2040: An Information Odyssey

Information operations (IO) has been experiencing something of a renaissance alongside the continuous evolution of the internet and social media. When compared with conventional warfare, IO based campaigns are cost effective, particularly suited to being delivered via proxies and activated long before the target realises an offensive against them has begun. No longer isolated to the theatre of war, modern IO campaigns embed themselves within civilian ecosystems and technological architecture to test the boundaries of national tolerance and response capabilities. Capitialising on the opportunities a noxious digital economy[1] creates, the West is experiencing a *fait au complet* as our adversaries destabilise societal norms and undermine trust in democratic institutions by using our information environment against us.

The future of IO is inextricably linked to the future of the global information environment. Conflicts and instability in the future are likely to arise from present day crises. These crises include the decay of democracy, climate change and resource scarcity. Artificial intelligence (AI) – and the race to AI dominance, will also play a part in shaping the information environment of the future. This essay will explore these emerging crises, the impacts they will have on the information environment and how they will shape NATO's IO challenges in 2040 and beyond.

THE MISINFOAPOCALYPSE

By the year 2040 NATO will have been in existence for nearly one hundred years. Witness to the rise and fall of regimes and nations; the end of communism in Europe and a century of relative stability and security in the North Atlantic region; the future relevance and existence of the Alliance depends on how it adapts to the degradation of our natural and information environments against the backdrop of a changing geopolitical situation that will see the rise of national powers traditionally outside the sphere of European security interests.

It must be acknowledged that we are starting this information environment odyssey from a maturing but inherently defensive hybrid warfare posture. Information environment researcher Alicia Wanless explains that "We now live in what information philosopher Luciano Floridi refers to as 'hyper history', where information community technologies (ICT's) and their data processing capabilities are the necessary condition for the maintenance and further development of societal welfare, personal

[1] Braun, Joshua A. Eklund, Jessica, L. (2019) Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes and the Business of Journalism. Journal of Digital Journalism 7: 1 pp 1-12.

well-being, as well as intellectual flourishing[2]." With the information environment now firmly embedded in all facets of our lives, it is difficult to envisage the hybrid warfare model we've become acclimatised to changing significantly. However, in looking forward through the next two decades, the developments that unfold in the lead up to 2040 will have cascading impacts on how IO practitioners are able to deliver offensive and defensive campaigns. Accepting that a rigid definition of peace and war existing as two separate states is in stark contrast to the single continuum of war[3] NATO's current and future adversaries operate in – particularly in modern political warfare, according to scholar Mike Caulfield we are at least three years past day zero in this misinfoapocalyspe[4] where "one group benefits: authoritarians (who) flourish when citizens become overwhelmed (by misinformation) and … give up on trying to figure out the truth[5]."

2040: WHAT WE KNOW SO FAR

Perhaps one of the most unexpected challenges of our time, and one of the biggest contributors to a fracturing information environment, has been the decay of democracy in the West. Researchers from the Varieties of Democracy Institute in their 2019 report observed that one-third of the world's population are impacted by autocratization, representing some 24 countries[6]. The study, noting that "democracy is still the most common type of regime," identifies that Greece, Hungary and Poland have made a full transition into electoral democracies, while other nations such as Lithuania and Slovakia remain on the verge of transition. Countries where democracy is in retreat include India, Turkey, Brazil, Poland, Russia and the United States. The 2020 Edelman Trust Barometer offers deeper insights with 66% of global respondents declaring they have no confidence in their country's current leaders, believing they will not be able to successfully address their country's challenges. Religious and Government leaders along with the very wealthy, are ranked as the least trusted cohorts of all - in favour of scientists, local citizens and community members[7].

---

[2] Wanless, Alicia (2018) We have a problem, but it isn't technology.

[3] Babbage, Ross (2019) The Return of Direct Defense in Europe: The Challenge to the Infrastructures of the Liberal Democratic Societies.

[4] According to Washington State University's Mike Caulfield (@Holden) in a since deleted tweet.

[5] McIlwain, Andy (2019) Our misinformation apocalypse.

[6] Autocratization as defined by the Varieties of Democracy Institute as "any substantial or significant worsening on the scale of liberal democracy in a country. It is a matter of degree and a phenomena that can occur both in democracies and autocracies. Thus autocratization is an umbrella term that covers both erosion in democratic countries (democratic backsliding), breakdown of democracy as well as worsening conditions in electoral authoritarian countries. Semantically, it signals the opposite of democratization, describing a move away from [full] democracy. Refer also page 14 of their 2019 report.

[7] Edelman Trust Barometer (2020) Global Report, pp. 17.

The resulting societal shift of this democratic decay will significantly impact the future information environment, particularly as populations rise in nations where regimes are undergoing autocratization or are already well established socialist republics. The global population is predicted to increase[8] to 9.7 billion people by 2050; and with a third of world's population undergoing autocratization today – geopolitics as we know is changing. We know from history that increasingly autocratic regimes stifle media independence and freedom of speech. In an increasingly autocratic information environment, the opportunities for IO practitioners to understand audiences and deliver effects behind the proverbial iron-curtain diminishes, while the rhetoric of the increasingly autocratic regime in-country strengthens.

Defining the geopolitical situation of the future in an unlikely dichotomy, the rise of two new global superpowers contrast the world's biggest democracy – India, with the world's biggest socialist communist republic - China. That these two nations are also the world's largest in terms of current and projected population growth should not go unnoticed, nor should the fact that democracy is in retreat in India. The UN predicts China's population to be 1.44 Billion in 2020, making it the largest country in the world, with India's population only slightly lower in a global ranking at 1.339 billion. By 2027 however, the UN predicts India will surpass China as the world's most populous country. Concurrently by 2050 the UN expects an exponential population growth in regions such as sub-Saharan Africa (99% increase) which together with India, Nigeria, Pakistan, the Democratic Republic of the Congo, Ethiopia, the United Republic of Tanzania, Indonesia, Egypt and the United States of America - will represent more than half of the world's projected population growth. In stark contrast, NATO nations have a predicted population growth of just 2% over the same time period.

The consumer information technology market will adapt to serve these key new markets with access to the internet predicted to result in 90% of the world's population connected by 2030. However, with China and India already ranking first and second in the population connectivity stakes, the future impact on the information environment and ability for IO practitioners to create, deliver and measure effects amongst these audiences is likely to be significant diminished given both countries are already taking steps to future proof their populations. China's implementation of a 'social credit system' will have far reaching consequences not only for its citizens, but potentially for the sovereignty of other nations. China's "use of big-data collection and analysis to monitor, shape and rate behaviour via economic and social processes[9]"are directly linked with their Government's Artificial Intelligence Development Plan. While the convergence of big data and surveillance isn't new, that the Chinese Government intend to use the system to manage their citizens' rights,

[8] The current global population in 2020 is estimated to be 7.8 billion people.

[9] Hoffman, Samantha (2017) 'What is Social Credit?' Special Report for the Australian Strategic Policy Institute.

movements and opportunities goes well beyond social governance and social management[10]. Businesses and companies will also be subject to the same system, with evidence already seen of Chinese Government over-reach into the affairs of other nations in disputes about listing Taiwan, Hong Kong and Macau as part of China[11] [12].

NATO IO practitioners should also take close note of China's 'The Belt and Road Initiative' (BRI), which signals their intention to be far more engaged in future global affairs. The BRI policy goals are broadly focused around information connectivity by:

- Improving intergovernmental communication to better align high-level government policies like economic development strategies and plans for regional cooperation
- Strengthening the coordination of infrastructure plans to better connect hard infrastructure networks like transportation systems and power grids
- Encouraging the development of soft infrastructure such as the signing of trade deals, aligning of regulatory standards and improving financial integration; and
- Bolstering people-to-people connections but cultivating student, expert and cultural exchanges and tourism[13].

Of the 138 countries to have already signed up for the BRI, among them are Nigeria, Pakistan, the Democratic Republic of the Congo, Ethiopia, the United Republic of Tanzania, Indonesia and Egypt - the very same countries predicted by the UN to experience significant population growth in the coming decades. This cannot be viewed as coincidental. IO practitioners must appreciate the magnitude of China's BRI push into the totality of the information and sensing environments, in nations where population growth is predicted to rise significantly because with that growth comes the opportunity to influence their information environments beyond IO into ICT and sense-making infrastructure.

Changing Foreign Information Eco-Systems

The similarities between the Chinese BRI and the military DIME (FIL)[14] model is clear, with significant soft power projection options factored into diplomatic, economic and financial engagement. China's

[10] Hoffman, Samantha (2017) Managing the State: Social Credit, Surveillance and the CCP's Plan for China.

[11] Rogin, Josh (2018) White House calls China's threats to airlines 'Orwellian nonsense.'

[12] Palmer et al (2018) China Threatens U.S. Airlines over Taiwan References.

[13] Center for Strategic and International studies (2019) How will the Belt and Road Initiative advance China's interests?

[14] DIME (FIL): a military acronym meaning Diplomatic, Informational, Military, Economic and Financial, Intelligence and Law. DIME (FIL)

controversial technology multi-national enterprise Huawei – also known as "China's BRI eyes and ears[15]," is seen as a risky prospect by many nations due to the relationship between the company and the Chinese Government. The Australian Strategic Policy Institute's Danielle Cave notes that "a range of risks of working with Huawei are already on the record, from allegations of systematic intellectual property theft and dubious ethics to allegations of sensitive data theft that have occurred under the company's watch." Cave further points out that "governments also need to ensure they analyse, and fully understand, the laws that govern a company's home environment … particularly critical when such laws mean a foreign government can exert extrajudicial direction[16]." The United Kingdom's decision to allow Huawei limited access into its 5G network in early 2020 has already sparked diplomatic tension with Australia and is likely to lead to reduced intelligence sharing cooperation amongst its Five Eyes allies. The United States believes Huawei poses a national security risk and has blacklisted the company from doing business with US based companies.

If China's social credit system, BRI and approach more broadly to cyber via Huawei (as a vehicle) aren't enough, the People's Liberation Army's (PLA) goal is to "build China's first-mover advantage in artificial intelligence development, (to) accelerate the construction of innovation countries and (harness) the world's science and technology power[17]." According to Elsa Kania, China's quest to "become a science and technology superpower" has been influenced thus far via observation of the United States' military capabilities. The PLA anticipates " that the advent of AI could fundamentally change the character of warfare, resulting in a transformation from today's informatised ways of warfare to future intelligenised warfare – in which AI will be critical to military power.[18]" With China speculated to beat the United States to AI supremacy[19] - and the EU taking a more measured approach aiming to regulate and control AI (whether Chinese owned or not), the national security implications of the militarisation of AI is far reaching. From drones to robots, facial recognition software to advanced cyber capabilities – through China's BRI and rollout of Huawei, its ability to harness the data of future populations around the world puts it in a uniquely influential IO position.

China is not alone in moving towards a more authoritarian information and cyber posture. In 2018 India's Government took steps to give itself the ability to censor the world-wide-web in a move to gain control over content that they deem to be "libellous, invasive of privacy, hateful or deceptive."

---

[15] Rust, Bob (2019) Huawei is the eyes and ears of China's Belt and Road Initiative.

[16] Cave, Danielle (2019) Australia and the great Huawei debate: risks, transparency and trust. The Australian Strategic Policy Institute.

[17] CPC Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan. Translated by the Foundation for Law and International Affairs.

[18] Kania, Elsa (2017) Battlefield Singularity. Artificial Intelligence, Military Revolution and China's Future Military Power.

[19] Allison, Graham (2019) Is China Beating America to AI Supremacy?

This control would extend to social media companies, with Indian internet service providers required to build censorship software to block citizens from seeing such content. The draft guidelines also seek to impose additional rules on how big-tech firms can use the personal data of Indian users; and to combat the threat encrypted messaging services posed to national interests. China already has similar levels of control over its populations information sources, with most Western social media networks and search engines blocked in favour of State approved alternatives.

Closer to the Alliance, Russia's so called 'Sovereign Internet Law' - a series of amendments to existing laws that were introduced in 2019, aims for the "centralised state management of the internet within Russian Borders." In a report for the German Council on Foreign Relations published this year, author Alena Epifanova outlines Russia's three key goals in "protecting the internet within Russia from external threats:" (1) The creation of an internet surveillance apparatus that "counteracts threats" while allowing for ubiquitous control of information; (2) the Government becoming the ultimate regulator of the internet inside its borders; and (3) International expansion of this infrastructure to create a distinctly separate Russian segment of the world wide web. Epifanova explains that "Russia is not seeking to isolate itself from the rest of the world, but rather create a precedent which other states aspiring to sovereignty over their 'segments' of the internet could follow" and that Russia will likely build its relations with China to achieve this objective[20]. Other countries that temporarily 'shut down' or 'cut off' their citizens from the global internet in 2019 alone included: Bangladesh, The Democratic Republic of Congo, Egypt, India, Indonesia, Iran, Iraq, Sudan, Myanmar and Zimbabwe. Beyond obvious shut downs, some Governments have taken to throttling internet speeds or blocking specific content, social media networks or messaging apps in a bid to control their information environment, particularly during times of political unrest or civil unrest. Countries that segment themselves from the broader internet will reduce the ability of foreign nations to conduct IO on their populations while concurrently bolstering their own, domestically focused, influence.

NATO's understanding of the growing partnership between Russia and China warrants dedicated analysis and resourcing now and into the future. Professor Paul Dibb explains that it has become increasingly clear that "China and Russia want to shape the world consistent with their authoritarian model" and that they are both "well versed in using these sorts of *grey-zone*[21] operations[22]." Dibb's

---

[20] Epifanova, Alena (2020) Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet. German Council on Foreign Relations.

[21] Grey-Zone operations as defined in the Australian Strategic Policy Institute Special Report: 'How the geopolitical partnership between China and Russia threatens the West.' as: "totalitarian powers unrestrained by rules are willing to use information campaigns, cyber operations, thefts of intellectual property, coercion and propaganda to weaken Western democracies."

[22] Dibb, Paul (2019) Australian Strategic Policy Institute Special Report: 'How the geopolitical partnership between China and Russia threatens the West.'

report goes on to remark that China and Russia's alliance is in part due to the fact that they share a common enemy in the United States of America. Dibb further contends that the United States' does not have the capability to fight two conflicts concurrently. For its part, Russia could alter its posture if an opportunity such as China's engagement of the United States in the Asia-Pacific theatre presented itself, leveraging the knowledge that the United States' absence in a NATO led coalition would allow it "to secure full control of its western non-NATO member states."

With both China and Russia already having proven their proactive willingness to fight in the information environment – across the IO spectrum including practices seen as unethical and immoral by Western standards, together with a closing proverbial information iron curtain around China's BRI participant nations and Russia's intention to protect itself in its own segment of the internet – the ability for opposing forces to penetrate into these fortified information environments circa 2040 will be limited at best. Foreshadowing these kinds of future challenges, Australia's Chief of the Defence Force Major General Angus Campbell in a 2019 speech recognised that regimes that operate well in 'grey zones' have a broader concept of war and are "better able to harness political warfare in a more controlled way than the West." Quoting Leon Trotsky, Major General Campbell aptly noted of the nature of wars to come "You may not be interested in war… but war is interested in you[23]."

Non-Traditional threats: Climate Change and Resource Scarcity

The impact non-traditional threats will have on and for the NATO IO environment of the future cannot be underestimated. The cascading impacts climate change and resource scarcity will have on destabilising the future information environment will converge in a parallel timeline with global population growth, the rise of nations with potentially competing interests in China, India and African nations; and the increasing autocratization of Western liberal democracies. NATO has previously not focused on China, India and Africa beyond tackling ad-hoc security challenges in Africa and discussions on the security implications of China's rise and therefore have limited understanding of the span of control ICTs in those geographies have or will continue to have into the future.

The Intergovernmental Panel on Climate Change[24] reported in 2018 that by 2040 "worsening food shortages, wildfires and a mass die-off of coral reefs" will occur. The impacts will be far reaching – inundating coastlines and intensifying droughts will cost the global economy an estimated $54 trillion in damage, with this figure rising to $69 trillion if the temperature rose higher still." This will result in

[23] Campbell, Angus – Major General, Chief of the Australian Defence Force (2019) Australian Strategic Policy Institute International Conference 'War in 2025' Keynote Speech.

[24] The Intergovernmental Panel on Climate Change (IPCC) consists of a group of scientists 91 scientists from 40 countries convened by the United Nations to guide world leaders. This group analysed more than 6,000 scientific studies in coming to their conclusions.

a "disproportionately rapid evacuation of people from the tropics;" and mass migration of climate-refugees[25]. Migration is already a political and societal flashpoint for many NATO nations with "Europe facing the greatest refugee and migrant crisis since the end of the Second World War." The current migration crisis "caused by conflict and instability on NATO's southern borders[26]" is resulting in a resurgence of right-wing and populist politics that base their platforms on a frustration with "globalisation, immigration and a dilution of national identity and European Values.[27]" These are all issues that will only intensify in the lead up to 2040.

Bulgarian political scientist Ivan Krastev, in his 2018 assessment of Eastern European populism wrote that their intentions are focused "not to the existence of democracy at the level of the nation – but to the cohesion of the EU. As more countries in the region turn toward illiberalism, they will continue to come into conflict with Brussels and probe the limits of the EU's power… Eventually the risk is that the EU could disintegrate and Europe could become a contingent divided and unfree[28]." While NATO existed well before the EU and could reasonably be expected to exist should the EU disintegrate, the degradation of inter-country relations would at the very least present unique administrative and cooperation conflicts, diminishing IO capabilities and prospectively turning a current ally into a future target audience.

There can be no doubt that migration will be used as a trigger for conflict into the future with the UN human rights committee recently ruling it is unlawful for Governments to return people to countries where their lives might be put at risk by climate change[29]. There is no place more evident of race politics and social division than online, where social and digital media are routinely manipulated to fuel outrage via IO campaigns backed by both nation state and non-state actors. The role of the information environment in both fuelling attacks via the promulgation of anti-migrant sentiment while concurrently creating safe spaces for terrorists to commune online is undeniable. The resurgence of right-wing terrorism committed by lone actors and ethno-nationalists has "risen 320%

[25] New York Times (2018) Major Climate Report Describes a Strong Risk of Crisis as Early as 2040.

[26] NATO (2019) Assistance for the refugee and migrant crisis in the Aegean Sea.

[27] BBC (2019) Europe and right-wing nationalism: A country by country guide.

[28] Krastev, Ivan (2018) Eastern Europe's Illiberation Revolution: The Long Road to Democratic Decline. Foreign Affairs May/June 2019 issue pp. 49-56.

[29] United Nations (2020) CCPR/C/127/D/2728/2016 Citing the case of a resident of Kiribati, the UN notes that "relating to conditions on Tarwa (Kiribati) at the time of the individuals removal do not concern a hypothetical future harm but a real predicament caused by lack of portable water and employment possibilities, and a threat of serious violence caused by land disputes… due to the impact of climate change and associated sea level rise on the habitability of the nation and on the security situation on the islands the individual is a real risk of impairment to his right to life.

in the past five years[30]" alone with anti-migration reasoning a central theme in many attacker manifestos.

Regional turmoil, particularly around resource scarcity, is another area of concern for NATO and it's future IO practitioners. The World Resources Institute predicts further regional volatility as nations such as Bahrain, Kuwait, Palestine, Qatar, the United Arab Emirates, Israel, Saudi Arabia, Oman and Lebanon deal with extreme water scarcity. "With regional violence and political turmoil commanding global attention, water may seem tangential however we have already seen how water shortages in Syria likely contributed to the 2011 unrest that contributed to the civil war[31]." Concurrently, oil dependant nations, many of which are categorised as water-stressed, will concurrently be facing economic pressures as oil production slows down. Seth Blumsack, Assistant Professor of Energy Policy at Pennsylvania State University explains that "the reality is not that we are running out of oil, but rather that we are transitioning from a period of easily-accessible oil at lower prices to an era of increasingly unconventional production which has higher costs. Companies will not try to develop these unconventional resources unless consumers are willing to pay the (economic and environmental) price … at some point, unconventional oil exploration will get so expensive consumers will look to low-cost alternatives.[32]" Long time Saudi Oil Minister and key founder of OPEC Sheik Ahmed Zahi Yamani sums up this change as "the stone age came to an end, not for lack of stones, and the oil age will end, but not for lack of oil."

2040: THE PROXY WARS

The concurrent convergence of political, technological, informational, environmental and economic crises has the potential to manifest global instability, insecurity and conflict on a scale never seen before. If we take a Clausewtizian view of what an all-domains environment may look like by acknowledging war in theory limits of our current knowledge in favour of a war in reality approach, we can understand the conflicts of 2040 to be non-conventional, frequently interrupted, highly asymmetrical and strategically poised.

We have already seen the beginning of non-conventional informational warfare being played out in world politics. The Russian active measures campaign into the 2016 United States' Presidential election, while not surprising, highlighted the seismic shift possible in IO effect generation via social and online media. Terrorist organisations such as ISIS have similarly weaponised social media to

[30] Global Terrorism Index 2019.

[31] World Resource Institute (2015) Ranking the World's Most Water-Stressed Countries in 2040.

[32] Blumsack, Seth (unk) Are we running out of oil?

conduct broad scale IO campaigns against both the near and far enemy. Cambridge Analytica's links to firms involved in the Brexit campaign highlighted the influence proxies for hire can generate. The resulting effects have put the world in a more congested and contested information environment than ever before, hacking human cognition to capitalise on the effects of negativity and confirmation biases whilst simultaneously activating the reward centre of audience neurophysiology to generate in-group conformity. In what is assumed to be a symmetrical battlespace, Russia, ISIS and Cambridge Analytica have proven that this is not the case. The difference is not in the funding, technical capability or resources needed to wage such an IO campaign, but in the nation's will to fight on a battlefield that is inherently unethical and at its core, damaging to social cohesion, democracy and peace.

NATO will need to reinvent itself to remain relevant into the future. This means the Alliance must reconceptualise what it's future strategic purpose is and what benefits it delivers to its members. While this won't be the first time NATO has had to reimagine itself to remain relevant in dynamic geopolitical times[33], it will be the first time non-security based global events converge to present multiple destabilising forces of scale concurrently. Notwithstanding the possibility that individual nations (both in and outside of the Alliance) may take a military approach to managing the challenges presented by climate change, exponential population growth, democratic decay and resource scarcity - the contest of ideas around these predictions has already begun.

The 2040 NATO Operation: Through the Looking-Glass

2040 is likely to be a time of intense, prolonged crisis for the world. Population growth in areas experiencing resource scarcity and/or climate change will drive people towards cities in their own, or other, nations creating large waves of migration on almost every continent. Conflict over those same limited resources is likely to displace even more people in geographies where human habitability is in sharp decline. Populists will view this through the lens of migration 'invasion' and leverage events to ignite and fuel ethno-nationalist conflicts, creating insecurity in already strained democratic nations. For these reasons, NATO must rapidly expand its threat lexicon to include the identification of global challenges that are likely to trigger security-based conflicts long before battlelines are drawn. This expansion must look beyond direct impacts to member States and consider the broader geopolitical and environmental costs of inaction. Most importantly, NATO cannot lose the ability to project soft

[33] From NATO's 1995 intervention in the former Yugoslavia as a multinational implementation force (IFOR) under a UN mandate to implement the Bosnian peace agreement; to 2003 when NATO took command of the UN peacekeeping force in Kabul, Afghanistan – in its first operations outside of Europe; to a realignment of strategic focus in 2010 that sought to "cut costs while prioritising defence against new and emerging threats, such as cyber attacks" while missile defence systems were deployed to cover the territory of all its European members; to 2014, when Russia annexed Crimea from the Ukraine."The idea of collective defence" Secretary-General Jens Stoltenberg was quoted as saying in 2019 "has become more important given how Russia is using force to change borders in Europe".

power and influence into regions of future instability and conflict, particularly as informational structures in those terrains constrict and become hardened against foreign influence.

The 2040 NATO operation will involve significant focus on humanitarian issues and the resulting insecurity internal ethno-nationalists will create.

IO in 2040 must contend with a constrained and hardened information environment across the majority of the world's population. China's BRI and rollout of Huawei is will impact NATO's ability to project soft power and influence at-will globally. This includes in areas of conflict where it will be virtually impossible to create operationally desirable conditions pre-deployment or even during deployments without the pre-emptive degradation of the target nation's information architecture. Even then, sudden informational change may not induce the intended effects in the target population due to resulting in-group cognitive dissonance. It must be recognised that in the conflicts of the future, IO practitioners will need to grapple with target populations that have been subject to ongoing domestic influence campaigns by their Governments for *at least* two decades. This is likely to leave in-group audiences fearful of or outright hostile toward foreign information and nations.

This will necessitate a change in IO analysis, with the cognitive component of the aggregate information environment taking primacy over the currently favoured physical and informational dimensions. With the information environment of potential target nations of the future, akin to for conceptual example present day North Korea, the ability of NATO to conduct information environment analyses in order to construct IO campaigns will be limited to opportunities created by successful cyber infiltration operations or physical surveillance activities. Further, IO campaigns delivering efforts to influence adversary decision making will almost certainly need to be deployed via those same cyber conduits or military deception operations. Measurement of effects will be confined to observations gathered via surveillance of physical actions or cyber capabilities.

The shift to cognitive primacy in IO design and deployment will arise as a result of the conditioning targets will have undergone over the long term. Using North Korea again as an example, if NATO were to intervene in the present day to liberate its people, would North Koreans embrace NATO forces? Or would they retaliate against a Western invading power fulfilling the 'Western invasion prophecy' they have been indoctrinated in over successive generations?
The longer NATO is absent from the affairs of State and indeed the public consciousness of nations on the cusp of informational segmentation, the harder it will be to deradicalise entire populations at-will in times of conflict (if this is even at all achievable). IO campaigns that focus on building resilience and providing contextual sense making in target populations will therefore be essential to normalising the overall comprehension of current or forthcoming events and the development of independent critical thinking.

It is for these reasons that the IO practitioner of the future must not only work closely with Psychological Operations (PSYOP) and Cyber warfare units; but develop a robust understanding of contemporary cultural psychology as well as the ability to operationalise behavioural economics choice architecture frameworks, that provide familiar structures for the delivery of heuristically laden, sense making IO payloads. Further, these IO payloads must be able to be delivered outside of and in parallel to social networking and online media in a multi-spectral approach that creates or changes perceptions enough to cultivate independent critical thinking while stopping just short of inducing cognitive dissonance. Just as war is a contest of wills, in many respects so too is the battle for perceptions and worldviews. IO practitioners must develop an appreciation of future populations as internally homogenous but externally fragile to avoid hostile reactions to IO campaigns.

Conversely, NATO can expect its current and future adversaries to continue to innovate and wage sophisticated IO campaigns designed to undermine the Alliance, it's members and its operations. Building and resourcing the capability of IO practitioners to detect, deflect and/or defeat such attacks – not only on military targets but also in the civilian and political environments, must be a priority. Shining light on foreign interference has done little to dissuade current noxious actors from their agendas. Further research must be conducted to ascertain the strategic weaknesses this new operating environment presents for exploitation across IO, PSYOP, Cyber warfare and old-school propaganda platforms. Defensive inoculation of populations – such as has occurred in Finland, present valid, generational counter measures to foreign interference which can be more broadly adopted.

NATO's goals of peace, stability and security have never been more relevant.

NATO must decide if it is for its members only – or for a geographically broader alliance of like-minded nations invested in global stability and security. The question is no longer if climate change, resource scarcity and growing populism will impact NATO's future, but when – and what impacts that will have on global peace, stability and security.

The ability for NATO to operate in silo of broader global events without creating cascading impacts for itself, its members, allies and other nations will be severely constrained by 2040. Mission creep over the next two decades will force NATO to face the challenges associated with making decisions in multi-consequential environments. Changes in the information environment that impact NATO's operations may become irrevocable if action isn't taken soon to counter the threat autocratic regimes will have on the accessibility of the internet.

NATO must develop a deep understanding of China's BRI, social credit system and Huawei networks. How will those informational ecosystems open up or close off growing populations to global voices? What impact will India and Russia's plans to segment their citizens from the broader internet have on NATO's ability to develop and deepen bilateral relations with the largest populations and economies in the future world? How will China and Russia's growing cooperative partnership change the way information wars are fought, won or lost?

In perhaps the most challenging aspect of future IO, NATO must find it's ethical comfort zone to enable it to navigate up to measures short of war in the IO environment. The will to fight, meaningfully with intent, in the information environment must be fully appreciated by leaders as a critical element of the Alliance's overall defensive capability. Building the IO capability of the future – with the dexterity to remain dynamic across the political, economic, environmental and security areas of operation - is most certainly a multi-disciplinary generational prospect spanning both the technological and physical environments.

NATO may not be particularly inclined towards information warfare, but information warfare has long been interested in NATO.

--- ENDS
4978 words excluding footnotes and references.

REFERENCES

ABC News Australia (2020) British Government grants Huawei a limited role in 5G network, defying warnings from US.

Allison, Graham (2019) Is China Beating America to AI Supremacy? The Center for the National Interest.

Babbage, Ross (2019) The Return of Direct Defense in Europe: The Challenge to the Infrastructures of the Liberal Democratic Societies.

BBC (2019) Europe and right-wing nationalism: A country-by-country guide.

BBC (2019) What is defence alliance NATO?

Blumsack, Seth (unk) Are we running out of oil? Subject Syllabus for EME 801 Energy Markets, Policy and Regulation. Penn State University Department of Energy and Mineral Engineering.

Braun, Joshua A. Eklund, Jessica, L. (2019) Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes and the Business of Journalism. Journal of Digital Journalism 7: 1 pp 1-12.

Campbell, Angus (2019) 'War in 2025.' Keynote Speech. Australian Strategic Policy Institute International Conference 2019.

Caulfield, Mike (2020) @Holden Tweet 27 January 2020 (since deleted but archived here).

Cave, Danielle (2019) Australia and the great Huawei debate: risks, transparency and trust. The Australian Strategic Policy Institute.

Center for Strategic and International studies (2019) How will the Belt and Road Initiative advance China's interests?

China Trade Research (2020) The Belt and Road Initiative: Country Profiles.

Chinese Government (2017) CPC Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan. Translated by the Foundation for Law and International Affairs.

Davenport, Carole (2018) Major Climate Report Describes a Strong Risk of Crisis as Early as 2040. The New York Times.

Dibb, Paul (2019) 'How the geopolitical partnership between China and Russia threatens the West.' Australian Strategic Policy Institute Special Report.

Edeleman (2020) Edelman Trust Barometer 2020, Global Report p.17.

Epifanova, Alena (2020) Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet. German Council on Foreign Relations.

Goel, Vindu (2019) India Proposes Chinese-Style Internet Censorship. The New York Times.

Greene, Andrew (2020) Intelligence committee cancels UK visit amid diplomatic tensions over Huawei policy leak. ABC news Australia.

Hoffman, Samantha (2017) Social Credit: Technology-Enhanced Authoritarian Control with Global Consequences. Policy Brief for the Australian Strategic Policy Institute.

Hoffman, Samantha (2017) 'What is Social Credit?' Special Report for the Australian Strategic Policy Institute.

Indian Government (2018) Comments invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018. Ministry of Electronics and Information Technology.

Institute for Economics and Peace (2019) Global Terrorism Index 2019: Measuring the Impact of Terrorism.

Kania, Elsa (2017) Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power. Center for a New American Security.

Keane, Sean (2020) Huawei ban: Full timeline as Google warns against sideloading its apps on P40 phones. CNet.

Krastev, Ivan (2018) Eastern Europe's Illiberation Revolution: The Long Road to Democratic Decline. Foreign Affairs May/June 2019 issue pp. 49-56.

Kumar, Akshaya (2019) Shutting Down the Internet to Shut Up Critics. Human Rights Watch.

Laird, Robbin (2019) The Return of Direct Defense in Europe: The Challenge to the Infrastructures of the Liberal Democratic Societies.

Lake, Eli (2019) Finland's Plan to Prevent Russian Aggression. Bloomberg.

Maddocks, Andrew et al (2015) Ranking the World's Most Water-Stressed Countries in 2040. World Resources Institute.

McIlwain, Andy (2019) Our misinformation apocalypse.

Morgan, Steve (2019) Humans on the Internet will Triple from 2015 to 2022 and hit 6 Billion. CyberCrime Magazine.

NATO (2019) Assistance for the refugee and migrant crisis.

NATO (2019) Cooperation with the African Union.

NATO (2019) London Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019.

New, Ash (2019) Brexit: The Uncivil War showed us how the EU Referendum was won with Data Science. Towards Data Science.

Palmer et al (2018) China Threatens U.S. Airlines over Taiwan References. Foreign Policy.

Rogin, Josh (2018) White House calls China's threats to airlines 'Orwellian nonsense.' The Washington Post.

Rust, Bob (2019) Huawei is the eyes and ears of China's Belt and Road Initiative. Trade Winds News.

United Nations (2019) Special Report: Global Warming of 1.5°C. Intergovernmental Panel on Climate Change.

United Nations (2020) Views Adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 2728. UN Treaty Database.

United Nations (2019) World Population Prospects 2019: Highlights.

/2016.

United States of America (2019) Unclassified Report of the Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 2 Russia's use of Social Media with additional views.

V-Dem Institute (2019) Democracy Facing Global Challenges, V-Dem Annual Democracy Report 2019.

Wanless, Alicia (2019) We have a problem, but it isn't technology.