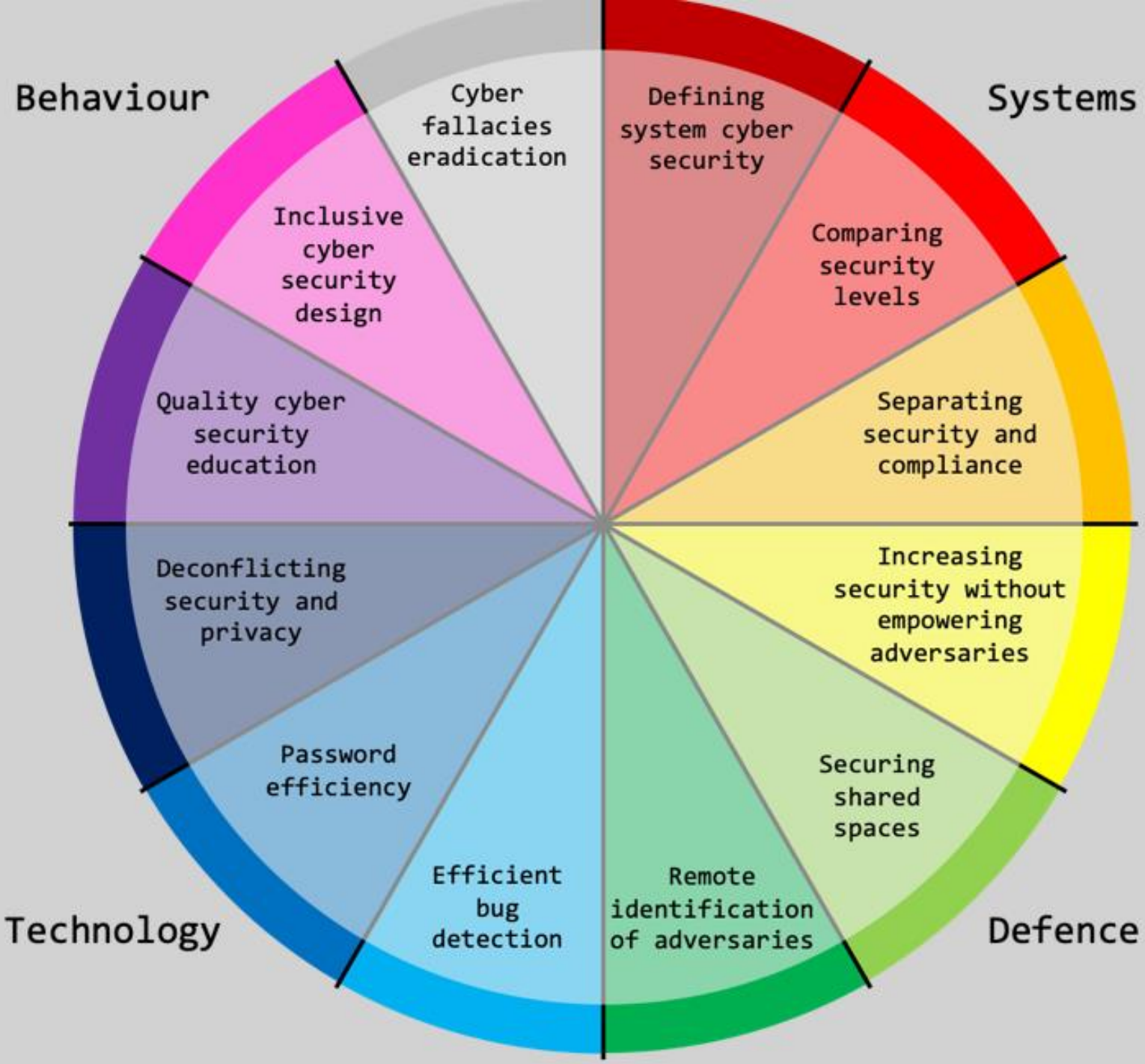
hot off the press!

Our study results

From out blog **CyberBitsEtc.org** we asked practitioners in our network to list up to 3 major cybersecurity problems for the 21st century

2658 people from **29 industries** took part in our study:

- **2498** mid-management and up
- **124** employee-level
- **36** consultants or had other background (e.g., academic researchers, etc.)



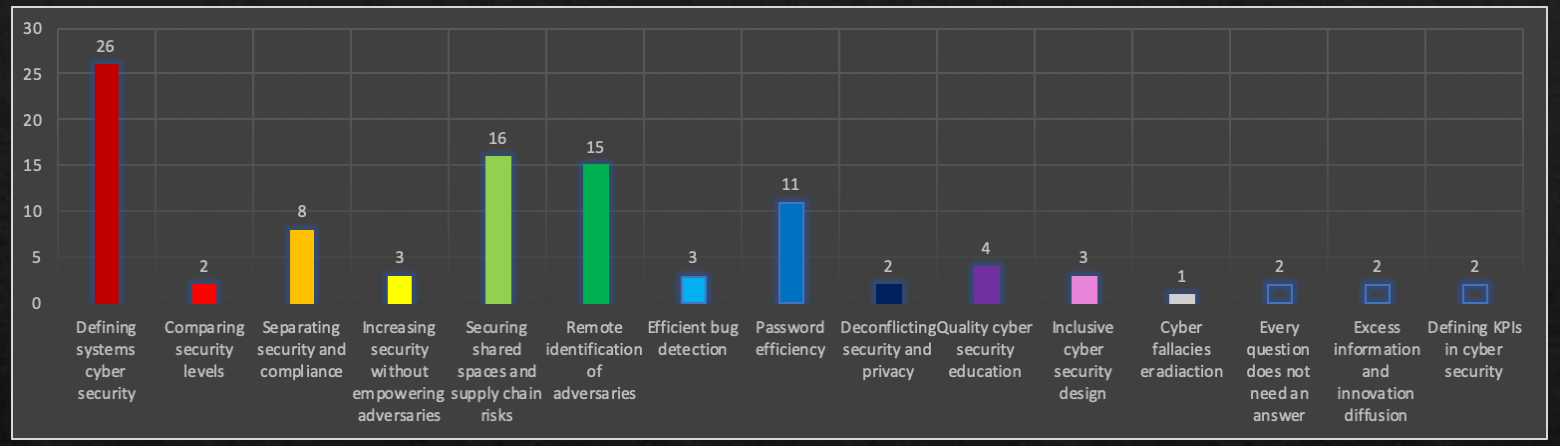
Our study results

We used unsupervised topic modelling approach (Latent Dirichlet Allocation or LDA) to map the topics

The analysis revealed **15 topics**:

- **11 of 12** problems mapped well onto the "wheel" as expected
- **1** problem had an additional aspect (i.e., supply chain risks)
- 3 problems were new

Frequency of problem occurrence in the sample (%)



Top 3 problems:

1. Defining systems cyber security
2. Securing shared spaces & supply chain risk
3. Remote Identification of adversaries

"New" problems:

- Every question does not have to be answered
- Excess information and innovation diffusion
- Defining KPIs in cyber security

Problems and Example Answers:

Defining systems cyber security	*Cybersecurity is like running the A&E of a major hospital. All of the best processes, best practices, best controls and best planning can fail you at any time when there is a virus outbreak and panic ensues. We need cybersecurity enough to keep "the lights on", to "keep the business in business", and to "stay ahead".*
Comparing security levels	*I am not sure how to compare security preparedness or security training between businesses or between divisions in my own organisation. It is an on-going struggle.*
Separating security and compliance	*There is much confusion between compliance and security and they are not the same.*
Increasing security without empowering adversaries	*I feel every time we make a progress we make cybercriminals stronger.*
Securing shared spaces and supply chain risks	*No matter how protected my stronghold is, there is always someone in my supply chain weak enough to cause me enough damage.*
Remote identification of adversaries	*Big problem is how to get to the top of cybercriminal supply chain remotely.*
Efficient bug detection	*We need more automation in simple tasks like bug detection, etc.*
Password efficiency	*Password policies are not realistic. Employee fail to remember their own passwords.*
Deconflicting security and privacy	*There is a huge trade-off between security and privacy. We need to access private information to understand or increase security, but is it always the right thing to do?*
Quality cyber security education	*Humans are getting tired of being careful*
Inclusive cyber security design	*We need to think of cyber security training for all - much of it only works for large organisations (not SMEs) and certain kind of employees*
Cyber fallacies eradiaction	*Many misconceptions in this area, which need proper education.*
Defining KPIs in cyber security	*KPIs are ill-defined. Security is often measured by the number of purchased or implemented tools and not by the number of breaches prevented, etc.*
Excess information and innovation diffusion	*Accepting "that's how everyone else says they do it" leads to a lack of innovation and a cheapest bid wins culture*
Every question does not need an answer	*Thinking that every question needs an answer leads to a lot of time wasted that could be spent on the innovation stifled*

We admit that we do not know all answers, however, we believe some of these goals can be set and achieved in our lifetime through interdisciplinary collaboration and public debate.

Boris Taratine

Principal Architect, Farsight Security Inc.

Boris Taratine is a passionate visionary and an influential ambassador of cybersecurity and cyber defence. He has been working with renowned companies across the Globe, was engaged in consulting with numerous organizations. During the decades of his career, he has held senior technical and leadership roles across several industries. Being a trusted adviser to the c-suite, he has helped global businesses understand the importance of cyber disciplines and take proactive actions for improvements. He is very analytical; his problem-solving skills are hard to match: he sees the roots of the problems through the elephants in the room. He is often at odds with the conventional wisdom that can be quite annoying until you understand the point. He actively promotes industry collaboration, participates in various industry forums, and is a frequent speaker at various industry events to influence global cybersecurity development. He volunteers his time advising to cybersecurity start-ups seeing a weakness in super-duper secure stuff whilst is still on napkin drawings - can be quite annoying too. Boris is the highest honour graduate at the Saint-Petersburg State University. During his Ph.D. studies, he co-authored a number of publications and patents granted under the NATO HiTech project; further has many publications and dozens of patents granted and pending. He is willing to share all the knowledge with anyone who wants to learn – this can be you.

Ganna Pogrebna

Professor Business Analytics and Data Science, Fellow at the Alan Turing Institute

Ganna Pogrebna is a Professor of Business Analytics and Data Science, ESRC-Turing Fellow and Lead for Behavioral Data Science at the Alan Turing Institute. Blending behavioral science, computer science, data analytics, engineering, and business model innovation, Ganna helps cities, businesses, charities, and individuals to better understand why they make decisions they make and how they can optimize their behavior to achieve higher profit, better social outcomes, as well as flourish and bolster their well-being. She is interested in analysing individual and group decision-making under risk and uncertainty (ambiguity) using laboratory experiments, field experiments and non-experimental data (specifically Big Data). She studies how decision-makers reveal their preferences, learn, co-ordinate and make trade-offs in static and dynamic environments. Her work aims to develop quantitative models capable of describing and predicting individual and group behaviour. Her research focuses on behavioural change for digital security. She published extensively on human behaviour and cyber security in peer-refereed journals. Her risk-tolerance scale for digital security (CyberDoSpeRT) received the British Academy of Management Award in 2018. She is also a winner of the 2019 TechWomen100 Award for her contribution to cybersecurity as a behavioural science.