RISCS Research Institute for Sociotechnical Cyber Security

The confusion of tongues: why cyber security professionals still talk past each other

This blog is written by the RISCS Associate Fellow Dr Ola Michalec. Ola is a social scientist based at the University of Bristol, researching technological expertise and collaboration in the context of digital innovation. She also leads the SPRITE+ "Communicating Cyber Security" community of interest and coordinates policy engagement activities at the REPHRAIN National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online.

Introduction

The 22nd of March was a typical early Spring day according to British standards: a kaleidoscope of drizzle, gusts, sunshine and seagulls welcomed over 50 delegates from across the country in Bristol's civic history and conference centre, M-Shed. Practitioners representing educational institutions, public bodies and start-ups gathered to celebrate the launch of the new phase of RISCS, the Research Institute for Sociotechnical Cyber Security.

Since its inception in 2012, RISCS has been striving to reframe cyber security as an inherently interdisciplinary and people-centred field, mobilising original research on crime, international politics, literacy, and cyber risk (among many other topics). Funded by the National Cyber Security Centre, the Institute will be hosted by the University of Bristol and led by Prof Genevieve Lively.

The RISCS 2023 conference was filled with thought-provoking presentations and activities, out of which two points caught my attention in particular. I was intrigued by a call from one of the delegates, who exclaimed 'we need a new word for cyber security!'. I was also struck by the presentation featuring Tobias' Weickert PhD research on the conceptual linkages between habit theory and cyber security (spoiler alert: the theory has not travelled as intended so far!).

Let's discuss these points further…

Conceptual globetrotting

In his recent paper co-authored with Prof Adam Joinson and Dr Barney Craggs, Tobias Weickert, a late-stage PhD student at Bristol and Bath Centre for Doctoral Training in Cyber Security, compared cyber security and psychology literature to understand to what extent the theory of habit has been adopted for security. Researchers found that important aspects of habit theory aren't considered in security literature, e.g., the role of cues in triggering behaviours or the mechanisms of habit formation.

Understanding the trajectories of concepts is not just a matter of satisfying our curiosity. Tobias' paper showed that applied computer science research is not fully engaging with psychology, despite using its key terminology. This is an important wake-up call for our community. Looking further back, researchers like Maarten Derksen traced the origin of human factors (whether in engineering or cyber security) and its links to ergonomics - a discipline historically tasked with the aim of making workers more efficient. This leaves little space for recognising and addressing social inequalities, discrimination, or even re-imagining cyber security technologies outside the dominant paradigm of labour productivity.

I also think that we, social scientists, have an obligation to move beyond critique. The goal is *not* to gatekeep and prevent 'conceptual globetrotting', as this can only lead to further siloes. What we should highlight, however, is the pressing need to support the fundamental work underlying interdisciplinary research programmes. Such work, as Tobias' paper shows, demands a sustained commitment to **the unearthing the history of ideas.** This is precisely where RISCS could make advances and I sincerely hope this is the path it will pursue.

Cyber security – the modern Tower of Babel?

The call for 'coming up with a new word for cyber' was met with a series of enthusiastic hums and nods from across the room. However, as someone familiar with the key (cyber) security debates spanning the past two decades, I wanted to acknowledge a serious progress we have made already!

Gone are the days where cyber security is understood solely as 'fixing networks' problems' (cf. Dunn Cavelty and Wenger, 2019). Our remit now also includes users, communities, and politics behind the protection of computer networks. Who is worthy of security? At what cost? For example, scholars like Prof Lizzie Coles Kemp and Dr Rikke Bjerg Jensen (2019) pointed out the difficult dilemmas where cyber security hampers social progress by restricting access to basic services for the most marginalised. My own research questioned who is involved in cyber security decisions and how to make security politics more democratic.

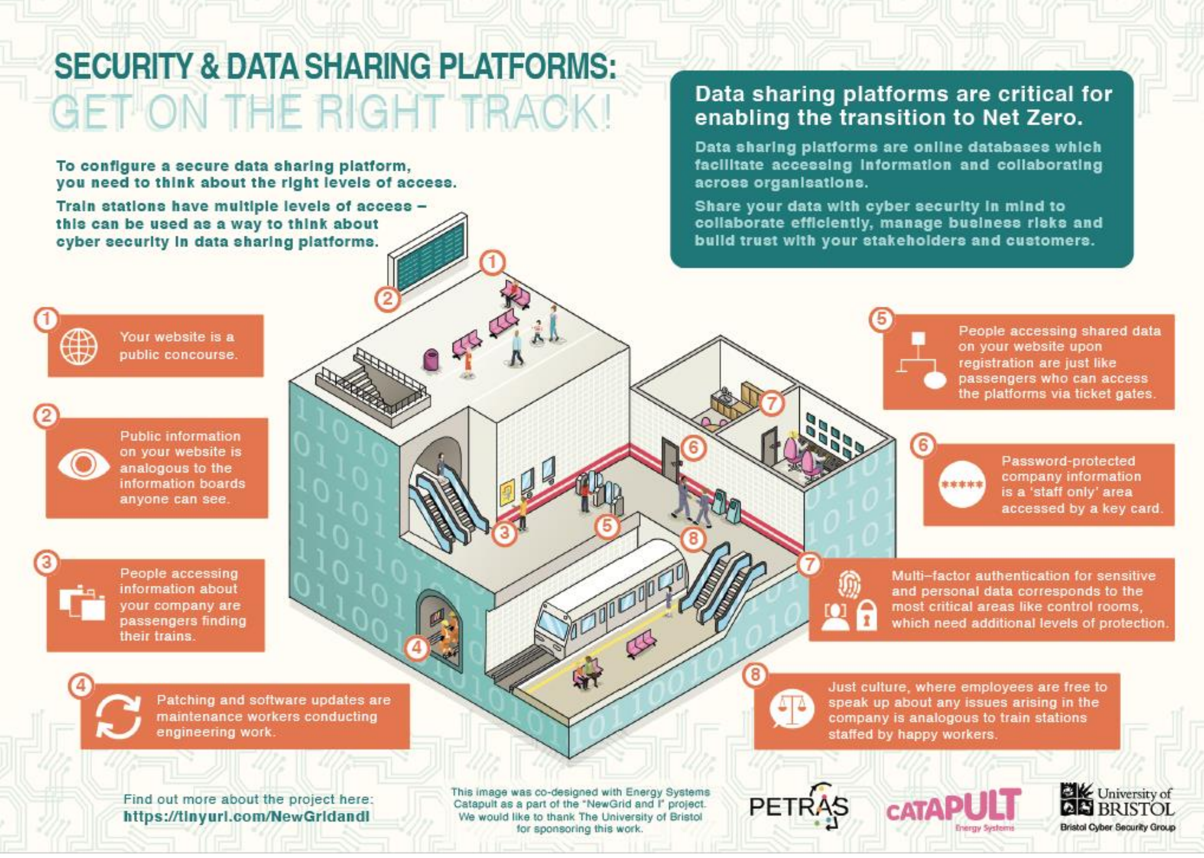
In academia, we have participated in myriad debates considered with defining security: information security, data security, computer security (see an influential 2013 paper by Prof Rossouw von Solms and Prof Johan van Niekerk). I might be a cynic, but personally I'm not sure what a repetition of these debates could achieve other than further demarcation of various key researchers and groups involved in security. This is symptomatic of boundary work (Gieryn, 1983), a process involving an interplay between newcomers expanding the field and incumbent researchers holding the boundaries of the concept (and perhaps, occasionally, loosening them as well!).

So, perhaps, we don't necessarily need to come up with *a new word* for cyber security but reflect on the language contained in our discussions. Which metaphors do we adopt? How do we frame cyber security advice? What colour schemes and images do we use? There are some emerging exciting examples in this area, including Julia Slupska's (2021) paper on security metaphors, Dan Lockton's (2019) game for creating new metaphors, or our "secure data platforms" infographics. As a lead of "Communicating Cyber Security" initiative at SPRITE+, I have been organising seminars and workshops exploring the above ideas, with the next one taking place on the 31st May (look out for registration).

While it's promising to see that cyber security professionals take interest in language and creativity, there is still a lot of work to do to. We need to move the field away from the overly masculine and militaristic representations. For example, the community would benefit from a **concerted effort to refresh and diversify its glossary and images** (perhaps taking inspiration from the wonderful initiative Better Images of AI). This is my second wish for RISCS.

A way forward

Over the past decade, cyber security expertise has come a long way. Seeing 'sociotechnical' in project titles, professionals' bios or research papers is no longer surprising to stakeholders and this is undoubtedly RISCS' major achievement. I hope that in the next phase of the Institute's operations, we will have a chance to see more exciting provocations from humanities, arts, and critical social sciences!



SECURITY & DATA SHARING PLATFORMS: GET ON THE RIGHT TRACK!

To configure a secure data sharing platform, you need to think about the right levels of access.

Train stations have multiple levels of access – this can be used as a way to think about cyber security in data sharing platforms.

Data sharing platforms are critical for enabling the transition to Net Zero.

Data sharing platforms are online databases which facilitate accessing information and collaborating across organisations.

Share your data with cyber security in mind to collaborate efficiently, manage business risks and build trust with your stakeholders and customers.

1. Your website is a public concourse.
2. Public information on your website is analogous to the information boards anyone can see.
3. People accessing information about your company are passengers finding their trains.
4. Patching and software updates are maintenance workers conducting engineering work.
5. People accessing shared data on your website upon registration are just like passengers who can access the platforms via ticket gates.
6. Password-protected company information is a 'staff only' area accessed by a key card.
7. Multi–factor authentication for sensitive and personal data corresponds to the most critical areas like control rooms, which need additional levels of protection.
8. Just culture, where employees are free to speak up about any issues arising in the company is analogous to train stations staffed by happy workers.

Find out more about the project here:
https://tinyurl.com/NewGridandI

This image was co-designed with Energy Systems Catapult as a part of the "NewGrid and I" project. We would like to thank The University of Bristol for sponsoring this work.

Security and Data Sharing Platforms: Get on the Right Track! 2022. Illustration by Oliver Dean. For project 'NEW GRID AND I' led by Dr Ola Michalec, developed in collaboration with Energy Systems Catapult and Dr Ruzanna Chitchyan. Funded by the University of Bristol Impact Accelerator Account and PETRAS.