Information Disorder and Future Threats

Professor Neil G. Verrall
Defence Science and Technology Laboratory
Porton Down, Wiltshire
UNITED KINGDOM

ngverrall@dstl.gov.uk

ABSTRACT

The presentation will describe some of the potential ways in which Information Disorder will evolve in the future – as a function of changes in technology and society. Fifteen threat trends are identified, which will have the potential to either help or hinder both threat actors and governments, i.e. what works for me, works against my opponent. Therefore, the risk is how, and indeed 'if', future governments decide to address the impact of predicted changes in society and technology, and whether to, and how to, mitigate the potential applications of these by a range of threat actors.

The future of information disorder is set against the backdrop of what is soon to become human history's first 'information civilization', which will be influenced by two major factors: (1) global issues such as population growth, migration and the environment; and (2) a post-digital society, concerning issues such as connectivity, digitalisation, digital human rights, digital economies and digital governance.

The future of information disorder is important to understand because of its enduring role within a future information civilization and the increased potential for information confrontation among future generations; thereby leading to increased national and global security threats.

1.0 INTRODUCTION

Confrontation can lead to disorder, which can lead to conflict, which can lead to war – and in the words of Margaret Atwood "Wars happen because the ones who start them think they can win" [1]. Therefore, militaries can no longer wait to be involved at the warfighting stage of human disorder and conflict. The military must take a proactive stance in order to protect against, engage with, and constrain threats, before they become fully realised as conflicts and wars [2]. There is a need to now fully accept how confrontation and disorder in the information environment sits alongside confrontation and disorder in the physical environment, where physical force can be used in order to intimidate or control, as well as the desire to cause injury or death. This symbiotic interaction between the physical and virtual domains has clearly been seen with Russia's invasion of Ukraine, which has produced a more mature version of the relationship that began with the military operations in Iraq and Afghanistan, and their occurrence during the rise of mainstream internet and the creation of social media and social platforms.

2.0 RATIONALE

Human engagement with digital Information and Communications Technologies (ICT) is producing societal challenges, as well as pro-social societal change. In addition, the tradecraft and tactics, techniques and procedures (TTP) of adversaries, hostile states and authoritative regimes in the information environment, particularly in terms of disinformation, is becoming better recognised, understood and countered [3,4,5,6]. However, the issue is not just whether nation states and militaries can perform effectively in the here and now, but how they will also perform in the future, where changes in technology and society will continue to occur, but may also change more rapidly, and potentially in unanticipated and unintended ways. NATO's

latest strategic concept touches on this rationale [7] and the current paper will also touch on numerous and related topics as part of the symposium's theme, objectives and outputs.

3.0 DESCRIPTION

The paper is divided into four key areas. It will start with some scene setting of how global and digital drivers will bring about the world's first information civilization. Next, the concepts of information confrontation and information disorder will be introduced and described. Thirdly, the nature of the threat will be described, as well as the associated risks, benefits and opportunities that will either help or hinder, depending on whether governments decide to take a proactive or reactive approach to mitigating or counteracting such threats. Finally, some of the implications for human behaviour are touched upon.

3.1 The Global Big Picture

The world, and the inhabitants of it, are always undergoing some form of change. However, there is a perception that some of these changes are accelerating at rates faster than had previously been known or predicted to occur. Figure 1 presents a visualisation of the global big picture, within which there will be societal challenges for operations in the information environment.

3.1.1 Population growth

The global population will continue to rise, albeit at lower levels than previously predicted. Nevertheless, it is estimated by the United Nations Department of Economic and Social Affairs [8] that the current population of approximately 8 billion global inhabitants could likely plateau at 11 billion by the end of the century, which is a rise of 30% in a little under 80 years; with the largest growth rates expected to be in Asia and Africa. Therefore, **there will be more people to be connected to digital ICT, and more people connected to each other**.

3.1.2 Migration

Humans are increasingly moving to urban conurbations, and by 2050 it is estimated that 68% of the global population will be living in urban environments. This could be accelerated with the rapidly increasing effects of climate change. These urban conurbations will also spread out, therefore, there will be a rise in the number of 'megacities', with the top ten megacities having populations ranging between 35-50 million inhabitants. Therefore, **there will be more people connected in large population centres.**

3.1.3 Digitization and digitalization

The digitization of systems continues at pace. Traditional records and systems will become fully digitized and increasingly automated, meaning that the 'digital by default' philosophy will become fully realised. As the population grows, and those people predominantly live in urban environments then more people will be digital by default. However, outlying communities and the poor will continue to be behind the curve; therefore, **digital literacy rates will widen between the richest and the poorest.**

3.1.4 Connectivity

The rising number of human beings will be connected to an even larger number of networked devices. By 2030 it is estimated that the number of devices could range between 50-125 billion. The generation after next (GAN) may be **the first post-digital society, which could be defined by what is not connected and automated, as opposed to what is**; which is to say, that the expectation of 'digital by default' and the

mainstreaming of the Internet of Things (IoT) is constant and normalised.

Figure 1: The global big picture.
Source: Author generated.

3.2 An Emerging Information Civilization

An information civilization could be described as one that is global, hyper-connected, and information- and data-centric [9].

Figure 2: Digital factors.
Source: Author generated.

3.2.1 Digital and post-digital society

As described above, the post-digital society is defined by what is not connected and automated, as opposed to what is; which is to say that society will automatically assume that connectivity, internet speed and daily human life online will be constant and normalised. Previous research on military personnel and their families has shown that younger military personnel see the issue of connectivity as a human right [10]. Other issues that shape a post-digital society include the hyper-connectivity of places, such as smart towns and cities; and the IoT becomes fully realised. In addition, the consumer is fully digital, including associated behaviour aspects of engagement, experience and empowerment.

3.2.2 Digital human rights

The promotion, protection and enjoyment of human rights on the internet has been enshrined in law [11], as well as a wider set of digital rights, such the right to be forgotten (aka the right of erasure). Civil Society will have made significant strides toward the eradication of digital exclusion and digital poverty in developed societies; although it will be impossible to eradicate these in their entirety, and it will still exist in larger ratios within developing nations; therefore, digital inequalities will still exist as far as digital literacy is

concerned. Empowered consumers will also possess improved rights in terms of data privacy and data ownership. However, the corollary of this is that companies, industries and sectors (e.g. the consumer sector) will shift the risk of data protection and data security onto the individual, who will now be responsible for their individual data security, which they will be able to keep, update or delete on an individual basis.

3.2.3 Digital economy

This relates to how national industries, productivity and prosperity will be increasing driven, or led, by digital economies. The balance between traditional economies and digital economies will have permanently shifted as a product of digital and technological transformation.

3.2.4 Digital governance

The 'digital by default' philosophy will have been fully realised, and replaced by the 'secure by design' philosophy, which seeks to protect the IoT and the billions of digital devices connected to the internet, or series of internets such as the decentralised internet (aka DWeb) [12]. A set of established charters, standards, regulations and codes will govern the digital ecosystem and its underpinning infrastructure of systems and technologies.

3.3 A Realised Information Civilization

The interaction between the digital and global drivers of human existence will mean that the world's first information civilization will be realised. The eldest people on the planet will have been originally born into a digital world, where they only knew digital ICT and connectivity to the internet.

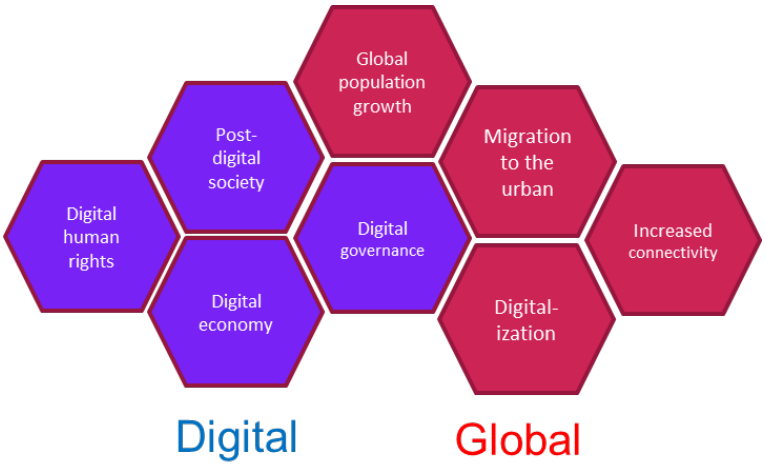

Figure 3: Factors that shape an Information Civilization.
Source: Author generated.

3.4 Information Confrontation and Information Disorder

Persistent confrontation in the modern information environment is giving rise to a generalised feeling of information disorder. Information Confrontation (IC) is a recognised term in the Russian military lexicon [13], whereby it refers to targeting impact on the information infrastructure of the enemy, while simultaneously protecting one's own infrastructure from enemy activities. A further term, Information and psychological confrontation, is part of the same concept, but differs in that it is aimed at the consciousness and feelings of populations, armies, and governments of opposing, friendly and neutral countries; it is

weapon, a resource and a goal; and that it is a channel (method) or means of delivery.

The concept of Information Disorder (ID) (Table 1) was initially conceived as an amalgamation of disinformation, misinformation and malinformation [14]. By considering both of these concepts in unison, they give a more up-to-date and nuanced appreciation of what happening in the contemporary information environment, which replaces the hitherto one-dimensional and over-simplistic reference to 'disinformation' per se.

Table 1: Key elements of Information Disorder.
Source: Refs [5,14,15]

Types	Elements	Phases
Disinformation Deliberate creation and dissemination of false information.	**Agent** The person / people who create, produce and distribute.	**Creation** The message is created.
Misinformation Inadvertent sharing of false information.	**Message** The format, characteristics and content of messages.	**Production** The message is turned into a media product.
Malinformation Based on reality, used to inflict harm on a person, organisation or country.	**Interpreter** How the information / message is received, perceived and believed, i.e. interpretation.	**Distribution** The message is distributed or made public.

3.5 The Nature of the Threat

3.5.1 The threat actor wish list

In 2014 the UK Government published a report on the IoT [16], which contained a useful visualisation of the IoT aspirations (Figure 4). This image can be flipped and seen through the eyes of an adversary or threat actor, who would seek to employ IC/ID in order to:

- 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. This is currently employed to target general national politics by seeking to undermine democracy; to target democratic processes, such as elections; by targeting health issues (e.g. COVID-19); and also the environmental, via the climate change debate. Therefore, IC/ID is particularly powerful when targeted at 'wedge issues' that seek to push people into the extremes of their respective echo chambers.

Figure 4: Internet of Things.
Source: UK GO Science [16].

3.5.2 The threat trends

Societal and technological change is occurring at a faster pace than previously assumed. Figure 5 presents examples of some of these changes; some are already with us and are improving, and others are yet to be realised. These threat trends represent topics that adversaries, hostile states, authoritative regimes, organised crime, and even activist groups, could potentially exploit in support of their objectives.

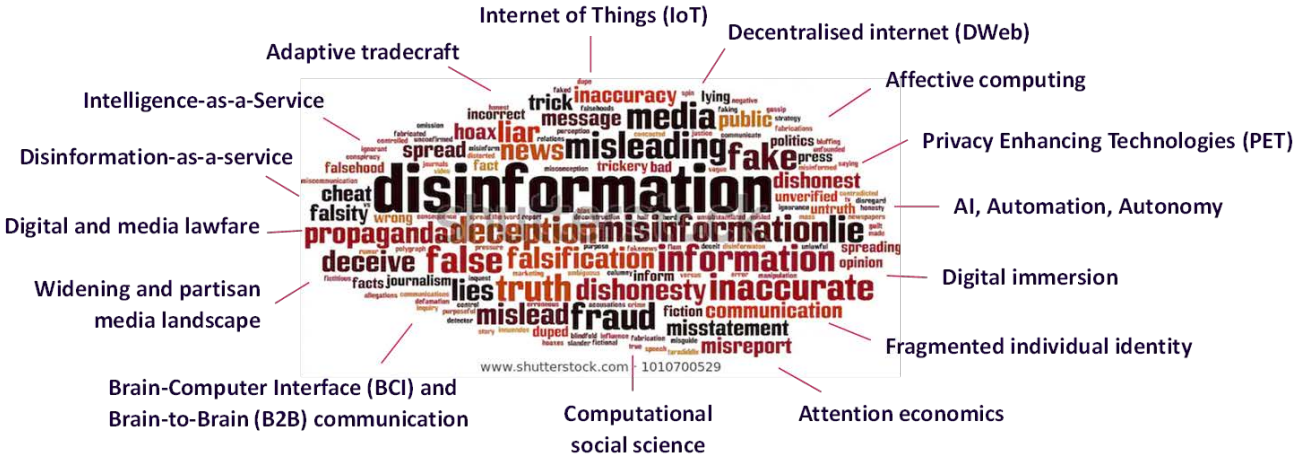

Figure 5: Examples of emerging threat trends.
Source: Author generated [17].

3.5.3 Decisions or mitigations that help or hinder

There is an old unattributed military maxim that says ‘what works for me, works against my enemy’. Figure 6 presents an example 2x2 matrix interaction that shows how the IoT concept could either help or hinder a threat actor (Red); or alternatively, help or hinder a friendly nation of force (Blue), depending on how they each use a proactive or reactive mindset to countering or mitigating the potential risks and benefits from the

IoT concept. The interaction occurs whereby a proactive action by Blue, which is to its benefit should produce a challenge to Red, i.e. what helps Blue, should hinder Red. This matrix style thinking can be applied to any emerging threat, whether technological or societal, as shown above in Figure 5.

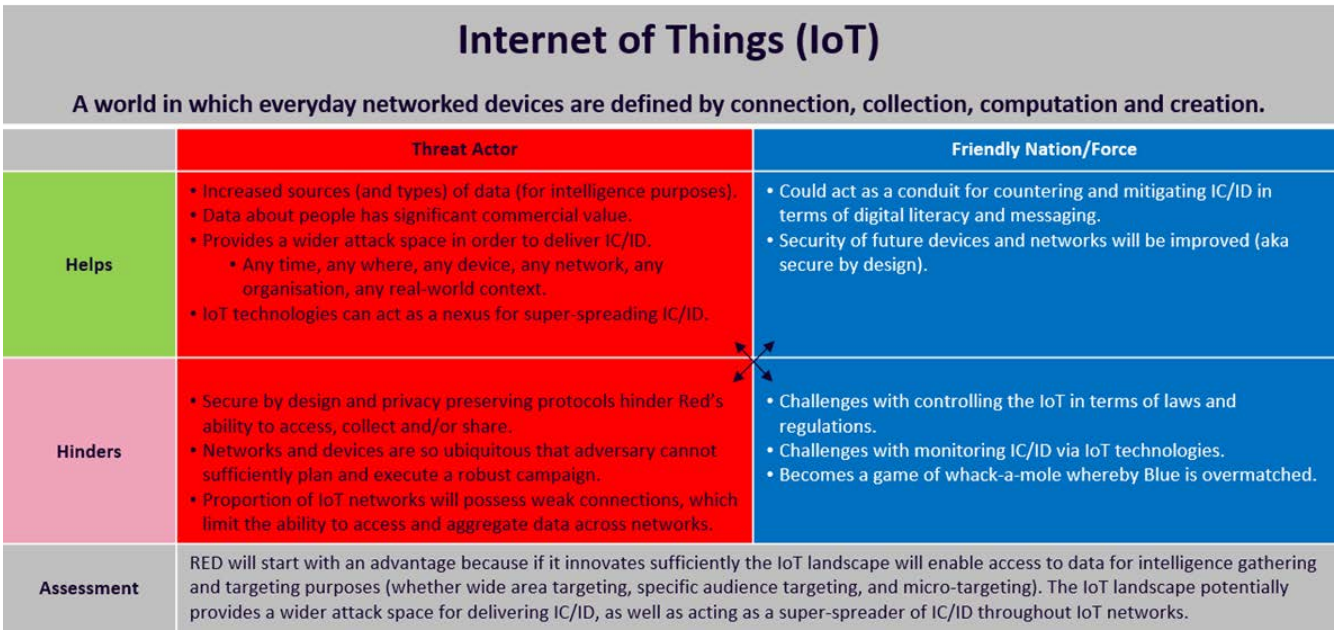

Figure 6: The help or hinder matrix.
Source: Author generated [17].

4 IMPLICATIONS FOR HUMAN BEHAVIOUR

Naturally, societal and technological changes, as well as the activities of governments and belligerents, possess implications for subsequent human behaviour. Without wishing to go into extensive detail, or accounting for the entirety of permutations, a short list of potential implications is provided below.

- **Confidence and trust.** This refers to the increasing loss of confidence and trust that people have in institutions.

- **Empowerment, control and ownership.** People want increasing control of their personal data; therefore, the issue shifts from 'their' data instead of 'data on them'.

- **Group polarisation.** IC/ID will push people to more radical and extreme peripheries of polarised echo chambers. This is already evidence for some wedge issues, but an increasing number of complex societal issues will only increase the potential for IC on a range of issues and real-world events.

- **Digital deficit.** Cognitive abilities will be challenged in multiple ways, including the capacity for analytical thinking, memory, focus and mental resilience (incl. mental health and well-being).

- **Socio-digital dissonance.** The biopsychosocial conflict within individuals' psyche implies two competing tensions: (1) the desired ease of connectivity and access to things that make life quicker,

simpler, better, versus (2) individual threats and risks, because individual online data protection and security is boring and time consuming.

- **Morals and ethics.** This refers to how changes in social morals will slowly shift to more codified ethics of IC/ID as part of the Online Harms philosophy. This feeds into the post-digital aspects of digital human rights, which will later be addressed by changes in digital governance.

5 CONCLUSION

The world is fast moving towards an 'information civilization'. Central to this are changes in the global big picture, which is to say, increased population growth, which requires more and better connectivity; mass migration of people to urban environments and the rise of meta-cities; as well as the continued digitization of systems and digitalization of people. This occurs at the same time as society moves toward a post-digital society, which is where society is defined by what is not connected and automatic, rather than what is, which becomes expected and normalised. Underpinning a post-digital society are issues surrounding digital human tight and digital governance, which seek to drive and support digital economies, digital consumers; ergo, national and human culture is digital.

Unfortunately, changes in society and technology provide a larger attack space for IC/ID, as well as range of broader online harms. This is exploited by adversaries, threat actors and belligerents, who are diffuse, and operate with agility, demonstrate innovation at pace, and enjoy a greater freedom of manoeuvre in information environments. Therefore, IC/ID becomes mainstream, unless the Defence and Security domain, in concert with the wider apparatus of Government (incl. ICT companies, industries and sectors) proactively address the future threat trends that will either help or hinder themselves, and their opponents – 'what works for me, works against my opponent'. All of this means implications for human behaviour (individual, group, national, cultural) for all populations and target audiences within post-digital societies.

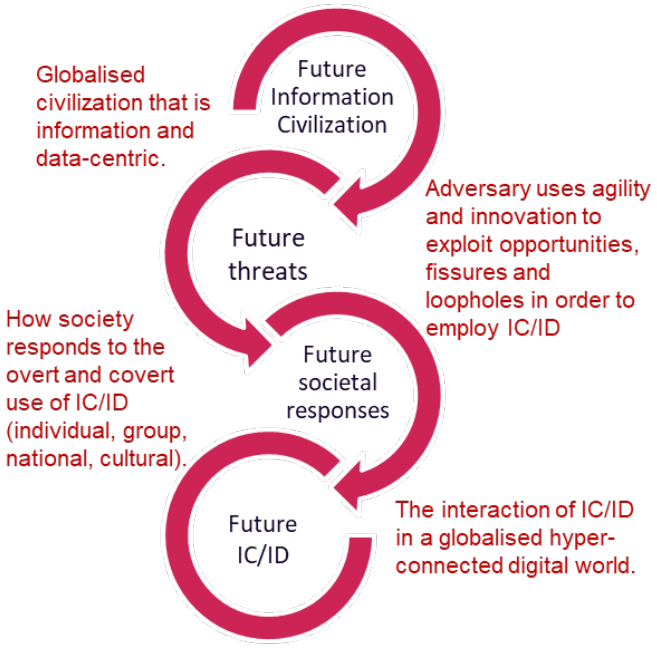

Figure 7: The concluding future scenario. Source: Author generated [5].

References

[1] Atwood, M. (1995). "The Loneliness of the Military Historian" (pp. 49-53) from *Morning in the Burned House* (Toronto: McClelland & Stewart).
https://www.poetryfoundation.org/poems/47788/the-loneliness-of-the-military-historian

[2] UK Ministry of Defence. (2021). *Integrated Operating Concept* (London: MOD).
https://www.gov.uk/government/publications/the-integrated-operating-concept-2025

[3] Government Communications Service. (2019). RES*IST Counter-Disinformation Toolkit* (London: Government Communications Service).
https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf

[4] Government Communications Service. (2021). RESIST 2 Counter-Disinformation Toolkit (London: Government Communications Service).
https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/

[5] Verrall, N. (2022). Chapter 4 - COVID-19 Disinformation, Misinformation and Malinformation during the Pandemic Infodemic: A View from the United Kingdom. In R. Gill & R. Goolsby (Eds.), *COVID-19 Disinformation: A Multi-National, Whole of Society Perspective* (Switzerland: Springer).
https://link.springer.com/book/10.1007/978-3-030-94825-2

[6] Verrall, N. & Mason, D. (2018). The taming of the shrewd – how can the military tackle sophistry, fake news and post-truth in the digital age? *RUSI Journal*, 163(1), pp. 20-28.
https://doi.org/10.1080/03071847.2018.1445169

[7] NATO. (2022). *NATO 2022 Strategic Concept* (Brussels: NATO).
https://www.nato.int/strategic-concept/

[8] United Nations. (2022). *World Population Prospectus 2022* (New York: UN).
https://population.un.org/wpp/

[9] Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, pp. 75-89.
https://doi.org/10.1057/jit.2015.5

[10] Adey, P., Denney, D., Jensen, R. & Pinkerton, A. (2016). Blurred lines: Intimacy, mobility, and the social military. *Critical Military Studies*, 2(1–2), pp. 7-24.
https://doi.org/10.1080/23337486.2016.1148281

[11] United Nations. (2021). Resolution A/HRC/47/L.22 he promotion, protection and enjoyment of human rights on the Internet, 7th July 2021, UN Human Rights Commission.
https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/47/L.22

[12] Pierce, D. (2021). 'The Decentralized Internet is Coming'. *Protocol*, 17 January 2021. Available at:
https://www.protocol.com/newsletters/sourcecode/decentralized-blockchain-internet?rebelltitem=1#rebelltitem1

[13] Ministry of Defence of the Russian Federation. Military encyclopaedia available at:
https://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm

[14] Wardle, C. (2019). *Understanding Information Disorder* (London, UK: First Draft). https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701

[15] HM Government. (2019). *Online Harms White Paper* (London: HM Government). https://www.gov.uk/government/consultations/online-harms-white-paper

[16] UK Government Office for Science. (2014). *The Internet of Things: making the most of the Second Digital Revolution* (London: GO Science). https://www.gov.uk/government/publications/internet-of-things-blackett-review

[17] Verrall, N. (2021). *Analysis of Future Threats from Disinformation*, DSTL/TR130028 (Porton, UK: DSTL).