UCD DUBLIN

RISING
TO THE FUTURE
UCD Strategy 2020-2024

Cyber Resilience Education for Primary & Post-Primary Schools (CREPS): A UCD School of Education Collaborative and Innovative Cyber Security Outreach Programme

rachel.rarrell@ucd.ie

@econrachel

Trends Shaping Education (OECD, 2022)

Our changing nature

There is no Planet B
Is the pace at which we are using our planet's resources sustainable?

The natural world
How is our relationship with the natural world evolving?

Food for thought
How is food production and consumption affecting our planet and our well-being?

Our human body
What opportunities are emerging from advancements in medicine and human enhancement?

No one lives in cyberspace
In what ways are our daily communication and social interactions changing?

Background

- Health Service Executive (HSE) of Ireland ransomware cyberattack.

- The COVID-19 rendered us vulnerable to cybercrime.

- Increasing reliance on online technology.

- Malicious actors are exploiting these vulnerabilities (Council of the European Union, 2020).

- Catalyst for an impending "cyber pandemic" (OECD, 2021).

- Potential threat of Russian cyber warfare.
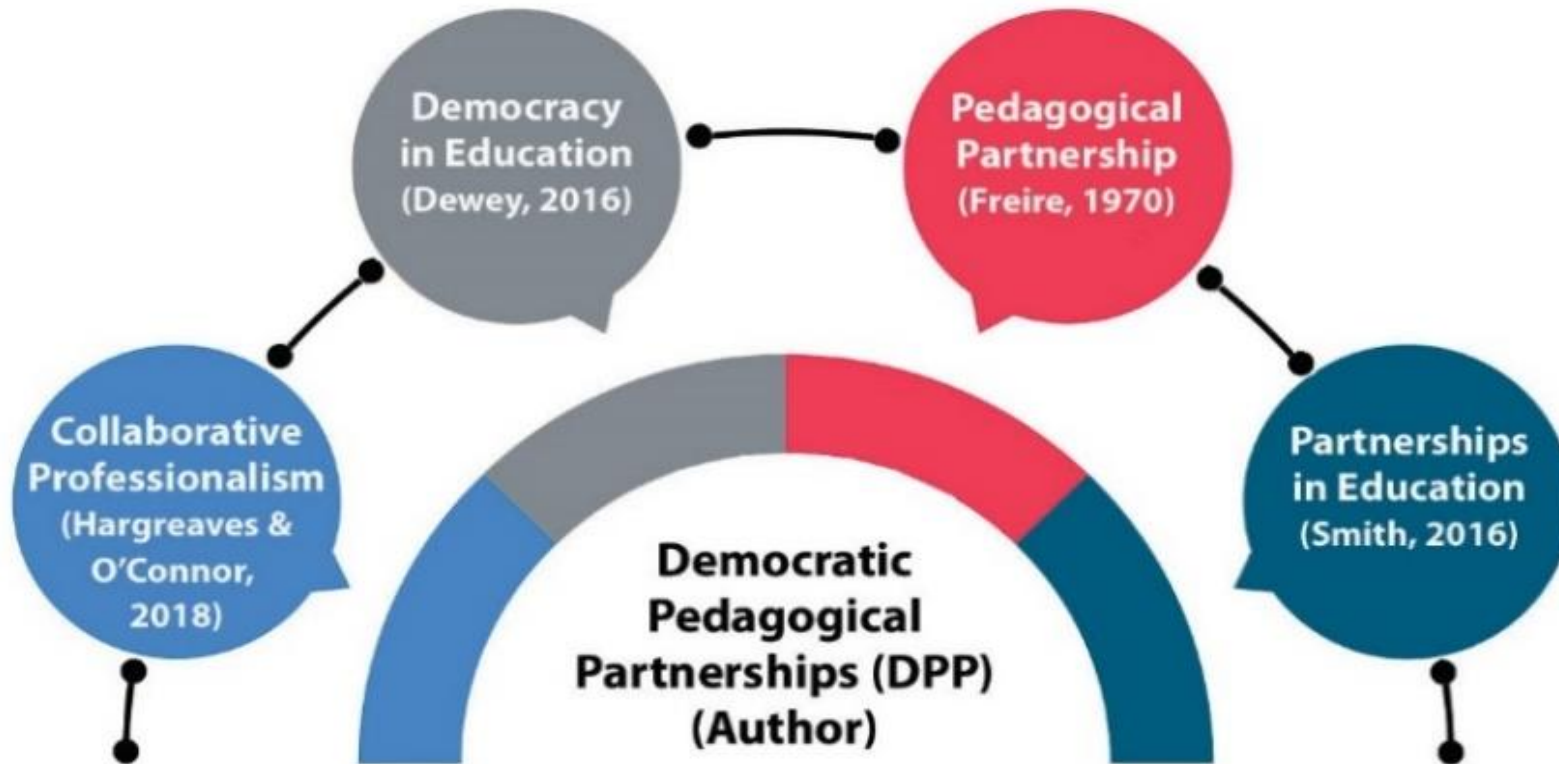
The National Cyber Security Strategy

Seeks to:

"support the development of a Junior Cycle short course in cyber security, which will provide for the inclusion of cyber security education in second level"

(GOI, 2019, Measure 12:4, p. 39)

This is being achieved through a "democratic pedagogical partnership" approach

(Farrell, 2021)

Democratic Pedagogical Partnerships

A Democratic Pedagogical Partnership in Teacher Education is "a formal but flexible structure/agreement between all stakeholders, including teacher educators, who engage in *collaborative professionalism* to improve learning for all students in a variety of contexts through effective pedagogy and practice" (Farrell, 2021).
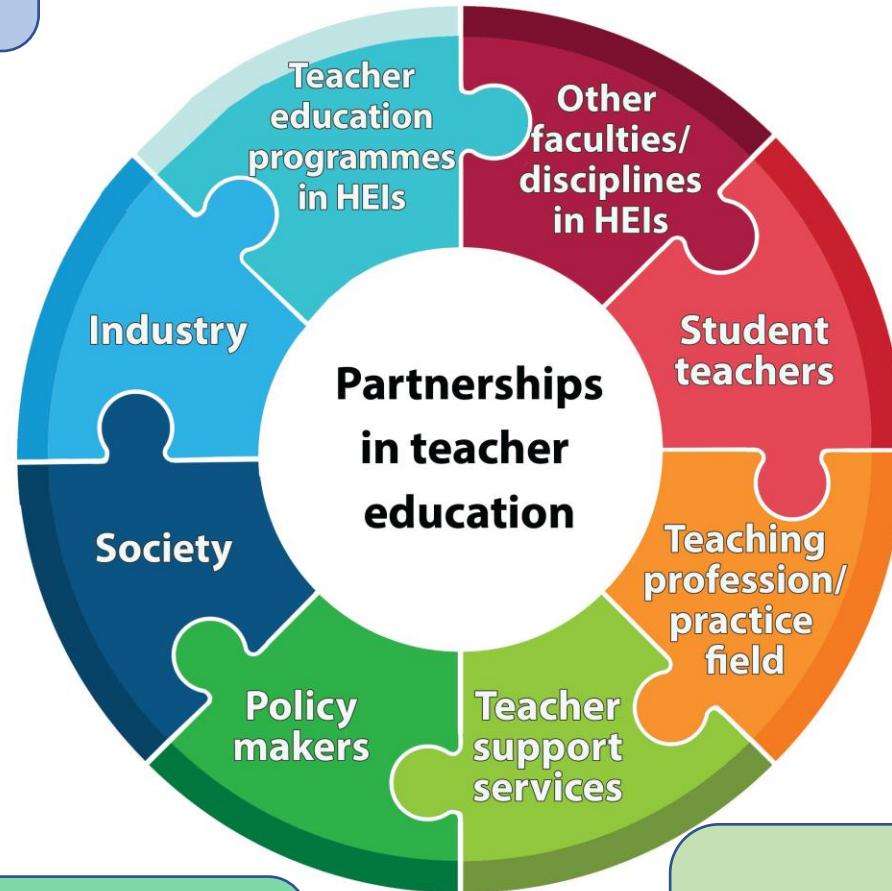
Smith – Partnerships
Zeichner – 3rd space
Engeström – Expansive Learning
Research & creation of new knowledge
4th space

NCAD Change Lab Project
Art & Music – SDGs
Ubuntu Network Funding

Concurrent Programmes across UCD
Maths & Statistics
Computer Science
Languages
Economics (YEOTY)
Interdisciplinary Research

Digital Technology
Microsoft Education Ireland
Digital Portfolios
SchooVR

Reverse Mentoring & Leadership
Digital Portfolios
Immersive Technology

Outreach Programmes
Sustainable Societies
EDI STEM
Innovation & Creativity

Capacity Building
Co-operating Teachers
Teacher Mentors
School Leaders

Curriculum Development
National Council for Curriculum & Assessment
e.g. Cyber Security Short Course

Network of Supports
Professional Development Services for Teachers
Junior Cycle for Teachers
National Council for Special Education

Partnerships in teacher education

- Teacher education programmes in HEIs
- Other faculties/disciplines in HEIs
- Student teachers
- Teaching profession/practice field
- Teacher support services
- Policy makers
- Society
- Industry

Pedagogical Democratic Partnerships (Farrell, 2021) in co-designing a short course on cyber security

Teacher educators from UCD School of Education collaborated with a cross-sectoral multi-disciplinary working group comprising:

- Department of the Environment Climate and Communications
- National Centre for Cyber Security
- National Council for Curriculum and Assessment
- UCD School of Computer Science
- Computer Education Society of Ireland
- Cyber Ireland
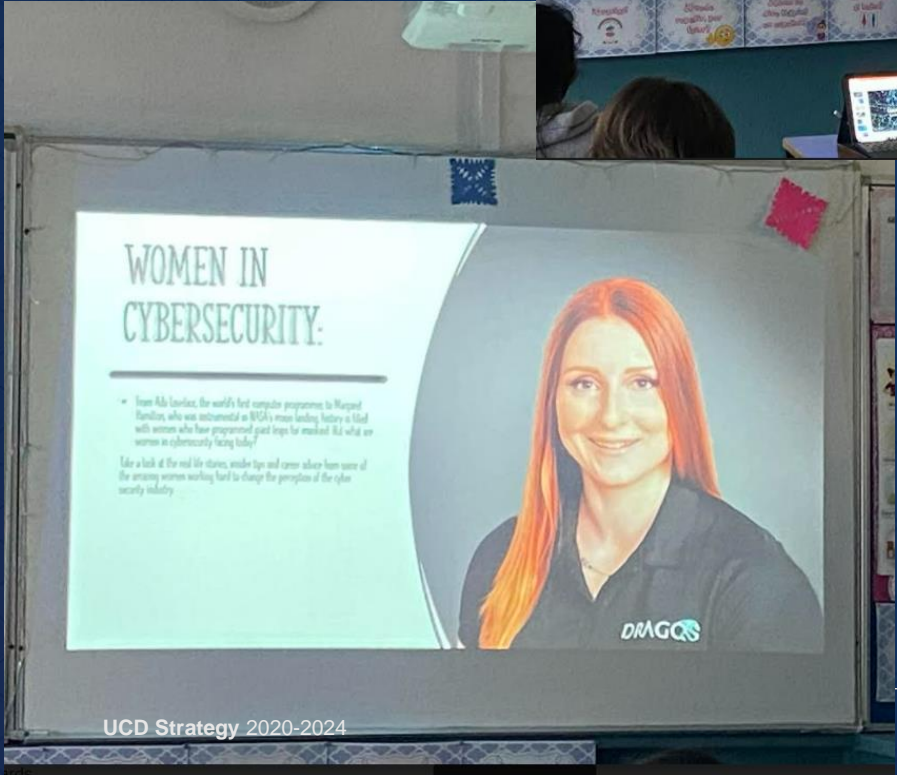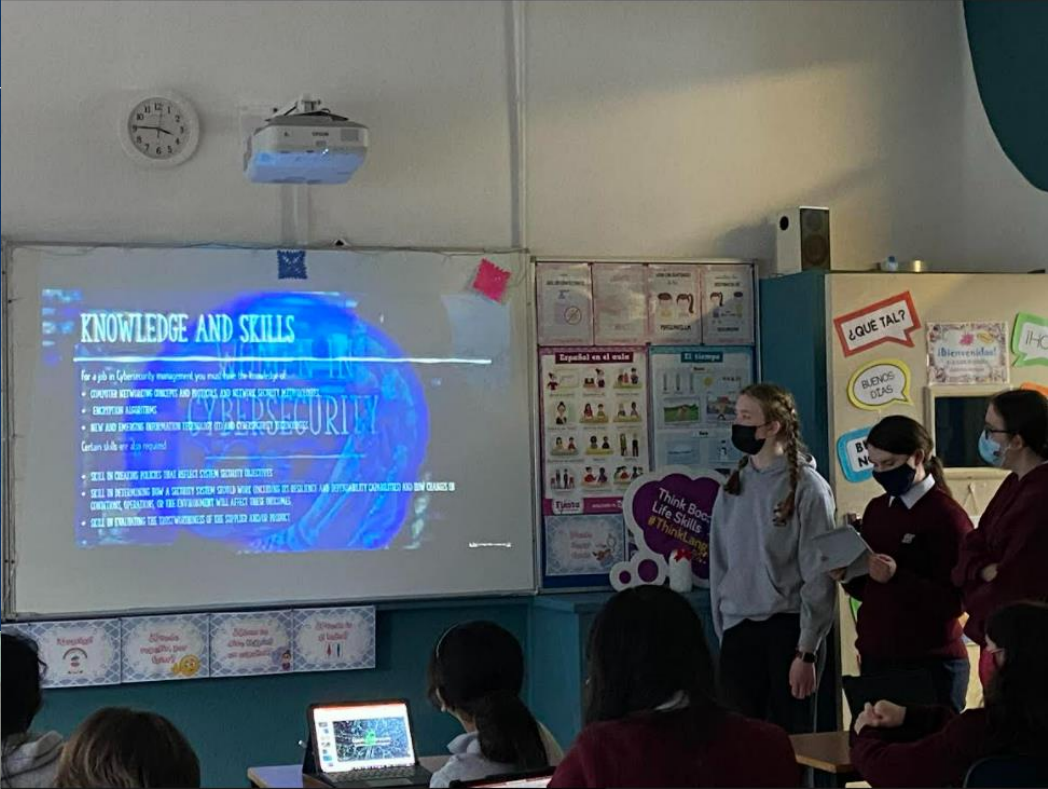- Practicing teachers in pilot schools

www.cybered.ie will host up-to-date student-centered resources and teacher professional development supports emanating from the project and will be freely available to the wider education community

Draft Junior Cycle Cyber Security Short Course

Unifying Elements	Strand 1 Exploring Cyberspace	Strand 2 Cybersecurity Solutions	Strand 3 Cybersecurity in a Global Village
Philosophy of Cyber Security Recognise the interdisciplinary and complex nature of cyberspace and the personal, local, national and global role it has in our lives. Critically engage, evaluate and reflect on the implications cyberspace has for privacy, security and freedom. Collaboratively create, inquire and reflect upon philosophical questions that arise when exploring cyberspace and cyber security.	**Making Sense of Cyberspace** Consider the variety of uses of digital technologies for individuals, communities, businesses and governments that make up cyberspace. Discuss the core functions of cyber security and appreciate its importance in society. Understand the concept of cyber hygiene and the key steps for good cyber hygiene Explore the role of codes in cyber security (data compression, cryptography, error detection and correction, data transmission and data storage)	**Who goes my way?** Explore the historical role of passwords and encryption to secure valuable information. Develop an understanding of the properties of codes Identify the factors needed to make a successful encryption Appreciate why passwords should be managed well and kept safe. Understand the features of a strong password or passphrase and the common errors made when creating or maintaining them. Understand how to improve personal online account security by enabling screen locks, changing default passwords, using passphrases and using multi-function authentication (mfa) and password managers	**Communication and Crisis Management** Understand what the NCSC's role is during a major cyber security incident. Describe some of the high-profile cyber security crises in modern times. Evaluate the risks to cyber security during a crisis Explain how to plan and respond to a cyber security attack as an individual. Explain how an organisation can plan and respond to a cyber security attack - i.e Local level, corporate level, policies, response plans, communication plans, simulation exercises List examples of how the Irish Government communicates cyber security threats during a crisis
Careers in Cyber Security Investigate career opportunities in cyber security. Identify qualities, skills, and qualifications that are suitable for a career in cyber security. Evaluate if a career in cyber security is of interest to you. Examine the portrayal of people in cyber security	**Data is the new oil** Consider what data is, and what makes data politically, economically and personally valuable. Investigate the ways data is legally collected. Reflect on the concept of privacy and the value they place on their own privacy. Access and amend privacy settings appropriately on a variety of relevant digital media platforms and software apps.	**Building Security** Describe and evaluate different ways to back-up data. Outline the role of the Firewall in cybersecurity and know how to implement and maintain a firewall. Explain how to improve your home router security against malicious cyber activity by taking some simple steps Evaluate the benefits and risks of using public wifi systems and consider cybersecurity methods that could be used to protect their data, such as a VPN	**Regulation and Legislation** Investigate the role of regulation in cybersecurity. Examine the distinctions between voluntary versus mandatory regulation, and ethical versus government regulation. Describe the positive and negative implications of regulation around cybersecurity. Understand the principles of cyber security legislation investigate and evaluate national, european and international cyber security legislation
The Psychology of Cyber Security Internet psychology Cyberpsychology How has society changed after an event? Why do people engage in threatening behaviour in cyberspace?	**Cyber Events** Describe the types of cyber events, including attacks, identifying who the victim is, and who benefits. Examine examples of political, economic, social and personal cyber-attacks. Investigate how cyber security breaches occur for individuals, institutions and businesses.	**Spotting Cyber Attacks** Investigate the impact of different types of malware used to attack individuals, businesses, organisations and governments. Discern the difference between fake profiles and messages and authentic online communications. Know how to authenticate data before sharing and how to block and report unwanted communication. Explore current methods used by cybercriminals to access sensitive data such as PINS and passwords	**Reporting breaches of Cyber Security** Recognise when something is a threat and should be reported Identify who or what organisation you should contact and how to contact them. How to report online crime or threats -illegal content -financial transaction -fraud -a leak of personal information -extortion

Sample Units of Learning

- Case studies of **cyber events/cyber crimes**
- **Social engineering -** modern day con artists
- **Data is the new oil** - could your life online help design a new product? bring down a government?
- Black Hats and White Hats - **careers** in cyber security
- **Women** in cyber security
- **Securing your online world** - passcodes, firewalls, backing up
- What is the **economic cost** of cyber crime?
- **Cyber psychology**
- Cyber security in the **film study**

Design-based learning and research

This design-based project (Hall, 2020) seeks to expand the successful pilot of the junior cycle short course to provide:

- **blended modules** for student teachers and established teachers engaging in continuing professional development in cyber resilience education for all

- **age and stage appropriate** cyber resilience education to include 6th class students in primary school and transition year students in post-primary school

- insights into how cyber resilience education may be embedded **across a range of subjects and programmes** in post-primary education.

Cyber Resilience Education for All

Innovative pedagogy

- Philosophy for Children (P4C)
- Philosophical Inquiry
- Student generated book The Adventures in Cyberland"
- First Lego League
- Immersive Technology (SchooVR)
- LIFT Leadership – round table theme on Cyber security

Target audience

- Teachers
- Student Teachers
- Pupils in primary & secondary schools
- Parents
- Government Departments
- Industry

UCD Centre for Cyber Resilience Education in Primary and Post-Primary Schools (CREPS)

- CREPS will have a sustainable and self-sustaining infrastructure to support cyber resilience education for all.

- Its purpose is to project manage and evaluate the development and implementation of cyber resilience education across the continuum of primary, post-primary and third level teacher education programmes in Ireland that may also be adapted for the international context.

References

Council of the European Union. (2020). Press release: Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic [Accessed 30/09/21] https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

Engeström, Y. & Sannino, A. (2021). From mediated actions to heterogenous coalitions: four generations of activity-theoretical studies of work and learning. Mind, Culture, and Activity. 28:1, 4-23, DOI: 10.1080/10749039.2020.1806328

Farrell, R. 2021. The School-University Nexus and Degrees of Partnership in Initial Teacher Education. Irish Educational Studies. https://doi.org/10.1080/03323315.2021.1899031

Government of Ireland. (2019). National Cyber Security Strategy. GOI: Dublin.

Hall, T. (2020). Bridging Practice and Theory: The Emerging Potential of Design-based Research (DBR) for Digital Innovation in Education. Education Research and Perspectives, 47, 157-173.

OECD. (2021). Global Forum on Building Digital Security for Prosperity. OECD. [Accessed 30/09/21] https://oecd-events.org/digital-security-for-prosperity.

OECD. (2022). Threats Shaping Education. [Accessed 28/02/21] https://www.oecd-ilibrary.org/sites/6ae8771a-en/index.html?itemId=/content/publication/6ae8771a-en

Thank You

UCD DUBLIN

RISING TO THE FUTURE
UCD Strategy 2020-2024