‘It Takes a (Global) Village’: Towards a Multi-Actor Networked Conception of Security

J. Keith L. Scott
De Montfort University, Leicester, UK

jklscott@dmu.ac.uk

Abstract: On December 4th 2023, Oliver Dowden, the British Deputy Prime Minister, issued his first annual resilience statement, outlining the range of threats faced by the United Kingdom, natural, economic, military, and technological. The purpose of this paper is to examine the contemporary threat landscape through the critical lens of complex interdependency (cf Keohane and Nye), and to consider the way in which approaches and theoretical models of threat and threat mitigation can and should (or should not) be applied in different domains. Multi-Domain conflict shows how the modern battlefield is a highly complex realm of interlinked environments (including the non-physical); in the same way, ‘unrestricted warfare’ (Qiao and Wang) collapses the traditional DIME concept of discrete arms of state power. How may a liberal democracy protect itself and its citizens against mis/disinformation, cyber warfare, hacktivism, NSAs and foreign powers ready and able to to wage ‘war’ in a wide range of ways, using IW both as a specific methodology and as a force multiplier for other forms of destabilization. Focusing largely but not overwhelmingly on the informational realm, the paper will consider models of threat mitigation applied in other domains, from the elite innovative force of the Rifle Brigade to the public health response to the COVID-19 pandemic to the behavioural science-based influence campaigns devised by the UK ‘Nudge Unit’ and beyond. It will ultimately argue that a nation which faces a range of internal and external threats to its stability must devise policy and strategy which themselves operate internally and externally. Any approach which is not based on action at all levels of society – civil, military, educational, technical, diplomatic – is doomed to failure before it starts. However, the key challenge will be how to build this in societies which have grown ever more atomised, divided, and opposed to cooperation.

Keywords: Cyber Security, Governance, Civil Defence, Mitigation, Resilience.

1. Introduction

‘there is nothing but networks, there is nothing in between them’ [Latour 1996: 370]

A recent article in the UK *Guardian* (Chayka 2024),discusses the proliferation of ‘hipster coffee shops’, offering quasi-identical environments, atmospheres and menus, not as part of a global corporate marketing strategy, but as a data-driven exercise in satisfying a widespread aesthetic determined by an algorithm derived from consumer posts on social media. Chayka dubs the zone(s) created by this process ‘AirSpace’:

> my coinage for the strangely frictionless geography created by digital platforms, in which you could move between places without straying beyond the boundaries of an app, or leaving the bubble of the generic aesthetic.

This tendency towards a universal sameness parallels observations made of the homogenising tendency of globalising corporate capitalism (Tomlinson 1995), but it springs from a very different driver. As with the concept of the ‘participatory panopticon’ (Stross 2002), where we accept continuous monitoring of our online activity as inseparable from our need to continually share our opinions and experiences, so this desire to inhabit a seamless AIrSpace results from the users’ wishes for stability, security, and the comfort of the familiar.

It is a truism to say that the modern world is built on ever-greater connectivity, but truisms rest on truth; we exist within a dynamic constellation of physical and informational networks, transmitting and transferring data, money, and ideas. As Manuel Castells (2011) observes, the network is *the* essential basis of modernity, on and within which which all power and influence reside. Identity and agency at all levels, from individual to global, is confined and defined by the place an actor occupies in relation to all the other actors, human, non-human, corporeal and abstract.

Castell’s work on the network society and the power structures within it elides well with a number of other theoretical models which we may loosely call ‘poststructuralist’ (and indeed to Classical philosophers such as Heraclitus, and the concept of ceaseless flow). In works by Deleuze and Guattari such as *A Thousand Plateaus*, they argue that the idea of a rigidly ordered, logical hierarchy of existence should be replaced by the idea of a dynamic, decentred organizing principle analogous to the *rhizome*, which ‘‘[…] has no beginning or end; it is always in the middle, between things, interbeing, intermezzo.’ (Deleuze and Guattari 1987; Bluemink (2015) offers a very clear discussion of the application of the concept of the rhizome to the structure of the online world). Similarly, Bruno Latour (whose words form the epigraph to this section) has been one of the founders of the school of Actor Network theory, which seeks to investigate:

> The attribution of human, unhuman, nonhuman, inhuman characteristics; the distribution of properties among these entities; the connections established between them; the circulation entailed by these attributions, distributions and connections; the transformation of those attributions, distributions and connections of the many elements that circulate, and of the few ways through which they are sent [373]

in other words, the systems of human, non-human and ideological/informational networks which form the basis of our work.

There can be no doubt that works such as these have not been welcomed unquestioningly by the academy and beyond; Deleuze and Guattari, for example, have been described as producing an 'avalanche of ill-digested scientific (and pseudo-scientific jargon' [Solal and Bricmont, 1998: 155), but their at times rebarbative style should not blind us to the utility of what they say, and the relevance of their discussion of networks to cyber security. The idea of non-linear, non hierarchical dynamic power structures maps directly onto much thinking about hybrid warfare (Robb 2007) and the complex of interacting systems which challenge attempts to create stability in an unstable world, but in a deeper, more fundamental way, the focus these writers have of interconnection and interaction between the human and non-human harks back to the the early years of Information science, and what could justifiably be called one of the *ur*-texts of our discipline.

In 1950, Norbert Wiener published *The Human Use of Human Beings*, the second in what can be seen as a loose trilogy of works[1] for the general reader setting out the relationship between humans and machines at the birth of the modern Information Age. Leaving aside the vexed question of defining 'cybernetics' in a way that captures its spread into so many fields, the key point here is that for Wiener, we must see the world as operating as a series of systems, as in many ways a self-governing machine, a 'machine' which like the rhizomatic 'assemblages' of Deleuze and Guattari and Latour's networks, is fundamentally heterogeneous:

> I have spoken of machines, but not only of machines having brains of brass and thews of iron. When human atoms are knit into an organization in which they are used, not in their full right as responsible human beings, but as cogs and levers and rods, it matters little that their raw material is flesh and blood. What is used as an element in a machine, is an element in the machine. [Wiener 1950: 212-3]

Wiener is speaking here of the danger of exploitation of the various components of the machine (humans and non-humans can be abused; 'robot' of course derives from the Czech for 'indentured labour'), but throughout his work, he sees networked existence as not inherently threatening, but inevitable. Those who seek to divorce themselves from the structures that sustain the modern world are doomed to failure, whether those networks are technological, political, or cultural.

2. Cyber Security in a World of Networks

Defining the nature and scope of cyber security is at best a challenging exercise, given that it covers all aspects of potential threat and risk to all aspects (physical, electronic, human) of information systems. However, at its heart lies the concept of the network (and all its component nodes), the totality rather than individual elements. This had been at the heart of the field since before the creation of the first wide area packet-switched network. ARPANET was switched on in 1969, the year after the publication of Licklider and Taylor's seminal paper, 'The Computer as a Communication Device'. However, the year before *this*, a paper had already been presented, discussing the inherent security risks in what was as yet an entirely theoretical entity: Willis Ware's 'Security and Privacy in Computer Systems'. It should be noted that even here, where the Internet as such does not exist, Ware is already discussing risk and threat deriving from hardware, software, and human factors; the computer network intersects with a wide range of other systems and networks , and only a holistic vision can lead to a truly effective scanning of the threat landscape.

Consider the various systems and networks on which modern technology relies, and the myriad different ways each of them can be compromised, kinetically and/or non-kinetically. The transfer of data from one user to another relies on the existence of virtual and physical networks, which depend on networks of construction and

[1] The other two works are *Cybernetics: Or Control and Communication in the Animal and the Machine* (1946) and *God & Golem, Inc.: A Comment on Certain Points Where Cybernetics Impinges on Religion* (1964).

distribution (to build and install the physical infrastructure), which depend on transport networks and logistics firms, and the whole is underpinned by a hugely complex network of global finance and investment – which is in turn governed and monitored by international organisations and national and international parliaments… 'there is nothing but networks', as it were. And the destruction or impairment of any aspect of any one of these networks can bring down the entire system of systems through a cascade failure. In 'Form, Substance, and Difference' (1987) Gregory Bateson use the example of a blind man walking with a stick to point out the impossibliity of establishing neatly bounded systems:

> Suppose I am a blind man, and I use a stick. I go tap, tap, tap. Where do *I* start? Is my mental system bounded at the handle of the stick? Is it bounded by my skin? Does it start halfway up the stick? Does it start at the tip of the stick? But these are nonsense questions. The stick is a pathway along which transforms of difference are being transmitted. The way to delineate the system is to draw the limiting line in such a way that you do not cut any of these pathways in ways which leave things inexplicable. If what you are trying to explain is a given piece of behavior, such as the locomotion of the blind man, then, for this purpose, you will need the street, the stick, the man; the street, the stick, and so on, round and round. [467]

Human beings, Bateson argues, seek to define neat boundaries between subjects, domains, fields of knowledge and experience; but reality is less tidy. Given the range of domains over which cyber security stretches, what are the necessary areas of knowledge for its practitioners? Specialisation and expert knowledge can all too easily lead to silo thinking and groupthink, how can we develop a theoretical model of, and practical training in, cyber security which meets our actual needs?

Such questions are already being asked in a military context, where traditional schemas and methodologies are challenged by the growth of asymmetric and hybrid conflicts, where the division between 'war' and 'peace' is largely one of perception and interpretation rather than degree (one is, after all, as dead if killed in a 'special military operation' that in a *proper* 'war')[2]. Modern military thinking across the globe (US Department of Defense 2022; UK Ministry of Defence 2020; Black et al. 2022) shows an increasing emphasis on developing the ability to operate across multiple domains simultaneously; the UK views the five domains of warfare as land, maritime, air, space, and cyber/electromagnetic, but the informational domain intersects and governs all of these domains. The multi-domain model poses severe challenges to the traditional divisions between the differing branches of the armed services, but there seems to be little willingness at present to consider what a true multi-domain fighting force could or indeed should look like. Such questions do however need to be asked, and rapidly, not least in the light of the publication of Qiao and Wang's *Unrestricted Warfare*, which reshapes the conception of 'war' as kinetic and non-kinetic, conducted in stock exchanges and newsrooms as much as on the battlefield. They declare:

> The battlefield will be everywhere […] all boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed [Part 1].

The growth of online misinformation as a tool of destabilisation, restriction of oil and gas flows (or the treat thereof), government sponsorship of criminal activity, the use of irregular forces in combat… all of these mark a clear step towards 'unrestricted warfare', though a fully-fledged, truly multi-domain conflict has yet to be seen (or, perhaps, we do not recognise it as such). And the cyber domain is a key component in all of them; how are cyber security practitioners to respond? The civil sphere cannot simply say 'leave cyber war to the military', because cyber conflict does not occur solely in the military sphere (it makes much more sense to launch cyber attacks against civilian targets, as they are much more likely to be poorly defended). How can we possibly prepare for an attack which may come at any time, in any domain, in any number of ways?

3. Models of Mitigation: Top-down, Bottom-up, and People Power

[2] There has already been some very interesting work drawing directly on Deleuze and Gyuattari's work and applying it to modern conflict; see Huhtinen, Hirvela, and Kangasmaa (2014); Huhtinen and Rantapelkonen (2016); Sartonen, Huhtinen, and Lehto, M. (2016).

The cyber security challenges of a networked world cannot be solved by technological means alone; cyber action is always already a political act, and operates within a world of international political and governmental accords. National action can only go so far; there must be an overarching global legal framework to allow coordinated action across boundaries. While the Tallinn Manual sets out an initial model for the regulation of cyber warfare, it is still an early step, and does not deal with the wider context of non-military cyber harm. If we wish to see the establishment of such a model for global cooperation against such threats, there are a number of major difficulties which must be addressed. Firstly, we are living through a period of growing isolationalism and anti-internationalism across the globe, with a growing number of governments and political parties espousing extreme nationalism; Hungary, India, Turkey are only three examples of this trend, with further significant rises for right wing nationalist parties in Germany, France, and the Netherlands. The prospect of a second presidential term for Donald Trump in the United States raises further red flags for the survival of NATO and the continued destabilising actions of Russia. The paradox here is that all states seeking to withdraw from international cooperation and declare renewed national autonomy act only to disadvantage themselves; as complex interdependence theory (Keohane and Nye 1973; 1987) points out, international relations depends, unsurprisingly, on relations, and cooperation and participation in multinational accords which act to the mutual benefit of all signatories. As post-Brexit Britain has discovered, withdrawal from membership of the European Union has lost the country all the advantages of belonging to one of the world's largest economies, from freedom of movement to barrier-free trade to the ability to coordinate international immigration accords. The idea of a totally autonomous nation state fre of external influence is, and has always been, a myth; even North Korea, overtly espousing the concept of *juche*, cannot exist without being propped up by China. However, the myth is potent, as can be seen by the number of actors calling for withdrawal from globalised economy and the establishment of '$NATIONNAME First' parties and policies. The only way to overcome such attitudes is low, painstaking diplomacy, and a willingness to reengage with the internationalist ideologies that helped shape the postwar world. As yet, the will for this does not seem to be present.

The second major challenge is practical; setting up any form of global accord is costly and time-consuming, and the proliferation of cyber security threats means that time is of the essence. There are moves at an international level to develop working systems of global cyber governance, such as the proposed expansion of the Abraham Accords (Warrick 2023), the recent review of cyber security under the aegis of the UN (Joint Inspection Unit 2021), and the issuing last year of *Guidelines for secure AI system development* (NCSC 2023). Within the commercial realm, the Cyber Security Tech Accord (https://cybertechaccord.org/) offers a possibility of developing a stable regulatory framework for global business, but there is as yet no guarantee of success. And while X/Twitter , for example, remains the personal fiefdom of Elon Musk, it seems that the cybersphere will continue to be awash with misinformation and disinformation (European Commission/TrustLab 2023; Climate Action Against Disinformation Coalition 2023).

The difficulty of designing and operationalizing a cyber security strategy at international level is matched at national level, for similar reasons; as the pandemic showed, developing effective courses of action against major threats to national security collides with party loyalties, resourcing crises, internal party tensions, and perhaps the greatest challenge, i.e. putting policies into action which will act beyond the term of the current administration. Within the UK, a further problem is that the overwhelming majority of members of the Cabinet are Humanities graduates (this is not necessarily a problem per se, but it does indicate a lack of relevant knowledge); more than that, the majority are graduates of only two institutions (Oxford and Cambridge), suggesting less a Government of All the Talents and more an opportunity for silo thinking. There is no doubt that a coordinated cyber security strategy requires top-down action at government level, and the National Cyber Security Centre has a vital role to play, acting as a coordinator and facilitator across the various wings of the state (primarily the judiciary and legal professions, law enforcement and the security services, but all other government departments must have involvement), but the current state of play, where the cabinet is riven by internal dissension, plotting, and the fear of electoral defeat, is in no way conducive to innovation. Add to this a pervasive lack pf trust in the government and Parliament among the general populace - 76% of the public in England do not trust MPs to take decisions that will improve their lives, and 73% do not trust the UK Government on the same measure (Carnegie Trust 2022) – and the chance of encouraging public buy in to an inevitably greater level of state scrutiny of internet use seems diminishingly small. By the same token, the idea that the British public would accept military oversight of their online activity seems unlikely; in the same way that armed troops have not been deployed on the streets of the mainland UK except for very rare security action (Northern Ireland was very definitely the exception to the rule), it seems more than likely that there would be significant resistance to the idea of 'boots on the ground' in British civilian cyberspace.

On January 23rd this year, the outgoing head of the British General staff, General Sir Patrick Sanders, argued that the UK should be ready to increase the size of its severely reduced military through the creation of a 'citizen army'; while he denied that this meant a return to conscription or compulsory military service (as ended in 1963), but it seems hard to see how a policy not based on conscription could achieve the desired level of recruitment. This proposal has not met with an overly favourable response, and it has been attacked on logistical as much as cultural or political grounds (Stross 2023). However, there can be no doubt that there will need to be development in the structure and numbers of the UK armed forces, as much due to the challenge of multi-domain operations as to the need to respond to growing cyber threats, and that these changes will need to be supported by the general public. More than that, owing to the hybrid threat posed by non-kinetic, unrestricted warfare (where civilian targets are as legitimate as military ones), there is a need to bridge the gap existing between the military and civilian domains. Three possible next steps:

1. Promote recruitment to the Territorial Army to build expertise in the wings of the military specialising in cyber conflict, Electronic and Informational Warfare, such as the Royal Corps of Signals and the 77th Brigade;
2. Develop a programme of seconding members of these forces to the civilian sphere (trade and industry, finance, local government..) to act as onsite subject matter experts, engage in two way knowledge share, and aid in the support and training of the general public and
3. A cyber equivalent of the Royal Observers Corps, disbanded in 1996. The Corps' aim during World War Two was to identify and track hostile aircraft, and this duty then became to be ready to monitor the effects of a nuclear bombardment of the UK in the event of a conflict using atomic weapons. In the cyber context, the Corps would work in the civilian world, collating and reporting threats, risks and hostile activity at the operational level, feeding back information to a coordinating hub such as the NCSC or the MOD's Ministry of Defence's Global Operations Security Control Centre at Corsham. Inserting a human in the monitoring and reporting loop adds a further level of oversight, and the ability to coordinate response if required, as well as to play a role in training employees and staff members to better mitigate against cyber risk.

My argument is that we need to consider a bottom-up strategy of engagement and empowerment, focusing on SMEs and individual users; larger companies and organisations are generally (though not universally) better resourced and better able to deal with cyber threat. In a world where attacks and misinformation are targeted at individuals as part of large-scale influence campaigns, individuals need to be engaged, educated and empowered to defend themselves and others. If we take the pandemic as an analogy, an essential element of public health campaigning was to make individuals aware of what they could do themselves to reduce the risk of transmission, through vaccination and/or/social distancing and/or handwashing and/or mask wearing. A similar approach can. (and, I contend, must) be adopted in cyber security (McNutt and Crow 2023).

The obvious example to cite here is the programme of public education adopted in Finland against disinformation and Fake News, based on the development of Critical Thinking skills in the population, starting from early schooling (Kivinen 2023; Henley 2020; Gross 2023). As Kivinen (2023) puts it, 'Education is seen as part of collective civil defense'. The difference between the Finnish approach and that seen in the UK, is striking, and depressing for a British citizen.

So, in the final analysis, a multidomain always-on conflict requires a citizenry that is aware of the risks, educated as to how they can be resisted, and empowered to overcome them, and/or able to identify where this information should be reported to. It is not a panacea, but if certainly offers a better state of affairs than the status quo, and we have already seen how it can pay dividends. In a book published last year, Ryan J. Reilly discussed the 'Sedition Hunters', a group of online activists who responded to the attack the Capitol on January 6 2021 by engaging in a painstaking campaign of OSINT gathering, tracking down and identifying many of those involved and passing on their information to the FBI, leading to a number of convictions. When such tools are employed by the script kiddies of 4Chan we dub it doxxing and harmful (which of course it is, as it is motivated by the desire to humiliate and wound). What we have here is something very different; a collaborative effort by ordinary individuals to confront a security threat and act upon it. There is of course the potential of vigilanteism, which is why such actions must not occur in isolation and ungoverned, Throughout this paper, I have argued that we face a multitude of threats brought about by our essential reliance on complex systems of networks. If we do not attempt to understand them, we are at risk. As Meghan Conroy puts is in her review of S*edition Hunters*:

> we are in an era of networks, facilitated by the internet, social media platforms, and chat apps. […] These sleuths [the Sedition Hunters] hail from a spectrum of political beliefs, voting histories, career

backgrounds, and states, but are united in a shared cause. All in all, the threat may be a network, but a network may also be the solution.

It takes a village to raise a child; it is up to those of us living in McLuhan's 'global village' to learn how to inhabot the networked world and work together to make it safer.

References

Bateson, G. (1970), 'Form, Substance, and Difference'. In Bateson, G. (1987). *Steps To An Ecology Of Mind: Collected Essays In Anthropology, Psychiatry, Evolution, And Epistemology*. Northvale, New Jersey: Jason Aronson, Inc., 455-71.

Black, J., Lynch, A. Gustafson, K., Blagden, D., Paillé, Quimbre, F. (2022). *Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea*. Santa Monica, CA: Rand.

Bluemink, M., (2015), 'The Web as Rhizome in Deleuze and Guattari', *bluelabyrinths.com*, 15 July, [online], https://bluelabyrinths.com/2015/07/15/the-web-as-rhizome-in-deleuze-and-guattari/.

Carnegie UK Trust. (2022). 'Loss of public trust in Government is the biggest threat to democracy in England', 21 january, [online], https://carnegieuktrust.org.uk/blog-posts/loss-of-public-trust-in-government-is-the-biggest-threat-to-democracy-in-england/.

Castells, M. (2011), 'A Network Theory of Power', *International Journal of Communications* 5, 773-87.

Chayka, K. (2014). 'The tyranny of the algorithm: why every coffee shop looks the same', *Guardian*, 16 January, [online], https://www.theguardian.com/news/2024/jan/16/the-tyranny-of-the-algorithm-why-every-coffee-shop-looks-the-same.

Climate Action Against Disinformation Coalition. (2023). *Climate of Misinformation: Ranking Big Tech*. [online], https://caad.info/wp-content/uploads/2023/09/Climate-of-Misinformation.pdf

Conroy, M. (2024). 'It takes a network to catch a network'. *Bindinghook.org*, 18 January, [online], https://bindinghook.com/articles-book-binder/it-takes-a-network-to-catch-a-network/.

Deleuze, G. and Felix Guattari, F. (1987) *A Thousand Plateaus: Capitalism and Schizophrenia.* Trans. Brian Massumi. Minneapolis: University of Minneapolis.

European Commission/TrustLab. (2023). *Code of Practice on Disinformation: A Comparative Analysis of the Prevalence and Sources of Disinformation across Major Social Media Platforms in Poland, Slovakia, and Spain*. Brussels: European Commission.

https://disinfocode.eu/wp-content/uploads/2023/09/code-of-practice-on-disinformation-september-22-2023.pdf

Gross, J. (2023). 'How Finland Is Teaching a Generation to Spot Misinformation', *New York Times*, 10 January 2023, [online] https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html.

Henley, J. (2020).' How Finland starts its fight against fake news in primary schools', *Guardian*, 29 January, [online], https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news.

Huhtinen, A-M, Hirvelä, A. and Kangasmaa, T. (2014). 'The Opportunities of National Cyber Strategy and Social Media in the Rhizome Networks'. *International Journal of Cyber Warfare and Terrorism*. 4. 23-34.

Huhtinen, A.M. J Rantapelkonen,J. (2016). 'Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere'. *Journal of Information Warfare*, Vol. 15, No. 4, 50-67.

Keohane, R. O. and Nye, J. S. (1973). "Power and interdependence". Survival. ***15*** *(4): 158–165.*

" (1987). 'Power and Interdependence Revisited'. *International Organization*, 41(4), 725–753.

Kivinen, Kari. (2023). 'In Finland, We Make Each Child a Scientist'. *Issues in Science and Technology*,

Vol. XXXIX, No. 3, [online], https://issues.org/finland-education-misinformation-social-resilience-kivinen/.

Latour, B. (1996), 'On actor-network theory: A few clarifications', *Soziale Welt*, 47. Jahrg., H. 4, 369-81.

Licklider, J.C.R. and R. W. Taylor, R.W., (1968). "The Computer As a Communication Device," *Science and Technology*, Vol. 76, 21-38.

McNutt, M., and Crow, M. C.. "Enhancing Trust in Science and Democracy in an Age of Misinformation ." *Issues in Science and Technology* 39, no. 3 (Spring 2023): 18–20, [online] https://issues.org/trust-science-democracy-misinformation-mcnutt-crow/.

National Cyber Security Centre. (2023). Guidelines for secure AI system development. London: National Cyber Security Centre. https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

Qiao, L., and Wang, X. (2020). *Unrestricted Warfare: China's Master Plan To Destroy America*, Shadow Lawn Press, Lambertville [Kindle Edition].

Robb, J. (2007). *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken, NJ: John Wiley.

Sartonen, M., Huhtinen, A.-M., & Lehto, M. (2016). 'Rhizomatic Target Audiences of the Cyber Domain'. *Journal of Information Warfare*, 15 (4), 1-13.

Solal, A. and Bricmont, J. (1998), *Fashionable Nonsense: Postmodern Intellectuals' Abuse Of Science*, New York, Picador.

Stross, C. (2002), 'The Panopticon Singularity', *antipope.org*, [online], https://www.antipope.org/charlie/old/rant/panopticon-essay.html.

Stross, C. (2023). 'Same Bullshit, new Tin'. *Antipope.org*, 24 January, [online], https://www.antipope.org/charlie/blog-static/2024/01/same-bullshit-new-tin.html.

Tomlinson, J. (1995), 'Homogenisation and globalisation', *History of European Ideas*, 20:4-6, 891-897.

United Nations Joint Inspection Unit. (2021). 'Cybersecurity in the United Nations System Organizations'. Geneva: United Nations, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

UK Ministry of Defence. (2020). *Joint Concept Note 1/20: Multi-Domain Integration.* Shrivenham: Development, Concepts and Doctrine Centre.

US Department of Defense. (2022). *National Defense Strategy*. Washington, DC: Department of Defense.

Ware, W.H. (1967). 'Security and Privacy in Computer Systems', Presented at the Spring Joint Computer Conference, Atlantic City, April 17-19, 1967. Available at https://www.rand.org/pubs/papers/P3544.html.

Warrick, T.S. (2023). 'Regional cyber powers are banking on a wired future. Expanding the Abraham Accords to cybersecurity will help'. *Atlanticcouncil.org*. 19 May, {online], https://www.atlanticcouncil.org/blogs/menasource/cybersecurity-iran-abraham-accords-israel/.

Wiener, N. (1950). *The Human Use of Human Beings: Cybernetics and Society*. Boston: Houghton Mifflin.