Full reference for citation: Verrall, N.G. (2022). *Information Disorder and Future Threats*. DSTL/CP143425 (Porton, UK: DSTL).

Presented at the NATO STO IST-195 Symposium on Societal Challenges for Operations in the Information Environment, Stockholm, Sweden, 4 October 2022.

[dstl] The Science Inside

Information Disorder and Future Threats

Prof Neil G. Verrall
Chief Behavioural Science
DSTL
ngverrall@dstl.gov.uk

Ministry of Defence

13 September 2022

The Global Big Picture

[dstl] The Science Inside

1 Increasing population

Currently at 7.8bn. Factors including lower fertility rates and aging populations lead to a plateau at 11bn by 2100. The largest growth rates in the 21st century are in Asia and Africa.
More people to be connected.

2 Migration to urban environment

More humans are moving to urban conurbations; with 68% of global population living in the urban by 2050. Also by 2050 there will be ~50 megacities, mostly in Asia and Africa. The individual population of the top ten megacities will range between 35-50 million inhabitants.
More people connected in large population centres.

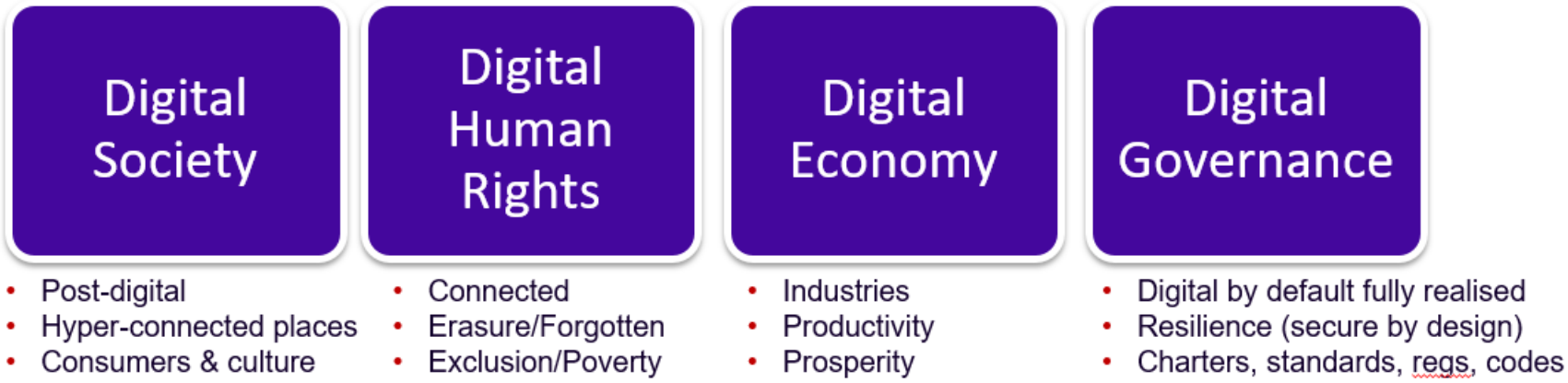
3 Digitization (of systems) Digitalization (of people)

Traditional records and systems become fully digitized and increasingly automated. 'Digital by default' is fully realised. Digital human rights are enshrined in law, and developed societies seek to eradicate digital poverty and digital exclusion.
More people digitized, but digital literacy rates vary and widen.

4 Connectivity

Estimated number of devices worldwide by 2030 is 50-125bn. Generation Alpha (born 2010-24) is the first generation in developed world nations to only know digital and connectivity.
A post-digital society will be defined by what is <u>not</u> connected and automated, as opposed to what is.

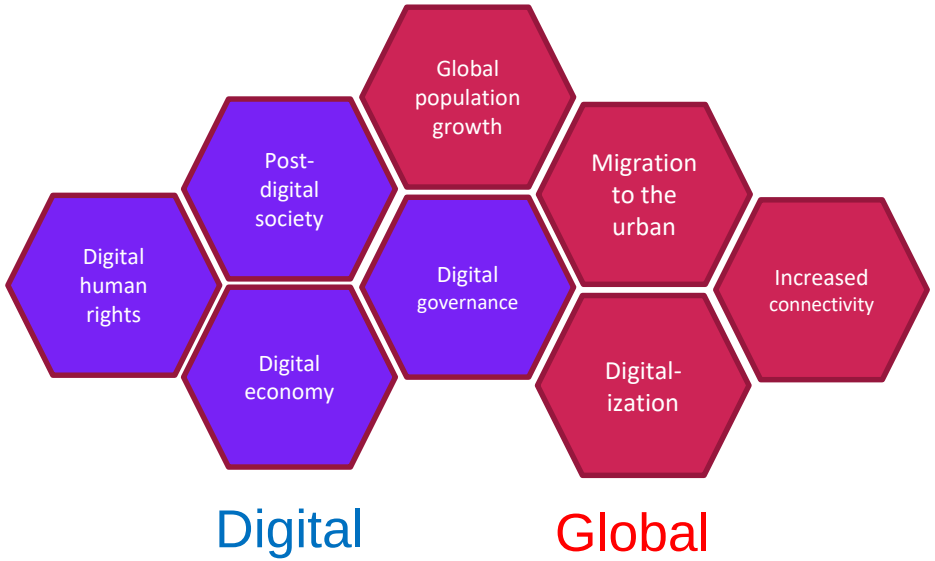
Society and digital



A realised information civilization

[dstl] The Science Inside

“Information Civilization”



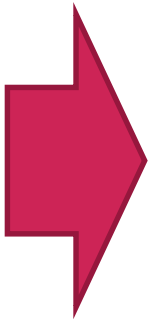
Future Threat

Information Confrontation and Information Disorder

[dstl] The Science Inside

Information Confrontation

- Target ICT infrastructure
- Target consciousness and feelings (perceptions, attitudes, beliefs, behaviour)
- Protect one's own ICT infrastructure
- It is a weapon, a resource, means of delivery and a goal



Information Disorder

- Disinformation (deliberate)
- Misinformation (inadvertent)
- Malinformation (malign / belligerent)
- Creation / production / distribution
- Sender / message / interpretation

The threat actor wish list

Source: UK GO Science (2014)

An adversary's or threat actor's ability to use IC/ID and:

- Target any device, on any network path.
- Target anybody, any place, any business, any organisation.
- Target anywhere, anytime.
- Apply this to any context or event.
  (elections, conflict, politics, health, environmental, etc.)
  (esp. 'wedge issues')

Threat trends

Internet of Things (IoT)

Decentralised internet (DWeb)

Adaptive tradecraft

Affective computing

Intelligence-as-a-Service

Privacy Enhancing Technologies (PET)

Disinformation-as-a-service

AI, Automation, Autonomy

Digital and media lawfare

Digital immersion

Widening and partisan media landscape

Fragmented individual identity

Brain-Computer Interface (BCI) and Brain-to-Brain (B2B) communication

Computational social science

Attention economics

Cost and benefit of a developing or future threat trend

dstl The Science Inside

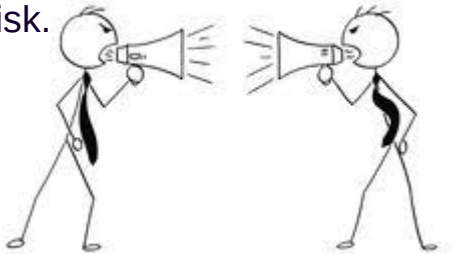
Internet of Things (IoT)

A world in which everyday networked devices are defined by connection, collection, computation and creation.

	Threat Actor	Friendly Nation/Force
Helps	• Increased sources (and types) of data (for intelligence purposes). • Data about people has significant commercial value. • Provides a wider attack space in order to deliver IC/ID. • Any time, any where, any device, any network, any organisation, any real-world context. • IoT technologies can act as a nexus for super-spreading IC/ID.	• Could act as a conduit for countering and mitigating IC/ID in terms of digital literacy and messaging. • Security of future devices and networks will be improved (aka secure by design).
Hinders	• Secure by design and privacy preserving protocols hinder Red's ability to access, collect and/or share. • Networks and devices are so ubiquitous that adversary cannot sufficiently plan and execute a robust campaign. • Proportion of IoT networks will possess weak connections, which limit the ability to access and aggregate data across networks.	• Challenges with controlling the IoT in terms of laws and regulations. • Challenges with monitoring IC/ID via IoT technologies. • Becomes a game of whack-a-mole whereby Blue is overmatched.
Assessment	RED will start with an advantage because if it innovates sufficiently the IoT landscape will enable access to data for intelligence gathering and targeting purposes (whether wide area targeting, specific audience targeting, and micro-targeting). The IoT landscape potentially provides a wider attack space for delivering IC/ID, as well as acting as a super-spreader of IC/ID throughout IoT networks.	

Examples of societal responses

- *Confidence and trust* in institutions is degraded.
- *Empowerment, control, ownership*: ‘Their’ data, not ‘data on them’.
- *Risk-centric consumer*: Increased agency of personal data also means owning the risk.
- *Polarised echo chambers of individual certainty*
  - Pushing people to radical and extreme peripheries.
- *Digital deficit*
  - Cognitive abilities will be challenged in multiple ways, incl. capacity for analytical thinking, memory, focus and mental resilience (incl. mental health and well-being).
- *Socio-digital dissonance*: Biopsychosocial conflict within individuals between two competing tensions:
  - (1) Ease of connectivity and access to things that make life quicker, simpler, better.
  - (2) Threats and risks: Individual online data protection and security is boring and time consuming.
- *Morals and ethics:* IC changes societal morals, leading to codified ethics, which impact on digital human rights and digital governance.



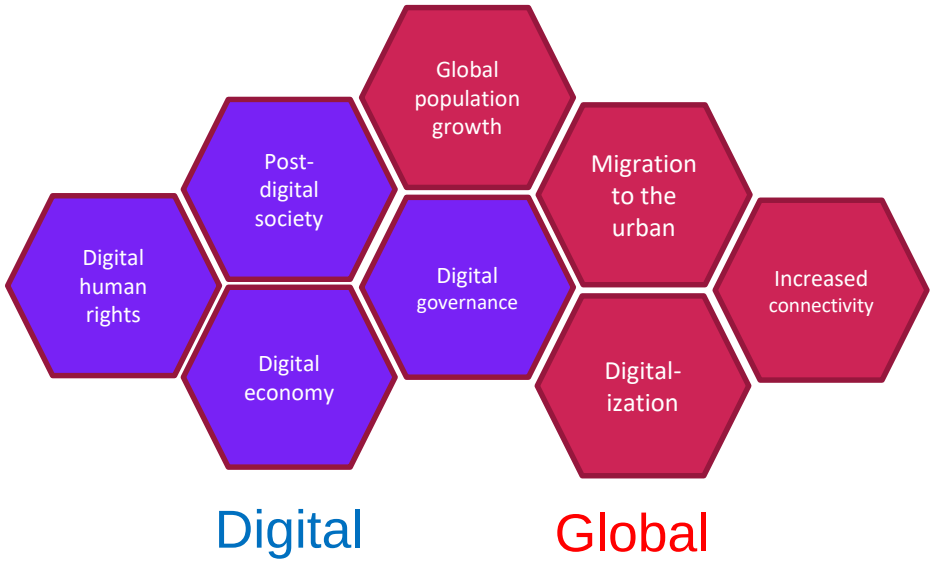
Source: Dreamstime.com

Source: VectorStock.com

Summary scenario

[dstl] The Science Inside

"Information Civilization" → "Information Confrontation" (IC)
"Information Disorder" (ID)



Globalised civilization that is information and data-centric.

Future Information Civilization

Future threats

Adversary uses agility and innovation to exploit opportunities, fissures and loopholes in order to employ IC/ID

How society responds to the overt and covert use of IC/ID (individual, group, national, cultural).

Future societal responses

Future IC/ID

The interaction of IC/ID in a globalised hyper-connected digital world.

Summary

- The world is moving towards an ‘information civilization’.
  - The global big picture meets the digital backbone of societies.
- Changes in society and technology provides benefits, but also threats and risks:
  - The attack space for IC/ID and online harms is increased.
  - Range of threat actors is diffuse (hostile states, authoritative regimes, proxies & non-state, organised crime, activists and webs of belligerent keyboard warriors)
  - Threat actors demonstrate agility, innovation at pace, a greater freedom of manoeuvre in the IE (or IEs [plural]).
  - IC/ID becomes mainstream and normalised.
- The challenges for Defence & Security domain, and wider apparatus of Governments:
  - Help vs. Hinder of threats – ‘what works for me works against my opponent’.
  - Proactive or reactive.
  - Interdependent operating model with ICT industries, sectors and companies (can’t do it alone).
- Implications for human behaviour (individual, group, national, cultural).

[dstl] The Science Inside

Discover more