futurum

RESEARCH • CAREER INSIGHTS • ACTIVITIES

ONLINE BATTLES: COMBATTING FALSE INFORMATION AND REDUCING ONLINE RISKS

INSTITUTE OF CYBER SECURITY FOR SOCIETY (iCSS), UNIVERSITY OF KENT

ONLINE BATTLES: COMBATTING FALSE INFORMATION AND REDUCING ONLINE RISKS

These days, we are all online, but it is difficult to have a full understanding of the risks this entails. **Professor Shujun Li** and his colleagues, **Sarah Turner, Dr Rahime Belen-Saglam** and **Dr Virginia N.L. Franqueira** at the **Institute of Cyber Security for Society (iCSS),** University of Kent in the UK, are working on enhancing people's awareness of the risks of online false information and sharing personal data online.

PROFESSOR SHUJUN LI

Professor of Cyber Security of School of Computing and Director of the Institute of Cyber Security for Society (iCSS), University of Kent, UK

PROFILE

Related research work
Investigating online false information, cyber fraud, online privacy risks, data protection, cyber security and online safety education

Funders
Engineering and Physical Sciences Research Council (EPSRC)/UK Research and Innovation (UKRI), National Cyber Security Centre (NCSC)/Government Communications Headquarters (GCHQ), Defence Science and Technology Laboratory (Dstl)/Ministry of Defence (MoD), Global Forum on Cyber Expertise (GFCE), Turkish government (Ministry of National Education), and others

TALK LIKE A...
CYBER SECURITY EXPERT

Artificial Intelligence (AI) — computer algorithms and systems able to perform tasks that would typically require human intelligence

Crowdsourcing — getting input or information by enlisting a large number of people to contribute

Deepfake — manipulation of existing digital media (image, video and/or audio) – e.g., by swapping faces and changing voices – or creation of new media, typically using machine learning-based techniques such as deep learning

Deep learning — technology able to automatically learn from a large set of digital media and apply what has been learnt to manipulate or create sophisticated media

Machine learning — AI algorithms and systems able to automatically learn from data to perform a specific task

Metadata — a (large) set of data giving information about other data

Misinformation — false or inaccurate information created and spread without an intention to harm others

Disinformation — false or inaccurate information created and spread maliciously, often used for deceptive purposes

Personal data — information relating to an identifiable individual

Online false information

Online false information, including misinformation and disinformation, has become rife, shaping social groups and political opinions, and leading to dangerous beliefs and conspiracy theories. The age of the internet allows false information, such as 'fake news', to spread like wildfire. It is now incredibly easy for claimed factual information, even if entirely false, to reach millions of people very quickly. Educating people about the harms caused by online false information, and how to detect and avoid it, is becoming a growing priority for many.

"Young people may be more likely to fall for false information, especially misinformation or conspiracy theories, because of their lack of life experience, sufficient technical knowledge and tendency to believe in others more easily," says Professor Shujun Li. Shujun is Professor of Cyber Security and Director of the Institute of Cyber Security for Society (iCSS) at the University of Kent, where many researchers are actively researching on understanding, detection and prevention of online false information and digital data deception. "Young people can be super-spreaders of online false information," he says. "This is because of their active use of social media, and they may read and share posts rapidly, without proper fact-checking."

Fact-checking

As more of our daily activity takes place online, the boundaries between the online and physical worlds are becoming increasingly blurred. Fact-checking has become an important tool to help distinguish what is true and what is false. Fact-checkers can be humans or machines. "Crowdsourcing methods have been developed so that fact-checking professionals or willing citizens can work together to identify and debunk false information online more efficiently," says Shujun. "This includes human-in-the-loop AI systems that allow humans and machines to work in tandem to fight against false information." Humans and AI algorithms are proficient at different things,

so combining their powers is often a more effective way of identifying false information.

It is not only words that can be misleading, but also non-textual data such as digital images and videos. The rise of powerful image- and video-editing software means that it is easier than ever to construct digital images and videos that look real but are fake or misleading. While some are easy to spot, the advent of more advanced fake-making technologies, such as those behind 'deepfakes', is making it harder to tell fact from fiction. However, advances in technology are combatting this. "Many methods using AI have been developed to automatically detect fake images and videos, and can help human fact-checkers do their job more easily," says Shujun.

Trustworthy experts

To differentiate fact from fiction, Shujun advocates the 'STOP, THINK, CHECK' technique from the Irish *Be Media Start* campaign (**www.bemediasmart.ie**). "Stop to take time to think, and then think about if and what you need to check," he says. 'Stop' involves taking time to read beyond a headline and not believing in what you read immediately. 'Think' involves considering what the purpose of the information is – e.g., to inform or persuade – and how our own biases might affect our likelihood of believing something. 'Check' involves looking at the source and investigating whether this information appears on a range of reliable platforms elsewhere online.

This final stage, identifying whether information comes from a reliable source, is not always straightforward. "Check if the information comes from experts," says Shujun. "This can include scientific papers at reputable scientific journals and conferences, statements from reputable research organisations and professional bodies for expertise in the subject they're talking about." Endorsements from other trustworthy sources can help build confidence. "Find out if the information has been endorsed by, for example, a public body, a reputable international body such as the World Health Organization (WHO), a charity with a good reputation on the subject matter, or a media platform with a long-term reputation for accurate reporting," he says.

Personal data sharing

"Sharing some personal information online with some online users is necessary for being part of cyber space," says Shujun. The cyber world offers lots of positives, but many of us are quite lax with our personal data, which is a valuable commodity that can be dangerous if it falls into the wrong hands. "Digital services suck up data about us in different ways," says Sarah Turner, Research Student at the iCSS. "Often, sharing data is an important part of getting full use of a digital platform, helping us connect with friends and contacts, for instance. Additionally, many apps and other digital platforms require access to your data to work correctly."

Threat modelling

Data can seem abstract, and it is all too easy to click the 'Accept' button without thinking too much about the consequences. Sarah suggests thinking about how you share your data in a more structured way. "Threat modelling is often used in software creation but can also be applied to your own personal data," she says. "It involves thinking about a threat and then considering the steps needed to overcome this threat and whether these steps are proportional to the risks." The Electronic Frontier Foundation's *Personal Threat Modelling* questions are as follows:

What do I want to protect?
Who do I want to protect it from?
How bad are the consequences if I fail?
How likely is it that I will need to protect it?
How much trouble am I willing to go through to try to prevent potential consequences?

Sarah also suggests adding in the following, final question: *What do I need to know or do to make that happen?*

Sarah points out that 'threats' are not just the anonymous malicious hackers of our mind's eye. "There are often other people who, intentionally or not, might cause you problems if they access certain bits of your personal information," says Sarah. "What if a possible employer finds questionable tweets you wrote five years ago? What if a mischievous sibling deleted your coursework because they knew your password?"

Games and data

While games can be a great way to relax and escape, they are not excluded from the online data-gathering world. "Most games want to hook you with the gameplay, which can be enriched by using your personal information," says Sarah. "For example, *Animal Crossing: New Horizons* uses your birthday to celebrate your big day and personalise the experience." Games can go further and encourage engagement with other online players, exposing your data more broadly. "Games also collect metadata," she says. "For instance, they can recognise what device you're playing on, and at what times, and details about your internet connection."

Names and birthdays may seem like harmless information to share widely, but Sarah points out it can be problematic. "Data can be stolen and sold to the highest bidder," she says. "They can do whatever they like with this – for example, a name and date of birth can be sufficient to carry out identity theft." More insidiously, advertising agencies use our data to suggest specific things for us to support or buy tailored to our interests. This may seem helpful rather than malicious, but it can contribute to the profiling of particular groups, such as by pigeonholing people into particular 'bubbles' where they only see information or products that reinforce or narrow their own worldview.

All that glitters

"Data is like glitter: once it's out, it's everywhere!" says Sarah. Once something is online, it often remains there for years and years, even if you think you have deleted it. "Try to get into the mindset of threat modelling before using a new service or buying a new device," says Sarah. "This will help you investigate how the service or device works and what it does with your data, which may influence your decision about using it."

ABOUT *CYBER SECURITY*

Cyber security focuses on making the world safer through preventing or mitigating online threats. This can involve technical careers in computing and software but, given the significant human aspect involved in cyber security, also involves social sciences and humanities.

The interdisciplinary nature of cyber security means different skills, knowledge and attributes are needed depending on what sort of cyber security career you might be interested in. From academic research to government policy to teaching young children how to be safe online, cyber security is a vast and vital field.

Pathway from school to *cyber security*

For technical degrees and careers, subjects like computer science and mathematics can be useful. For those more focused on social sciences or humanities, subjects like psychology, business studies, economics, criminology, politics and international relations, media and communications may be important.

Virginia and Shujun recommend extending what you learn at school through, for example:

- finding a relevant club
- doing an extended project, such as one leading to a Cyber EPQ, CIISec's Cyber Extended Project Qualification worth half an A-level and up to an extra 28 UCAS points (**cyberepq.org.uk**)
- participating in an experience week or an internship at a university (e.g., iCSS at the University of Kent), either within your curriculum, if it allows, or elsewhere.

Explore careers in *cyber security*

- The UK Cyber Security Council provides a careers route map for the profession, providing details on the 16 specialisms within cyber security and pathways to get there: **www.ukcybersecuritycouncil.org.uk/careers-learning/careers-route-map**
- To get a fuller understanding of what cyber security entails, Virginia and Shujun recommend getting involved in relevant activities, such as Safer Internet Day (**www.saferinternetday.org**), Cyber Security Challenge UK (**www.cybersecuritychallenge.org.uk**), and TryHackme (**tryhackme.com**).
- The National Cyber Security Centre (NCSC) runs CyberFirst, a programme of activities intended to encourage students to consider careers in the sector and apply for a related bursary: **www.ncsc.gov.uk/cyberfirst/overview**
- Read more about Shujun's career path: **futurumcareers.com/how-to-beat-the-cybercriminals-and-stay-safe-online**

Meet *the iCSS team*

Virginia N. L. Franqueira
Lecturer in Cyber Security, Deputy Director (Education) of the iCSS

I started my career working in industry, involved with software testing, maintenance and development projects. My specialisation in cyber security was triggered, quite by chance, when I decided to leave industry to pursue a PhD in The Netherlands.

I never assume I know everything I should know, which leads to the need for continuous learning. This is essential in the field of cyber security, since it develops at such a fast pace.

I was drawn to digital forensics and cybercrime investigations through my first lectureship post. I became passionate about these subjects, not only from a law enforcement perspective but also from the perspective of improving methods and processes that can ultimately make a positive difference for victims of interpersonal cybercrime (such as domestic abuse and exploitation of children).

Digital forensics is fascinating. It involves technical skills to understand how things work (such as devices, operating systems and applications), as well as where to collect data and how to interpret it to help answer important questions about past activities. It also involves investigative skills to approach the work in a systematic way, with attention to details and to documentation. Finally, digital forensics requires awareness of human behaviour and motivations since there is always a human directly or indirectly involved in a wrong-doing.

Machine learning has the potential of assisting digital forensic investigators in many ways. For example, in identifying previously unseen illegal images based on images already known to be illegal, or estimating the age of people appearing on an image/video of interest, or helping to speed up examination and analysis of digital evidence.

Virginia's top tips

1. **Be curious about technology.** Follow technology news, and take an interest in learning beyond what is taught at school and college.

Rahime Belen-Saglam

Research Associate, iCSS

I specialised in cyber security quite by chance! I was working in other research areas, including information retrieval and data quality. While working with a PhD student on his thesis, we needed guidance on cyber security, and this is how I met and started working with Professor Shujun Li.

I've always enjoyed reading and learning new things. As cyber security is a very dynamic field, those attributes help me to catch up well with the new research areas. I am also interested in analysing information and finding solutions to problems.

Currently, I am working on data privacy and security issues of blockchains, the technology behind cryptocurrencies such as Bitcoin. I am conducting a literature review study, where I read scientific articles published in a specific research area and generate knowledge from those studies in a systematic way. I've identified some research gaps in the literature regarding the algorithms proposed to protect personal data on blockchain systems.

I would like to conduct studies that aim to use technology for good. This includes projects that try to prevent the misuse of technologies. Improving the cyber security skills of younger people is another area I would like to keep studying.

Rahime's top tips

1. **Keep in mind that there are several ways to get into cyber security.** It is an interdisciplinary area – technical, legal, business, economic, psychological and societal perspectives are very important. Discover what excites you the most, and follow your own footsteps.

Sarah Turner

Research Student, iCSS

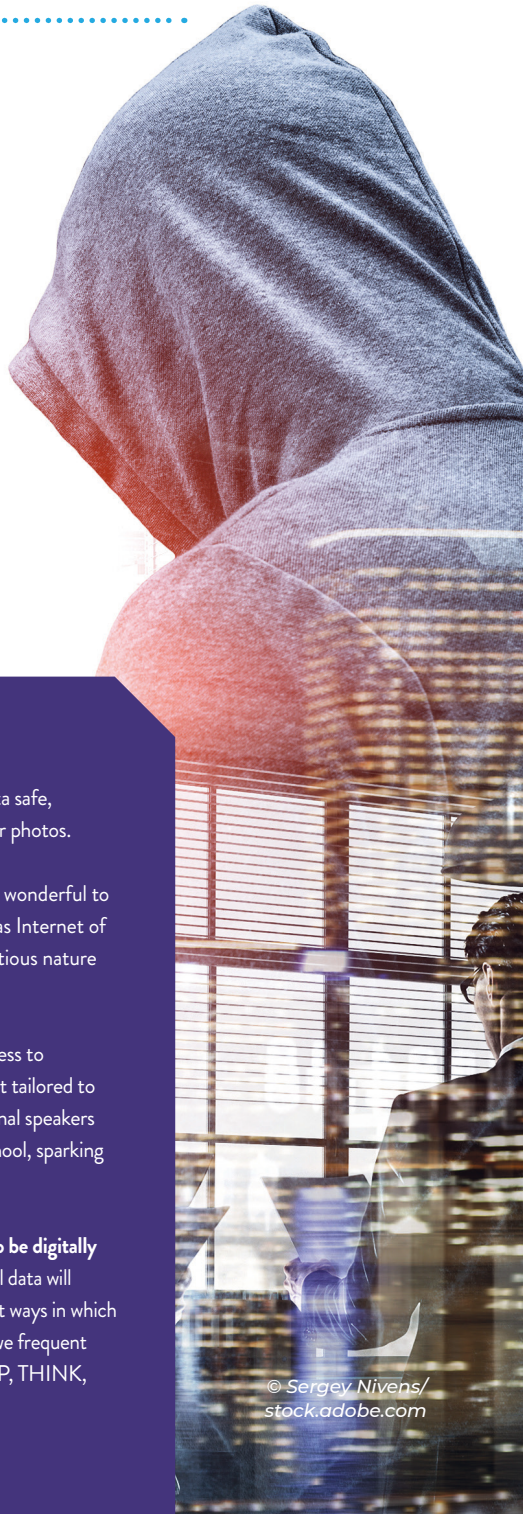
I came back to academia after spending 10 years working with regulation and technology in financial services. I started looking at how public policy needs to deal with technology, which led to the realisation that people need support to make sure the devices they use are as secure as possible.

People love the novelty of Internet of Things devices and will bring them into their homes with little to no understanding of how or why they work – or what that could mean for them if things go wrong.

Digital technologies and their place in society are in flux at the moment. I hope I can do something to make people less of an afterthought as these technologies become part of our daily lives!

Sarah's top tips

1. **Be sure of yourself, but always listen to others** – having multiple viewpoints almost always makes for a much better final result!



© Sergey Nivens/ stock.adobe.com

A teacher's *viewpoint*

Samantha Barnes

Head of Junior School ICT and Computer Science, St Edmund's Junior School, Canterbury, UK

"**Currently, there is no specific or dedicated curriculum on cyber security** across all key stages, and where there is a requirement for eSafety, historically the terminology used leads to a narrow view and misunderstandings of how vast cyber security is.

Younger students are taught that what we do offline should reflect what we do online in terms of our human behaviour, ensuring adults in our lives are aware of the activities of our cyber lives. Children are taught to fact check with various sources, with both adults and websites. Some already understand how to keep their data safe, including metadata that can be found within our photos.

Collaborating with the iCSS team, it has been wonderful to adjust our lens to more pressing matters such as Internet of Things awareness in the home and the surreptitious nature of misinformation.

We ran a Safer Internet Day where we had access to academic staff from the iCSS team and content tailored to our school. The children very much enjoy external speakers who come from the world of work beyond a school, sparking their curiosity to dig deeper.

Next, we'll be exploring further what it means to be digitally literate in a world where protecting your personal data will become ever more important. We will also look at ways in which we validate what we learn from the cyber space we frequent and inhabit, such as fact-checkers and the 'STOP, THINK, CHECK' technique."

CYBER SECURITY
WITH THE iCSS

Talking *points*

KNOWLEDGE & COMPREHENSION

1. What is cyber security?
2. Why is online false information a growing and important issue?
3. What are some of the factors that would make a piece of information or a source of information trustworthy or untrustworthy?
4. What can be some negative outcomes of over-sharing personal data online?
5. What is the boundary between sharing and over-sharing personal information?

APPLICATION

6. On social media or via a search engine, find a recently published piece of information (e.g., an article, a social media post or a YouTube video). Try out the 'STOP, THINK, CHECK' technique in the article. What did you learn?
7. Undertake a 'threat modelling' exercise on your own personal data following the questions in the article. In what way does it make you rethink your data sharing choices?

ANALYSIS

8. Why does cyber security need to be interdisciplinary? What disciplines are relevant and why? Name a number of disciplines and find one concrete example for each discipline.
9. What are the different roles of humans and AI algorithms, and how can they work together to identify online false information?

EVALUATION

10. Do you think online false information is likely to be a bigger or smaller issue ten years from now? Why?
11. Can you think of any examples in the news about data breaches? If not, see if you can find one using a trustworthy source online. What has been the impact of these data breaches? How might they have been avoided?

Activities

ONLINE FALSE INFORMATION

1. ACTIVITY:

With your classmates, play a game of Broken Telephone: one person whispers a certain sentence in the ear of their neighbour, who whispers what they hear in the ear of their neighbour, and so on. The last person says aloud what they heard.

Question:

How much did the statement change? This indicates how information, even if true at first, can be distorted as it is passed on by multiple people, each of whom may not fully understand it or know how to properly convey it. Though nobody (hopefully!) deliberately changed the message, it nonetheless changed its meaning. This indicates why misinformation happens so ubiquitously on the internet.

2. ACTIVITY:

Many important topics are frequently vulnerable to mis- and disinformation. Examples include climate change and COVID-19. In small groups, choose one of these topics or one of your own, and think of when you have heard about differing opinions on the subject. Discuss the topic in your group, and how a piece of misinformation can be changed to disinformation when the intent of the information creator becomes malicious.

Question:

Reading over the article, what would you need to do to determine which opinions best tally with scientific facts? Use the internet and other sources to carry out this process.

3. ACTIVITY:

Visit this website: www.whichfaceisreal.com

Play the game by choosing which of the pair of faces you think is a real photograph. The other is a fake image.

Question:

How good were you at telling which faces were real? What clues were you looking for? Read this page to see which clues the developers have identified: www.whichfaceisreal.com/learn.html

Did they match up with your own thoughts?

How do you think humans paired with AI could get as close to perfect accuracy as possible on determining which face is real or fake?

PERSONAL DATA SHARING

ACTIVITY:

Think about an app, a social media platform, or a game that you use regularly. If you do not use any of these things, pick one you have heard of. Look up what personal data the application requires to use it correctly. This may include:

- Name, date of birth, nationality, gender, etc.
- Location
- Access to your phone's camera and/or files

Questions:

For each of these pieces of data, answer the following:

- Can I see why the application needs this data to function properly?
- Does it improve my life to share this data so I can use this application?
- What are the risks of this particular application having this data?
- What are the risks if this data was stolen or sold?

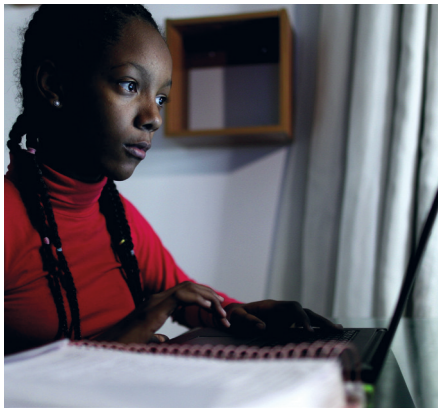


Photo *montage*

Top row: ***left and centre:*** *When reading information online, use the 'STOP, THINK, CHECK' technique: stop to take time to think, and then think about if and what you need to check. © Marco/stock.adobe.com*

Top row right: *Even games designed for younger children can be used to collect valuable personal information.*

Bottom: *As active users of social media, young people can be super-spreaders of online false information. © olly/stock.adobe.com*

+44 117 909 9150
info@futurumcareers.com
www.futurumcareers.com

futurum