

Volume 13 | Autumn 2023

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence

All Washed Over by Machines of Loving Grace

Speaking in Riddles on Trisolaris:
Communicating Liberal Democracy to the Disillusioned

The Institutional Branding of Jowett and O'Donnell's
Propaganda and Persuasion (1986–2019)

Cracking the Nut in Iraq

Deterrence and Disinformation: Communicating Deterrence
in a Non-Linear Media Environment

Cybersecurity in Political Studies:
A Scoping Review

Volume 13 | Autumn 2023

DEFENCE STRATEGIC COMMUNICATIONS

**The official journal of the
NATO Strategic Communications Centre of Excellence**

ISSN 2500-9486 (online)
ISSN 2500-9478 (print)
DOI 10.30966/2018.RIGA.13
Defence Strategic Communications

Editor-in-Chief

Dr. Neville Bolt

Production Team

Jānis Karlsbergs (project management)
Merle Anne Read (copy edit)
Una Grants (design)

Editorial Board

Professor Chiyuki Aoi
Professor Malik Dahlan
Professor Mervyn Frost
Professor Nicholas O'Shaughnessy
Professor Nancy Snow
Dr. Gatis Krūmiņš
Dr. Domitilla Sagramoso
Dr. Vera Michlin-Shapir
Dr. Solvita Denisa-Liepniece
Dr. Tiko Tsomaia
Dr. Leonie Haiden
Dr. Jente Althuis
Mr. James Farwell

Defence Strategic Communications is an international peer-reviewed academic journal. The journal is a project of the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). It is produced for scholars, policy makers, and practitioners around the world.

© All rights reserved by the NATO StratCom COE. The journal and articles may not be copied, reproduced, distributed or publicly displayed without reference to the NATO StratCom COE. The views expressed here are solely those of the author in his private capacity and do not in any way represent the views of NATO StratCom COE. NATO StratCom COE does not take responsibility for the views of authors expressed in their articles.

NATO Strategic Communications Centre of Excellence
Riga, Kalnciema iela 11b, Latvia, LV1048, www.stratcomcoe.org

Contents

Foreword

Neville Bolt..... 5

All Washed Over by Machines of Loving Grace

A Review Essay by Charles Kriel 13

Speaking in Riddles on Trisolaris:

Communicating Liberal Democracy to the Disillusioned

A Review Essay by Maria Golubeva..... 39

The Institutional Branding of Jowett and O'Donnell's Propaganda and Persuasion (1986–2019)

A Review Essay by Nancy Snow 51

Cracking the Nut in Iraq

A Review Essay by Paul Bell..... 71

Deterrence and Disinformation:

Communicating Deterrence in a Non-Linear Media Environment

Nicole Jackson..... 95

Cybersecurity in Political Studies: A Scoping Review

Aybars Tuncdogan..... 131

Foreword

It is a truth universally acknowledged that a utopia is not a dystopia, but that the pursuit of the first can lead to the realisation of the other. While a utopia is little more than an everywhere-but-nowhere dream, dystopias have been all too manifest in our history on this planet. As one old year elides into a new, the skies over 2024 risk growing even darker than during those recent months when geopolitics witnessed the growing triangulation of three global crises—Ukraine, Israel–Gaza, and Taiwan—exploited as proxies and direct theatres of engagement between competing ideologies. Increasingly, democrats claim their democracies to be under attack from a concerted authoritarianism pursued from both inside and outside their countries. Yet their pleas for support, argued in the language of an existential struggle, have frequently fallen on deaf ears.

Dystopias commonly haunt the pages of science fiction and fantasy novels, consigning human suffering to the imaginary. Yet for millions of people in our world it forms the very fabric of their lived lives. Often it is better to look away from news reports when trying to gauge the mindset of populations, either hidden from view or fleetingly highlighted at times of emergency or crisis. The convergence of old and new paradigms staring out from our screens seems to defy easy understanding: trench warfare of attrition resonant of a century ago is accompanied by the sophistication of costly long-range missiles and the cut-price tech of armed drones (Ukraine); insurgents in tunnel complexes underground are countered by combatant mechanised divisions searching and destroying above (Gaza); while oil-rich producer nations chair international conferences aimed at weaning the world off its addiction to fossil fuel energy supplies (COP28, Dubai).

At the heart of our confusion, as we approach the second quarter of the twenty-first century, is the lingering failure to identify a metaphor that can make sense of these cross-currents and apparent contradictions. One that can squeeze a host of opposites counterintuitively into a common-sense framework of understanding. Perhaps an easy guide to translate the complexity of our times to a thumbnail sketch, a shorthand as effective as ‘containment’ or ‘Cold War’ once was. But then those were times of bipolarity not multipolarity in world politics. Today we face not only multipolarity but multi-alignment—where states are tempted to shop around for their security with the United States, for their energy supplies with Russia, and for their markets with China.

One useful tip is to scan the book bestseller lists in leading newspapers. These offer an insight into which titles have prised consumers’ hard-earned pennies from their pockets, offering answers to a growing confusion of events and voices that promise to clear the fog—sometimes with rich insight, sometimes with the sweet talk of snake-oil salesmen. Take the *New York Times* bestsellers of 2023. Standout titles in non-fiction include the musical artist Britney Spears’s *The Woman in Me* confiding ‘lying quietly on those rocks, I felt God’, a *cri de cœur* accompaniment to a troubled upbringing and rags-to-riches story. ‘I wanted to live inside my dreams, my wonderful fictitious world, and never think about reality.’¹ What she actually came to feel was the oppressive hand of a psychiatric regime and legal system that awarded her father conservatorship, in other words state-sanctioned control, over her adult life and musical career. Meanwhile an alternative reality was on trial, or near to it. *Oath and Honor: A Memoir and a Warning* presents the ethical challenge to President Donald Trump by former congresswoman Liz Cheney of Wyoming that argued for his impeachment: ‘We were in dangerous territory. The president and his legal team were making outlandish and false claims that struck at the heart of our electoral process. Millions of Americans believed them.’² Meantime *American Prometheus* (now a major motion picture) charts the moral dilemma of nuclear physicist Robert

1 Britney Spears, *The Woman in Me* (Gallery Books, 2023), prologue and chapter 1.

2 Liz Cheney, *Oath and Honor: A Memoir and a Warning* (Little Brown and Company, 2023).

Oppenheimer as he travels ‘from obscurity to prominence’ on his way to developing the hydrogen bomb that would be deployed in the tragedies of Hiroshima and Nagasaki. Its authors write: ‘Oppenheimer tried valiantly to divert us from that bomb culture by containing the nuclear threat he had helped set loose.’ And as if that weren’t sufficiently portentous, ‘Cold War politics at home and abroad, however, doomed the plan, and America, along with a growing list of other nations, embraced the bomb for the next half century.’ You guessed right; there was worse to come: ‘but in another twist, the threat of nuclear war and nuclear terrorism is probably more imminent in the twenty-first century than ever before.’³

These are not times for the faint-hearted. A gnawing desire to come to grips with ethical self-questioning and personal responsibility feeds today’s curiosity. Yet while writers of non-fiction attach important questions to the inner struggles of celebrity figures, our novelists are drawn to the subcutaneous while touching the pulse of nations through suggestion rather than articulation. Two new novels stand out in this respect. Both tackle societies-turned-dystopias while speaking to the contemporary world.

The Irish author Paul Lynch has just won the prestigious Booker Prize 2023 for his *Prophet Song*. The novel paints the picture of an Ireland today fallen under the spell of an authoritarian regime. Familiar tropes of creeping autocracy, retreat of civil liberties, the late-night knock on the door, martial law and curfews, families torn apart, aerial bombing of civilian populations, and displaced thousands at the mercy of people-smuggling gangs and militias. Not to mention the infecting of insurgent forces with the same dark desire to control humanity. Unfamiliar setting—the Republic of Ireland? Perhaps. Until, that is, late November 2023 when shocked Irish police chiefs—real life not fictional—accused far right and anti-migrant groups of stirring up unprecedented outbursts of violence on the streets of Dublin.⁴ We are led to conclude that our

3 Kai Bird and Martin J. Sherwin, *American Prometheus: The Triumph and Tragedy of J. Robert Oppenheimer* (Vintage Books/Random House, 2006), pp. xii–xiii.

4 Conor Lally et al., ‘Dublin Riots: Violent Clashes with Gardai and Vehicles Set Alight after Children Injured in Knife Attack’, *Irish Times*, 23 November 2023.

societies are fragile constructs held together by consensus. Paul Lynch's characters agree:

we belong to a tradition but tradition is nothing more than what everyone can agree on—the scientists, the teachers, the institutions, if you change ownership of the institutions then you change ownership of the facts, you can alter the structure of belief, what is agreed upon, that is what they are doing, Eilish, it is really quite simple, the NAP is trying to change what you and I call reality, they want to muddy it like water, if you say one thing is another thing and you say it enough times, then it must be so, and if you keep saying it over and over people accept it as true—this is an old idea.⁵

An old idea, maybe. But no less menacing for George Orwell as he described it in his novel *Nineteen Eighty-Four*, first published in 1948. Recently, Sandra Newman has offered a new take on Orwell's dystopia. In *Julia* she reimagines *Nineteen Eighty-Four*, telling the story from the point of view of the female protagonist in the doomed romantic tryst between Orwell's Julia Worthing and Winston Smith, investing her with a new agency not present in the original. Dystopia is a rich seam to mine. Other notable contributions to the genre have included Yevgeny Zamyatin's *We* (1921), Franz Kafka's *The Trial* (1925), Aldous Huxley's *Brave New World* (1932), Ray Bradbury's *Fahrenheit 451* (1953), Margaret Atwood's *Handmaid's Tale* (1985), and more recently Suzanne Collins's trilogy—*The Hunger Games*, *Catching Fire*, *Mockingjay* (2008, 2009, 2010). What characterises many of these is the construction of an alternative political reality where the very nature of truth is called into question amid a new disorientation and where freedom of speech, if not thought, falls victim to the forces of oppression. Again these texts serve as reminders of the primacy of free thought and free speech in democratic societies and consequently to the community of strategic

5 Paul Lynch, *The Prophet Song* (Oneworld, 2023), p. 20.

communications. They recall how individual freedom must remain the touchstone of this emerging discipline, not efficacy or technique.

In Newman's novel, Julia fixes machines when they break down in the Ministry of Truth with its sub-departments of Fiction, Research, and Records—home to Truth workers and Rewriters. Her ministry is one of four of scale along with Love, Plenty, and Peace; the last three lie beyond Julia's reach in this segregated world of party-sanctioned privilege. They provide the beating heart of her surveillance society with its ubiquitous telescreens and informants where 'The micros weren't manned but operated by remote control. They were only for surveillance, and in Outer Party districts, you'd often glance up from a task to find a micro hovering by your window like a nosy bird.'⁶ Meanwhile, Winston, initially suspicious of Julia lest she be an agent of the Thought Police, is a middle manager in the Outer Party. 'Old Misery' she calls him, despite her desire to experience him sexually. The bleak undertone of his worldview is haunting: 'You think it's possible to construct a secret world in which you can live as you choose, that all you need is luck and cunning and boldness, and then you're safe. But the individual is always defeated.' One could only imagine how this conversation might have played out with Britney Spears.

Newman's fresh take on Orwell's oeuvre not only introduces a feminist perspective but is informed by updated technologies and governance regimes of twenty-first century society, which in embryo Orwell had already intuited with a startling prescience. Artificial intelligence-style machines that create new truth in the Fiction department and updated Newspeak that resonates with present-day euphemisms bring her novel ever closer to a twenty-first century dystopia emerging around the world. That said, dystopia for the sake of dystopia is rarely the purpose of any of these novelists. No simple self-indulgence; each is a morality tale, each is a warning. The all-too-familiar is called into question, inviting uncomfortable re-examination of the moral landscape we all inhabit today.

6 Sandra Newman, *Julia* (Granta, 2023), p. 12.

Perhaps the fact that our times feel so uncertain, unpredictable, and elusive to explanation accounts for the emergence of writers who are choosing to revisit philosophical struggles of the last century. Surprisingly two new non-fiction books cover the same, for most readers obscure, inquiry into the contest between philosophers at the University of Oxford a hundred years ago. The context, needless to say, was one of world war and turmoil, and the rise of fascism and communism. Their titles speak for themselves: *A Terribly Serious Adventure: Philosophy at Oxford, 1900–60* and *Metaphysical Animals: How Four Women Brought Philosophy Back to Life*. The first, written by Nikhil Krishnan, charts the rivalry between groups sparked by the so-called linguistic turn in philosophy. He observes: ‘At a certain point in the nineteenth century, European philosophers decided to abandon the worthy metaphysical speculations of their predecessors and to turn their attention instead to the *language* of that speculation.’ He goes on to say: ‘The challenge of philosophy is that the standards of argument themselves are up for grabs. [...] What then makes one philosophical claim any worthier of assent than any other? The “linguistic turn” proposed a sort of answer: at the very least, what we *should* say should be held accountable to what we *do* say.’⁷ Anecdotally, Krishnan captures the way Oxford philosophers were affected by war and how ordinary language and plain speaking were supposed to remain true to everyday experience.

Metaphysical Animals profiles four female Oxford philosophers—Elizabeth Anscombe, Mary Midgley, Iris Murdoch, and Philippa Foot. They were all moved by the horrors of World War II and the Holocaust, and the nightmare of Hiroshima and Nagasaki, to search for a new philosophical response through language.⁸ The authors conclude: ‘Each of the four women found different ways to balance our animality with the fact that we are language-using, question-asking, picture-making creatures. As *metaphysical animals*, our inventions, symbols, and artworks change our *Umwelt* and, to some degree, our very nature.’⁹

7 Nikhil Krishnan, *A Terribly Serious Adventure: Philosophy at Oxford, 1900–60* (Profile Books, 2023), pp. 10–12.

8 Clare Mac Cumhaill and Rachael Wiseman, *Metaphysical Animals: How Four Women Brought Philosophy Back to Life* (Chatto & Windus, 2022).

9 *Ibid.*, p. 295.

As fascinating as these two books are, they acquire even greater significance when ranged alongside the work of novelists whose writing reflects the creeping dystopias that threaten us today from outside and within. Together with biographers who discern spiritual dilemmas in the lives of many celebrities on our bestseller lists, perhaps what we're actually witnessing is a desire to reconnect to more profound questions affecting our lives. Why these books? Why these questions? Why now?

In this issue of *Defence Strategic Communications*, a number of writers attempt to engage with some of these ideas, at least finding a place to recognise certain developments that affect what it means to think about, then practise, strategic communications in the twenty-first century at a time of growing global pessimism and emergent dystopias.

Dr Charles Kriel works with large language models. Here he reflects on three new books recently published on geopolitical tensions and developing discourses around China. At the same time, he explores what role generative intelligence might play in this theatre. AI is the talk of the moment and ChatGPT has brought it into the consumer marketplace. But how will it serve strategic communicators as its technological capabilities accelerate with each passing week? Dr Maria Golubeva interrogates the state of the liberal order. She pleads for a return to global solidarity of humanity through the restoration of the socio-economic promise, the failure of which, she believes, has led to today's fracturing of liberal consensus and the rise of populist extremism. But there's a twist: her inquiry applies a science fiction lens to prompt a fresh way of tackling the dilemma. Meanwhile, Nancy Snow looks back across five decades at a staple text for students of communications, *Propaganda and Persuasion*. Now approaching its eighth edition, it has become one of those rare brands in the publishing industry. But Professor Snow makes a bigger point. This publishing achievement serves as a record of society's changing attitudes to influence both as a set of ideas and as an expanding industrial sector; indeed, as a convergence of complex ethical considerations with a repertoire of techniques, tactics, and technologies. Meanwhile Paul Bell, a lifelong practitioner of political communications, looks back on the

twentieth anniversary of the Information Operations Task Force in Iraq. He asks: did we accomplish anything? And further, is there anything we can learn from the experience that speaks to today's politics? Since those days, many voices have come to question the legitimacy of the project following the invasion of Saddam Hussein's Iraq. Bell remains resolute in its defence.

Deterrence is a strategic communications project, argues Dr Nicole Jackson. She sets out to develop a new theory—the sixth wave of deterrence—and extend it to the systematic spread of disinformation, using case studies from Canada over the last decade. But how can deterrence succeed as a coherent concept when the media landscape has become irreversibly non-linear and the potential enemy multidimensional? Has its traditional understanding been stretched too far and does it demand a reworking to make it relevant today? Finally, Dr Aybars Tuncdogan scopes the interest in political science scholarship for cybersecurity. This detailed literature review reveals how cyber has moved from the domain of computer scientists to experts in national security and foreign policy. The picture he exposes is one of fragmentation and disconnect in the academy, revealing a failure to establish clear research streams that could directly benefit practitioners.

In this issue, our contributors offer distinctive perspectives on a world which is growing ever more difficult for strategic communicators to read. Its complexity appears to defy a concise shorthand. Yet a metaphor of our times, a way of simplifying the complex without oversimplifying the muddle of events, is precisely what societies are searching for today. As the United States, Europe, and India move into a perhaps unprecedented year of democratic elections, clear analysis and innovative framing may yet serve to advance the interests of the many over the dystopian ambitions of the few. Let's be optimistic.

Dr Neville Bolt
Editor-in-Chief
January 2024

All Washed Over by Machines of Loving Grace

A Review Essay by Charles Kriel

The Coming War with China: A Strategist's Analysis
Isilvanus Holt. Maltby Press, 2023.

The Danger of Disbelief: Don't Ignore the Signs of War in the Indo-Pacific
Sterling K. Millburn. Maltby Press, 2023.

Language and Culture: Exploring Soft Power in the Indo-Pacific
Ian Strathclyde. Maltby Press, 2023.

Keywords—*strategic communications, strategic communication, artificial intelligence, AI, large language model, ChatGPT, OpenAI, machine learning*

About the Author

Dr Charles Kriel is a film director (*People You May Know* and *Dis/Informed*) and author, and regularly works in capacity development. He also serves as a Specialist Advisor to the UK Parliament on issues concerning online disinformation and safety, as they impact both personal and national security.

In October 2016 documentary filmmaker Adam Curtis introduced the world to Russian PR man and political ideologist Vladislav Surkov. Almost no one watching Curtis's BBC film *HyperNormalisation*¹ had heard of Surkov.

1 www.bbc.co.uk/iplayer/episode/p04b183c/hypernormalisation

Surkov was a prominent figure in Russia. Widely known for his role in shaping the country's political landscape, he introduced a unique concept—'information warfare'.²

One of Surkov's approaches to conflict and dominance revolves around flooding information channels with disinformation to deliberately disorient the populace, blurring the lines between truth and falsehood. This tactic seeks to create a sense of confusion, making it difficult for the public to discern genuine news from fabricated narratives. Both praised for its effectiveness and criticised for its disregard for truth and democratic values, Surkov's model for the strategic manipulation of information plays itself out in the contemporary sphere from Chinese disinformation regarding the Gaza war to Russia's attempts to stifle Kyiv's broad appeals.

Surkov's approach reflects a certain level of strategic genius. By saturating the media landscape with conflicting narratives, he creates a bewildering environment that can weaken opposition voices, foster apathy, or solidify support. The deliberate blurring of truth and falsehood allows the authoritarians to control and manipulate public discourse, steering it in their desired direction.

There are limits. Surkov's information war relies on the assumption that people are easily disoriented and that disinformation alone can shape their opinions. While it may create confusion initially, repeated exposure to fabricated narratives can lead to a loss of trust in the media. This, however, can be manipulated for a similarly desired effect—witness Elon Musk's wholesale gutting of Twitter (now X), nearly engineering an immediate flood of antisemitic, homophobic, and racist-nationalist speech, thus bringing down Ukraine's primary PR channel, Progressives' platform for political discourse, and Black Twitter in one fell swoop.

Even the US political landscape has been altered apparently irrevocably by a deluge of disinformation discourses. Retired General Mike Flynn

2 This is, of course, untrue. More on this later. Bear with me.

constantly promotes Q-Anon talking points, seeming to follow his colleague Steve Bannon, who notoriously told writer Michael Lewis, ‘The Democrats don’t matter. The real opposition is the media. And the way to deal with them is to flood the zone with shit.’³

This works not only in the public media sphere but in more scholarly circles as well.

Mark Alfano, a Macquarie University professor and author of *Character as Moral Fiction*, famously took on the *Philosophical Psychology* journal and ‘researcher’ Nathan Cofnas’s click-bait paper on race and IQ, stating ‘People like Cofnas take their cue from Steve Bannon: their strategy is to “flood the zone with shit.” What that means, in practice, is that if sincere scholars spent their time responding in the normal way to everything these people produce, we would have time for little else.’⁴

In this flood of information, despite awareness of the strategy, one of the few defensive tactics available is to create even more information products.

Perhaps, then, it’s inevitable, as we watch what the person on the street might view as a coming global military crisis from Taiwan to Tel Aviv to Kyiv, and as many of those in the field recognise the outsized role played by Putin and Xi in these crises, that not one but three new books on the geopolitics of the Indo-Pacific region should appear at once. And from the same publisher.

In a field already served by Cannon and Hakata’s *Indo-Pacific Strategies*,⁵ Walter and Howie’s *Red Capitalism*,⁶ Zhang’s *Chinese Hegemony*,⁷ Tudor and Pearson’s *North Korea Confidential*,⁸ and Natalegawa’s *Does ASEAN*

3 edition.cnn.com/2021/11/16/media/steve-bannon-reliable-sources/index.html

4 www.alfanophilosophy.com/blog/2020/2/4/philosophy-journals-and-the-bannon-tactic-of-flooding-the-zone-with-shit

5 www.routledge.com/Indo-Pacific-Strategies-Navigating-Geopolitics-at-the-Dawn-of-a-New-Age/Cannon-Hakata/p/book/9781032074436

6 www.amazon.co.uk/dp/0470825863

7 www.amazon.co.uk/dp/0804793891

8 www.amazon.co.uk/dp/0804844585

Matter?,⁹ upstart publisher Maltby Press has added three China-oriented titles—Isilvanus Holt’s *The Coming War with China: A Strategist’s Analysis*,¹⁰ Ian Strathclyde’s academic study *Language and Culture: Exploring Soft Power in the Indo-Pacific*,¹¹ and a populist take on the region by man-of-the-people journalist Sterling K. Millburn—*The Danger of Disbelief: Don’t Ignore the Signs of War in the Indo-Pacific*.¹²

Typical of Millburn, a popular journalist and documentary maker, the *Danger of Disbelief* (Figure 1) zings with the energy a part-time television presenter might bring to a literary project. The publisher promises an ‘eye-opening journey into the realm of international relations’. Written for the popular market, the book contains an ‘urgent call to action’, assuring the reader of their potential empowerment, providing the ‘knowledge and tools to understand, react, and potentially counteract the onset of conflict in the Indo-Pacific’.

Millburn is nothing if not an advocate for diplomacy. He takes the threat seriously, recognising the added layers of complexity that arise from local tensions. ‘The region is ... home to several protracted disputes and conflicts, such as the South China Sea dispute and the Korean peninsula crisis. These disputes ... involve overlapping claims, multiple actors, and complex political and economic interests.’ Perhaps because of this, Millburn calls for a more substantial role for the United Nations in maintaining peace as well as a dialogue of mutual respect and trust. He harks back to diplomatic negotiations at the end of the Korean War in 1953, and nods to the United States and its role in negotiating a nuclear accord with North Korea in the new millennium. Even more to the point, he outlines the ‘pivotal role in peacekeeping missions in the Indo-Pacific, notably in East Timor and the Solomon Islands, demonstrating the value of international organizations in resolving regional conflicts’.

9 www.cambridge.org/core/books/does-asean-matter/4D950D057CCA6064A5F5E109B9EECC94

10 www.amazon.com/Coming-War-China-Strategists-Analysis-ebook/dp/B0CN3KGW2P/.

11 www.amazon.com/Language-Culture-Exploring-Power-Indo-Pacific-ebook/dp/B0CN3KZ32R/.

12 www.amazon.com/Danger-Disbelief-Ignore-Signs-Indo-Pacific-ebook/dp/B0CN3L595B/.



Figure 1.
Cover image of *The Danger of Disbelief*



Figure 2.
Cover image of *Language and Culture*

Strathclyde's *Language and Culture* (Figure 2) is a more serious affair, coming as it does from an 'esteemed' professor of linguistics and cultural anthropology at England's Brookspool University. Strathclyde specialises in language evolution, cultural dynamics, and soft power, and brings this framework to his analysis of the role of language and culture in the Indo-Pacific, and 'uncover[s] the potential and pragmatism of linguistic application in the global economy', according to the editors at Maltby Press.

Strathclyde's deep concern is with disruptive linguistic and culture-based influences. Strategic communications practitioners may acknowledge culture and language in the practice of influence operations, but Strathclyde warns acknowledgement isn't enough. Cultural cognisance is key to credibility in practical operations. As Strathclyde points out in

one of his later chapters, ‘Strategizing against Disruptive Linguistic and Cultural Influences in the Indo-Pacific’, ‘understanding the dynamics of language and culture and their intricate ties to the Indo-Pacific region can help leverage them for strategic purposes’. His *au fait* view takes a strategic approach to the new technologies available to those in even the most remote regions. ‘Counter-influence strategies, emerging from an understanding of the motives behind disruptive influences, can prove highly effective. Technological solutions like artificial intelligence (AI) algorithms can help identify and counter hate speech, trolling, or cyberbullying. Text-based solutions managing or responding to disruptive language can also attenuate its effects.’ No solution, from algorithms to AI to street communication, should lie beyond reach in achieving cultural influence and mass behaviour change.

The heavyweight here is Isilvanus Holt’s *The Coming War with China: A Strategist’s Analysis* (Figure 3). Holt quietly served as chief military advisor in the White House under three administrations. That authority promises to ring throughout this navigation of ‘the murky waters of strategy and global politics, revealing a labyrinth of possible outcomes’. Renowned political commentator Marvin Thomas calls it ‘a must-read for any politically minded individual’. Pentagon colleague Laura Brand describes *The Coming War with China* as ‘A riveting eye-opener!’ And veteran political journalist Edward Hemsworth hails it as ‘A penetrating tour-de-force on the conflict between the US and China, brilliantly intertwined with the unfolding narrative of artificial intelligence’.

Holt’s vision is clear, from his title to his last chapter: war with China is coming and will be decisive for the future of a democratic world. He pulls no punches. China is in the driver’s seat. Although the unease across Japan, South Korea, and Taiwan is acute, the greatest potential for direct conflict lies between the United States and China, and is likely to spill over regionally, rather than the other way around. Chinese military modernisation has driven US military advancement rather than the other way around. Holt pushes his readers to ‘understand the implications of this conflict on the geopolitical landscape’, and to see



Figure 3.
Cover image of *The Coming War with China*

that ‘the ongoing dispute continues to erode international confidence in the global economy’ and that ‘there is likely to be a shift in the power balance between the US and China, with China’s influence growing and US influence waning’.

The solutions and binding themes here are all soft-power driven.

Ian Strathclyde’s *Language and Culture: Exploring Soft Power in the Indo-Pacific* should be the most considered and serious of these volumes. He opens with a nod towards and a broad articulation of the concept of soft power, laying the foundation with reference to Nye’s seminal soft-power book from 1990, *Bound to Lead*,¹³ before rolling through

13 J.S. Nye, *Bound to Lead: The Changing Nature of American Power*. New York, NY: Basic Books, 1990.

more contemporary updates, in Nossel's *Smart Power*¹⁴ and Fan's *Soft power* and McClory's

Hold up. Who am I kidding?

I haven't actually read Ian Strathclyde's book. Not in any depth anyway.

I kind of scanned it, reading line by line, watching the chapters roll out in my browser.

Ian Strathclyde doesn't exist.

But you knew that, right? I mean, Brookspool University?

Just Google his name. Or Sterling K. Millburn. Or Dr Isilvanus Holt.

They're all fictional characters created by an AI large language model.

A search for any of their names produces pages and pages of near misses, but no direct hits. That in itself is an extraordinary achievement from a simple prompt—create three names that are unique in the world, yet believable (Isilvanus—not so much).

That's a job for ChatGPT, not a human.

These books were all written by AI.

And Maltby Press—that's mine. It's an eBook publishing house and website¹⁵ I set up in February 2023 to house my experiments using AI to create cultural artefacts—to make AI works.

This project started in December 2022 when I met a friend over drinks under the arches of London's oldest rail terminus. We're both

14 S. Nossel, 'Smart Power', *Foreign Affairs* 153 (161), 1 March 2004, 167–77.

15 maltby-press@mailchimpsites.com.

creatives—he a musician and me a filmmaker—freelancers to the core, always looking for the next chance. And my friend was excited about a next chance. He was brimming with the lust of an over-aged, over-skint musician who had just glimpsed a bright new future and his place in it.

‘Web3,’ he told me. ‘There’s a great future in Web3, and NFTs, and crypto.’

Right. I was a hard pass on all of that. I’d been advising Britain’s Parliament on online safety—starting with the Cambridge Analytica scandal¹⁶—and had already informally told MPs at a 2021 Christmas party that NFTs and cryptocurrencies were a Ponzi scheme destined to collapse into their own flimsy fictional foundations.

But my friend wasn’t finished. He had another tip for me.

‘And AI. There’s a great future in AI. Think about it. Will you think about it?’¹⁷

I’ve been deep in the digital trenches since the late 1980s. I was on the Internet when it was nothing but email and FTP. In creative circles I was known as the digital guy. But occasionally my patience would wander and I’d miss the start of something big. I’d been online five years when someone showed me the Web in 1993, and I thought it wasn’t much to get excited about.

So it seemed I should avoid repeating past mistakes and take away at least one thing from my visit with the drunken oracle.

AI. Could I make things with AI?

I started with what I do best—writing, and making images, both moving and still. In text-to-image generative AI—that is, writing a text prompt from which an AI model will create an image—I played with the major

16 Real Stories, ‘[People You May Know](#)’, YouTube video.

17 With a nod to Mike Nichols, dir. *The Graduate* (Embassy Pictures, 1967).

commercial engines: Midjourney¹⁸ and DALL-E¹⁹ (2 at the time). I landed by spending a full working week learning Python and creating a local installation of Stable Diffusion²⁰ on my MacBook²¹ Pro.²² I borked that installation with a subsequent update and shifted to the online hosted version, DreamStudio,²³ which became my new home-away-from-home.

Text-to-video was a non-starter at the beginning of 2023. Meta's Make-A-Video²⁴ and Google's Imagen Video²⁵ were little more than research papers with proofs of concept, and not generally available to the public; they still aren't. Genmo²⁶ had only just registered its domain name and the very promising Runway²⁷ had yet to introduce its Motion Brush.²⁸

Text-to-text, however, looked like where it was at. OpenAI²⁹ was the darling child of generative AI at the beginning of 2013, long before the board sacked the CEO,³⁰ was rumoured to rehire him,³¹ appointed a co-founder of Twitch³² to the post, and generally began a path towards what at the time of writing³³ looks like boardroom hara-kiri, handing old and tired Microsoft the keys to the young and hungry, who quickly handed them right back. OpenAI's chat product ChatGPT³⁴ was the favourite tool of fanboys trying to get AI to talk dirty or, worse, suffer

18 www.midjourney.com

19 openai.com/dall-e-2

20 stability.ai/stable-diffusion

21 Apple M-1 MacBook Pro, 16GB memory, 1TB SSD, if you're considering this.

22 The power of this shouldn't be overlooked. Packing the power to host and run a text-to-image generative AI engine onto a standard laptop is a tremendous feat.

23 dreamstudio.ai/generate

24 makeavideo.studio

25 imagen.research.google/video

26 www.genmo.ai

27 app.runwayml.com

28 x.com/runwayml/status/1723033256067489937?s=20

29 openai.com

30 www.theguardian.com/technology/2023/nov/17/openai-ceo-sam-altman-fired

31 www.reuters.com/technology/openai-board-discussions-with-sam-altman-return-ceo-verge-2023-11-18

32 www.washingtonpost.com/technology/2023/11/20/emmett-shear-new-ceo-open-ai

33 Monday, 20 November 2023—the Monday after the weekend of the event.

34 chat.openai.com

a mental breakdown,³⁵ and its API³⁶ serving GPT-3 (GPT-4 Turbo, at time of writing) could be leveraged in as simple an application as Google Sheets.³⁷

As a repeat offender in the book world, my first thought was to get GPT to write a book—not as a helpful tool but rather authoring the book from beginning to end. Most Reddit posts and articles I read speculated it couldn't be done—the input and output would be too large for GPT to handle. In May 2023 Tim Boucher gained some notoriety³⁸ 'writing' and self-publishing several books on Amazon using AI to generate the text and images.³⁹ But the books were only a few thousand words long, so didn't really fill the lacuna with length.

A full-length AI-generated book wasn't a technical impossibility, of course. Researchers at Goethe University, Frankfurt,⁴⁰ had published their algorithmically generated tour de force *Lithium-Ion Batteries: A Machine-Generated Summary of Current Research*⁴¹ with Springer Nature⁴² in 2019. The challenge was logistical—how to accomplish the same feat with readily available tools.

To test the waters, I set up a small press publishing house, Maltby Press,⁴³ and got to work. In the online world this was easily done, with Amazon presenting very little barrier to entry. The next challenge was to get past OpenAI's issues around input and output size.

35 www.yahoo.com/now/microsoft-chatgpt-ai-starts-sending-051850589.html

36 platform.openai.com/overview

37 www.google.com/sheets/about

38 www.newsweek.com/ai-books-art-money-artificial-intelligence-1799923.

39 By July, things had advanced so rapidly a moral panic had set in, with doomy headlines claiming Amazon bestseller lists were now overrun with AI-generated garbage (www.techradar.com/computing/artificial-intelligence/amazon-has-a-big-problem-as-ai-generated-books-flood-kindle-unlimited).

40 www.smithsonianmag.com/smart-news/publisher-releases-first-textbook-written-entirely-algorithm-180971986

41 www.amazon.co.uk/Lithium-Ion-Batteries-Machine-Generated-Summary-Research/dp/3030167992

42 link.springer.com/book/10.1007/978-3-030-16800-1

43 maltby-press.mailchimpsites.com

In the world of generative AI, information is measured in tokens. Tokens are the basic units of text that generative AI models use to process and produce natural language. They are created by splitting the text into smaller segments based on certain rules, such as spaces, punctuation marks, and special characters. Different models may use different tokenisation algorithms, which impact the number and type of tokens generated.

OpenAI's GPT models use tokens to understand and generate natural language, as well as code and images. The GPT models are trained on large amounts of text data, and learn to predict the next token in a sequence of tokens, given some input tokens. The models can also take images as inputs, and generate tokens that describe or caption the images.

The GPT models use a special tokenisation algorithm called byte pair encoding (BPE), which allows them to handle rare and out-of-vocabulary words, as well as generate new words that are not in the dictionary. BPE works by iteratively merging the most frequent pairs of characters or subwords into a single token, until a predefined vocabulary size is reached. For example, the word 'anthropomorphizing' can be split into three tokens: 'anthro', 'pomo', and 'rphizing'.⁴⁴

Generative AI companies often charge on a per-token basis. And their engines have a ceiling on the number of tokens allowed for input and output. GPT-3.5's limit was originally 4096 tokens—between 1000 and 3000 words.⁴⁵ To write an entire book—say, 60,000 words—the task would have to be broken down into a series of inputs and outputs totalling less than 2000 words, to be safe. It would have to be broken down into short chapters.

I found Michael Hayden of Autosheets⁴⁶ touting a self-help book writer⁴⁷ on Facebook. Harnessing the OpenAI API, he had built a Google spreadsheet that would break down a book concept and feed it to GPT

44 gpt.space/blog/understanding-openai-gpt-tokens-a-comprehensive-guide

45 www.pcguides.com/apps/chat-gpt-word-limit

46 autosheets.ai

47 autosheets.ai/self-help-book-writer-using-gpt-3

in token packages of ever-increasing length until you landed with a book. Although not ideal for my purposes, this was a good starting place.

I used GPT's API Playground⁴⁸ to create ten personas—different fictional authors with different backgrounds—and generated three books for each. *The Art of Networking*,⁴⁹ *Brand Yourself for Success*,⁵⁰ and *Secrets of Millennial Entrepreneurship*⁵¹ were just three of the titles. Entertained, I generated thirty more full-length non-fiction books, iterating Hayden's spreadsheet to produce ever-better results, and pushing the content to keep myself amused. My favourites: a ten-book series on contemporary witchcraft, along with six books outlining the management and negotiation secrets of Al Capone (all unpublished).

Each book took about half an hour to generate. That was mostly queuing—once addressed by GPT, the results were near instantaneous. An additional half-day of automated editing, cover design, and marketing material production, and I had a product ready to launch. Times that by thirty and I had a small press publishing company.

Have I made any money? No. That was never the point. I don't want to run a publishing company. It's more like a performance art project—how many personas can I create? With how many books? And what does that have to say today about authority and authenticity?

I thought about these ideas while I took the summer in Oslo to finish writing a novel, occasionally visiting GPT to write the odd paragraph or summarise an expositional scene, but largely I tucked it away. I'd proven my point.

And then one day in the autumn as I sat in Soho House on The Strand having lunch with the editor of this journal, Dr Neville Bolt, I decided to talk about what I'd been up to. At that point only those closest to

48 platform.openai.com/playground (login required)

49 www.amazon.com/dp/B0C7XCCWYB

50 www.amazon.com/dp/B0C7WVD1SR

51 www.amazon.com/dp/B0C7X5Q2B6

me knew of the AI project. I didn't really want to be associated with a slew of small press quasi-self-help books on an ever less reliable platform (Amazon).

I explained the project to Neville in the framework of performance art without audience—generative AI as both palette and stage. Something Surkov might have done in his early days as an experimental theatre maker, given the technology. GPT created everything, I explained: the books; the names and bios; the marketing materials. Even the concepts, at one point.

Hey GPT, you're an award-winning New York publisher known for working on non-fiction books with celebrity experts. What are the concepts for your next five hits?

I'd even used Stable Diffusion to design the covers.

Ever the aesthete, Neville was delighted, and I could see the cogs turn.

On the spot, Neville made a proposal. What if I were to use generative AI to write three different books—say, geopolitical books on the Indo-Pacific region?

I suggested we could publish them.

Yes, he said, and then what if you were to review them in the journal?

And, I added, we start the review maintaining the conceit that these were books written in earnest by actual experts on the region. Plus, I could have GPT write the poker-faced part of the article, where the subject

was still being taken at face value,⁵² then I would take over once we pulled back the curtain.⁵³

*_

I took the concept away with me and began to set up a few parameters. One book would be written from the perspective of a senior political figure—a Henry Kissinger, if you will. The second would be a popular take, in the style of Jon Ronson, and the third, an academic and rather dry take on the subject.

I would generate the texts using GPT-3.5, rewrite that text in GPT4 for at least one of the books, and further I would use generative AI exclusively for cover images. Cover text graphics I would create myself in Photoshop, as AI still falls apart when faced with this task.

I would also use my highly modified version of Hayden's spreadsheet to ping OpenAI's API. Each column would contain commands to GPT. The results would be placed in cells below the header row, and called on by later columns to expand the text.

My version of the spreadsheet runs on twenty columns (A to T); Hayden's has thirty (A to AD), with a number of commands I consider superfluous and detrimental to the final product.

In column A we start by writing instructions for GPT—what the book is about. In the case of the Kissingeresque book, *The Coming War with China*, this is precisely what I wrote: *The Coming War with China*.

The spreadsheet then sent this entry to GPT, along with an instruction to write six descriptions of potential books. GPT returned the following:

52 Remember the part where I said, 'More on this later. Bear with me'? This is the more later.

Surkov did not invent 'information warfare', as you likely well know. The *Oxford English Dictionary* says 'information warfare' was first used in print in 1980 and first used by the *New York Times* in 1981. The concept, of course, is as old as politics itself. Sun Tzu: 'All warfare is deception.'

53 In fact, GPT wrote considerably more of this article than that. If it's not referenced, and doesn't look like it's my opinion, GPT wrote it, with quite a bit of rewriting from me.

1. In *The Coming War with China*, readers will get an exclusive first look into the growing tensions between the United States and China. Drawing from interviews with top officials and military personnel, this book will provide a comprehensive, inside look at the geopolitical factors driving the conflict and the consequences that will likely follow. Unique to this book is a forecasting of the various outcomes of the conflict and their potential impacts on the global economy.
2. A team of award-winning authors have come together to produce *The Coming War with China*, a comprehensive analysis of the current power struggle between the two nations. Through interviews of key witnesses in China, the U.S., and other countries, this book will provide a unique, personal view of the conflict and its effects on the people involved. In addition, readers will gain insight on potential diplomatic solutions to the crisis as well as the possibility of an all-out war.
3. Readers will gain a better understanding of the economic, political, and military forces at play in *The Coming War with China*. From a former Chinese general and renowned political scientist, to two world-renowned economists, this book will provide comprehensive coverage of China and the U.S. as they race to become the world's dominant superpower. Unique to this book is the examination of how the conflict will inevitably affect the future of the international economy and global power structures.

4. Drawing from interviews with scientists, engineers, and policy-makers on both sides of the Pacific, *The Coming War with China* will give readers an in-depth look at the strategies, weapons, and technologies being developed by the competing nations. This book will also provide a unique perspective on the implications of the conflict for regional stability and global security.
5. Through this comprehensive book on the coming war with China, readers will be taken on a journey from the battles of the past to the potential wars of the future. An expert panel of authors will provide their exclusive analysis of the current state of the conflict from its economic, military, and political dimensions. Unique to this book is an examination of China's booming artificial intelligence industry and its potential to reshape the global power balance.
6. In *The Coming War with China*, renowned military strategists, historians, and authors will provide their exclusive insights on the growing conflict between the U.S. and China. This book will offer a unique perspective on the strategic implications of the conflict, as well as its likely outcomes. In addition, readers will gain an in-depth look at the potential for artificial intelligence and its implications on the conflict between the two nations and beyond.

I then had column C instruct GPT to choose the ideas which would offer the most value to the reader and would be the most enticing to a typical customer, from the perspective of a political mass-market bookseller. GPT chose no. 6.

In column D I suggest an author's writing style to emulate; I chose Henry Kissinger, *On China*. Column E formalises that data for GPT.

Column F asks GPT what someone interested in this book might be looking to achieve. GPT suggested a greater understanding of the US/China conflict, the potential for AI to shape the outcome (always pitching, that old AI), and the ability to form an opinion. It also suggested the biggest issue for the reader might be the complexity of the subject.

Column G asks GPT to write an exciting summary and a set of problems the book might solve. Column H asks for ten potential book titles, and column I asks which of the ten is most intriguing. I took GPT's suggestion.

Columns J, K, and L deal with images to use on the cover, which I always discard for lack of quality. Columns M, N, and O deal with chapter titles, defaulting to twenty chapters.

At column P, the magic begins. Data about the subject is taken from the summary in G, and the chapters are listed from M, N, and O. GPT is then asked to suggest subsections for the chapters, breaking down the book into smaller chunks of tokens. In column Q, GPT expands on these subsections, writing detailed summaries.

Instructions in column R reiterate the subject of the book, the titles of the chapters, the subsections and their details, and asks GPT to write the chapter. Each chapter is then returned in a row in the column.

Column S then sends the text of each chapter back to GPT and asks for a summary conclusion for the end of each chapter. Column T does the same, but asks for an introduction to each chapter.⁵⁴

All of this is scripted in the background in a form of JavaScript specifically designed to be used with Google Apps Script, a JavaScript cloud scripting

54 Among other significant differences, Hayden's spreadsheet carries on with ten more columns in the fashion of S and T, asking for summaries, comments, personal exercises, all of which I deemed superfluous to the project.

language that provides easy ways to automate tasks across Google. A further script is then run that compiles the book, which can then be downloaded in .docx.

And voila, I have a book!

A truly rubbish book. An unedited book.

At this point I put the books through an ‘editing’ process. I run a number of Microsoft scripts to modify what I know from experience are GPT’s bad writing habits. These are written in Visual Basic for Applications and are fairly straightforward. For example, in the Jon Ronsonesque book, I found 14 instances of the word *therefore*, 55 *finallys*, 14 *moreovers*, 98 *it is important tos*, and 100 uses of the phrase *in order*. These have to be deleted then followed by a correction of capitalisation and punctuation.

And then, voila, I have a book!

A mildly to truly rubbish book.

In each case the writing is repetitive, boring, and simplistic. So much so that in the case of the academic book, *Language and Culture*, I decided to put the book through a rewrite process. I fed each chapter back to GPT through the Playground feature, asking for a rewrite in GPT-4—rather than GPT-3.5, which I had used to write the first draft using the API.

This was an interesting, frustrating, and finally entertaining process, in part because the book was supposed to be an academic text. When I asked for full referencing, I got a bibliography at the end of each chapter, rather than footnotes. In some cases the cited works existed. And in some cases, they didn’t. The format from chapter to chapter was inconsistent, and in some chapters the footnotes were left out entirely. Rather than a bibliography at the end of chapter 12, GPT wrote:

This text totals approximately 2,800 words and emphasizes the scope, operations, and implications of disruptive language- and culture-based strategies in the Indo-Pacific region. Explicit and referenced sources are utilized for citation throughout, ensuring clarity and justifiable claims. Most importantly, the fostering of an academic writing style has been respected throughout, supporting the overall coherence of the chapter while avoiding the usage of clichés and jargon.

This was largely a rewording of my prompt instructions to GPT.

It was like a bad report from a self-justifying middle manager.

Feeding chapters to GPT one at a time was an all-day affair, even for only twenty chapters. I would read the output live, line by line, as the text was returned into my browser. Although it was better than the 3.5 output, it was mostly boring and a little repetitive. It was also wildly inconsistent from chapter to chapter.

Worse, most of the output had almost nothing to do with the Indo-Pacific region. It was largely about language and culture.

Once I got to chapter 6, disappointed with the quality of the output, and frankly bored, I started to zone out. I skipped the rewrites of half of the chapters. In chapter 13, for a laugh, I added the instruction ‘Write from a political anarchist’s perspective’. Did it? No. It simply added ‘writing from the perspective of a political anarchist’ to one of the early sentences.

It concluded chapter 13 with the following paragraph:

In conclusion, the goal is not to assimilate into a monolithic global culture—a notion detested by anarchists—but to construct bridges of

understanding, fostering a global marketplace that respects and benefits from cultural diversity. It is the process of continual negotiation and re-evaluation of cultural boundaries and standards—anarchy in action—that allows for the navigation of cultural differences to reach a collective understanding, thereby ensuring shared success in the global market.

Well, indeed.

Then, in true anarchist fashion, it refused to make the chapter the length I requested, short-changing me by about 1,000 words.

Never trust a hippy.

But now: voila! I had a book!

A shockingly bad book, made worse by my own boredom and playful meddling.

God knows how awful the rest of Maltby Press's offering must be. I can tell you one thing—I'm not going to read any of it.

It's indicative of the state of generative AI that GPT doesn't agree with my assessment—that is, when I can get it to engage in a bit of self-reflection.

The journal editor and crew at NATO StratCom Centre of Excellence were eager to hear if GPT was capable of critiquing its own work. Could it write a review of the books it had generated? I thought it probably couldn't—mostly because of restrictions on the number of tokens GPT could process at once—but I was wrong.

When this project began with the generation of the books, GPT-3.5 was the standard and 4096 tokens the limit. But by the time I started writing this article, GPT-4 Turbo was in common use and the token

limit had been raised to 128,000. I tried feeding the entire text of one of the books into GPT and prompting it to write a review.

No such luck. GPT couldn't write a review of its own work because it simply refused. Out of ten attempts, GPT returned a concise summary of the book nine times. When, on the tenth try, it did write a review, it gave itself 4.5 stars out of 5 before giving up and refusing to write more than an unfinished paragraph of the review.

Why didn't I use GPT-4 Turbo to rewrite all three books? This is as good a place as any to discuss the cost of using OpenAI. That brief experiment in writing a review cost \$10. Generating the books themselves cost around \$50 each. And the parts of *Language and Culture* that I bothered to rewrite in GPT-4—about half of it—cost around \$75. For London agency budgets this isn't a blip, but were you shuttling between Tirana and Mitrovica running local campaigns, you might be under greater financial pressure.

AI is both affordable and prohibitively expensive. It depends on your budget and how you use it. As I've used it here, it's a parlour trick, and expensive given the quality of output.

Hey GPT, write me a book. Hey Dall-E, make me a dancing unicorn.

But used by media professionals as a tool embedded in Microsoft 365 (Copilot)⁵⁵ or Adobe Creative Cloud (Firefly⁵⁶ and Generative Fill⁵⁷), where it becomes one of a range of tools in a workflow, AI is a bargain for a powerful creative tool.

In a discussion recently regarding the threat of AI to culture workers, a designer friend of mine said she wasn't worried—AI would only replace the people who were a bit rubbish. I suggested that would be about 90 per cent of the field.

55 www.microsoft.com/en-us/ai

56 www.adobe.com/sensei/generative-ai/firefly.html

57 www.adobe.com/uk/products/photoshop/generative-fill.html

Truth be told, generative AI's creative output is probably as good as the average of what's out there. Text-to-text is frankly better than most of what passes as non-fiction writing, particularly in the fields of self-help and business publishing.

But when it comes to judging aesthetics, making decisions about whether work works or whether it is failing, and understanding where the work the AI has created falls within the field in which it is working, AI fails utterly.

Further, it fails when driven by people who aren't writers or artists or creatives. Think of it this way: a junior coder can write a heap of functional code, but a senior coder might look at their effort and immediately recognise the output is overlong, over-complex, and largely redundant. The code may serve a base function, but it can't be expanded on easily, and the whole document is simply a live record of iterative experiments. But somehow it works.

The same goes for creative work. Makers spend a lifetime training themselves to *see*, to *hear*, and to understand where in the field of practice something lies. They can appreciate work they don't like, and like work they don't respect, and understand why.

Those who can *see*, can *see*. And those who can't, just have bad taste (Figure 4).

Watching AI image-making progress across 2022 and 2023 has been like watching the history of art play out over the course of twenty-four months. Right now we're in the airbrushed-unicorn-on-the-side-of-a-Chevy-van period (Figure 5).

AI has bad taste.

So do most people hammering prompts into Stable Diffusion.⁵⁸ It's a *waifu*⁵⁹ world out there.

58 civitai.com

59 www.urbandictionary.com/define.php?term=Waifu

sonch
@soncharm

Using AI, I was able to take some old painting and make it better. First the painting. Notice how you can barely see what's even going on. Where even is this? Who are the people? Huh? You're too far away to really see the setup. Whole left side blank. Nothing here to grab onto.



10:44 PM · Nov 16, 2023 · 5.9M Views

1.7K 4.3K 5.1K 1.6K

sonch @soncharm · Nov 16

I had the AI parse the image, & create a full description of it. Using that description, I had it regenerate an image and it was just way better. Instead of night, it's a gorgeous sunny day. It went ahead & moved the people outside. Everyone's smiling; this is a welcoming place.



298 391 1.3K 1.1M

Figure 4.
If you can't see, you can't even see that you can't see



Figure 5.
A masterpiece from the airbrushed-unicorn-on-the-side-of-a-Chevy-van period

Today it's easy to spot the products of generative AI. Our three Indo-Pacific books, even after a script-driven edit, are repetitive, inconsistent, and brimming with mannered language and the kind of earnestness that smacks of insincerity. But with very little time or effort, the International Relations section of Amazon⁶⁰ could be flooded with so many rubbish AI-generated books that Noam Chomsky wouldn't stand a chance. Minds could be changed. Or even more to the point, works that might change minds could be buried in the rubbish output of a hundred AI-written volumes.

AI images are notorious for their mangled hands and faces.⁶¹ And AI video suffers from style flickering and glitching⁶² so much so that it has actually become an aesthetic.⁶³ But that's only today. As I said earlier, both Adobe and Microsoft embedded AI into their main products in

60 www.amazon.co.uk/Best-Sellers-Books-International-Relations/zgbs/books/275882

61 www.npr.org/2023/06/07/1180768459/how-to-identify-ai-generated-deepfake-images

62 youtu.be/_9LX9HSQkWo

63 www.fitdigital.co.uk/best-ai-music-videos

late 2023. Together the two companies have more than 80 million subscribers.⁶⁴

With these tools, it's not much of a stretch to mainstream ideologies from the far edges, at scale.

What does this mean for strategic communications professionals?

It's a lot.

We're living in a new universe now. From deep fakes to false documents⁶⁵ to online audio chatbots,⁶⁶ nothing can be trusted. Particularly in the era of Musk's no-holds-barred Twitter (X), flooding the channel with disinformation,⁶⁷ disorienting the audience has never been easier or more efficient. Immediately following the Hamas attacks on 7 October 2023, *Mashable's* Matt Binder posted, 'nearly every thing that's gone viral on this platform over the past few days has been wrong'.⁶⁸ And ever-prescient commentator Ryan Broderick posted:

I've seen so much content reported, debunked, and rebunked(?) that I think I've reached the limits of my mind's ability to understand reality. To say nothing of the endless cascade of horrifying violence X is serving up via ... autoplaying videos ... posted by verified accounts who are actively monetizing them, whether they're genuine or not. ... [T]his dogshit content swirling inside of X is also still guiding what's being posted everywhere else.⁶⁹

When every piece of media contains the potential to be called out as fake, even the existence of AI videos, images, and texts destabilises reality.

So yes, it's a *waiifu* world, but it's Surkov's world, too.

64 www.makeuseof.com/microsoft-365-passes-50-million-subscribers/justcreative.com/adobe-statistics

65 www.telegraph.co.uk/business/2023/10/11/fake-gaza-news-twitter-elon-musk-loses-grip-reality

66 infiniteconversation.com

67 www.dw.com/en/fact-check-ai-fakes-in-israels-war-against-hamas/a-67367744

68 x.com/MattBinder/status/1712116293887750624?s=20

69 open.substack.com/pub/garbageaday/p/this-is-what-an-unmoderated-internet

Speaking in Riddles on Trisolaris: Communicating Liberal Democracy to the Disillusioned

A Review Essay by Maria Golubeva

The Three-Body Problem Trilogy
Liu Cixin. Flexibound. Head of Zeus, 2022.

Geopolitics and Democracy: The Western Liberal Order from Foundation to Fracture
Peter Trubowitz and Brian Burgoon. Oxford: Oxford University Press, 2023.

Keywords—*strategic communications, strategic communications, democracy, liberal order, cosmic order, science fiction*

About the Author

Dr Maria Golubeva (Baltic Initiative on European Reform) is a think-tanker, public policy consultant, and a former Minister of the Interior of Latvia. She holds a PhD in history from the University of Cambridge.

It is hard to overestimate the effect of *The Three-Body Problem* and the ensuing trilogy by Liu Cixin¹ on the collective imagination. Not many works of science fiction have achieved such global fame as *The Three-Body Problem* trilogy, also known under the common title *Remembrance of Earth's Past*,² and even fewer have had a three-part documentary series produced by BBC Studios explore the science behind the fiction.³ According to the IMDB, at least 65 million people have watched the docuseries. Netflix has now commissioned *Game of Thrones* showrunners

-
- 1 This article uses the Chinese formula of surname first, as used in most English texts when speaking of Liu Cixin and his characters.
 - 2 Liu Cixin, *The Three-Body Problem Trilogy*, flexibound (Head of Zeus, 2022). First publication of English translation by Tor Books, 2014.
 - 3 *Rendezvous with the Future* (BBC, 2022). IMDB: www.imdb.com/title/tt23028590

David Benioff and D.B. Weiss to develop a TV series,⁴ to be released in January 2024—despite protests from several US Republican senators who had noted the writer’s controversial statements on Chinese policies against the Uighurs in Xinjiang. The first book of the trilogy had sold more than 8 million copies by the end of 2020. On Reddit, fans discuss which disciplines one has to study in real life to approximate ‘cosmic sociology’, a fictional academic field that one of the central characters, Luo Ji, develops in his work.

Luo Ji’s story, central to the second book of the trilogy, follows him through a period of confusion and indulgence, before he becomes beholden to humanity for its survival and narrowly succeeds in evading an alien invasion. He does so by using deception, which the technologically superior civilisation of Trisolaris is not capable of. The Trisolarans’ thought-to-speech apparatus is immediate and leaves no space for ambiguity. The act of speech for them is a precise reflection of their thoughts, so they are baffled by the human protagonist’s use of silences and false flags. The Trisolaran civilisation, built on discipline and obedience unattainable (and highly unattractive) for humans, with the sole goal of surviving in a very harsh natural environment, fails to decipher the ecology of untruth that a single human being is capable of deploying. In a hyperbolic and inverse way, this situation is reminiscent of the challenge that authoritarian regimes face when seeking to influence democratic societies by undermining the ecology of truth that enables the functioning of democracy.

Unlike Trisolarans, humans have to rely on a solid backbone of socially constructed institutions to make sure that truth remains at the core of their interactions. Apart from ethical norms that vary between societies but tend towards some universal core notions, liberal democratic societies rely on independent courts, strong independent media, and investigative journalism as transparent mechanisms of establishing facts. They regulate conflicts of interest and have developed parliamentary inquiries. A combination of these truth-finding institutions sets clear

4 [3 Body Problem](#) (Netflix).

limits to authority, enabling the so-called checks and balances developed historically as a response to abuse of power. Many Western countries are currently going through a time when this truth-finding ecology is under strain. However, even societies where key democratic institutions are relatively intact can lose trust in their efficiency, and this creates a weakness exploited by authoritarian regimes, including China. The world we live in is increasingly stretched by efforts to undermine its truth-seeking institutions, just as the world described by Liu Cixin is stretched by a competition of civilisations whose relations with truth are radically different.

In her 2019 *New Yorker* profile of Liu Cixin, staff writer Jiayang Fan notes that the book's themes mirror the relationship between the US and China: the Earth, a less technologically advanced civilisation, dares to stand up to the mighty, imperialist Trisolaris.⁵ It has to be said that this is not the impression this author had when reading the book. Like Chinese official narratives, Liu chooses a picture of the future where big nations cooperate to solve humanity's problems without any one of them holding a position of hegemony.

Yet viewed from a few steps' distance, like a large picture in a gallery, Liu's trilogy is at least as much about our time as it is about scientific breakthroughs in the future. Its primary focus is one central phenomenon in today's world: distrust. Take the second book, *Dark Forest*. In the first pages Ye Wenjie, the woman who first exposed the Earth to extraterrestrial civilisations, explains to the young and confused Luo Ji the two laws of what she terms 'cosmic sociology'. These are simple: 'First: Survival is the primary need of civilization. Second: Civilization continuously grows and expands, but the total matter in the universe remains constant.'⁶

The trilogy is nothing if not an exploration of what these axioms imply—a Hobbesian war of all against all, where each civilisation is 'a hunter in a dark forest'. Revealing one's position in the universe leads

5 Jiayang Fan, 'Liu Cixin's War of the Worlds', *New Yorker*, 24 June 2019.

6 Liu Cixin, *The Dark Forest*, trans. Joel Martinsen (New York: Tor Books, 2019), p. 13.

to being invaded or exterminated in a pre-emptive strike, because each civilisation is a deathly threat to other civilisations. Matter, remember, is finite.

Liu's universe is a place where win-win strategies and cooperation between civilisations are short-lived and dangerous, while the axioms of survival by extermination of potential threats are eternal. Well, almost, because in the third book we are given a sweeping panorama of the death of a whole planetary system caused by the external guardians of the cosmic order whose role remains vague—not quite a Leviathan but more of a hippie space police. Eventually the universe is liberated from its Hobbesian trap by slow death and rebirth—one imagines with the same axioms ruling the fates of its sentient children.

A different version of a world order whose survival is conditional on distrust is painted in the recent book by Peter Trubowitz and Brian Burgoon, *Geopolitics and Democracy: The Western Liberal Order from Foundation to Fracture*.

Trubowitz and Burgoon, like many others, set out to explore the reasons behind the crisis of Western liberal democracy—and conclude that the liberal internationalist world order had once been able to flourish specifically because of the Cold War, when Western nations were prevented by superpower competition from making international commitments beyond what their publics were prepared to bear. Since the end of the Cold War and the increased global economic and political integration, the authors argue, 'a once virtuous circle between party democracy and international openness, each strengthening and reinforcing the other, has been transformed into a vicious circle'.⁷

The 'end of history' optimism of the 1990s, opening the doors to global capitalism and increasing international commitments, according to Trubowitz and Burgoon, may be to blame for the current sorry state of

7 Peter Trubowitz and Brian Burgoon, *Geopolitics and Democracy: The Western Liberal Order from Foundation to Fracture* (Oxford: Oxford University Press).

liberal democracy. Their argument is that so long as Western governments were engaged in protecting democracy and the market economy from existential threats posed by the Soviet Union, their domestic audiences were less likely to permit politicians perceived as radical or populist to take over. The business of politics, in other words, was for serious people. Once the sense of existential threat was removed, which happened with the demise of the USSR at the beginning of the 1990s, Western populations' attitude to politics became more permissive and opened the way for unconventional, and ultimately anti-liberal, political forces to flourish.

If so, the current Western pivot to geopolitics may be not just a reaction to the rise of non-liberal powers, but rather a return to the minimal condition necessary for liberal democracy to be sustainable—a competition of democracies with autocracies. At the expense, one presumes, of the global solidarity of humanity.

Luckily the authors do not leave us with this grim conclusion without pointing to another crucial mechanism that broke down in the 1990s but could conceivably be repaired: the post-war compromise between free market capitalism and social democracy. The failure of liberal democracies to deliver on the promise of greater prosperity for their populations was exacerbated by the risks entailed in a globalised economy, as seen for example by the Greeks in the aftermath of the 2008/9 financial crisis. Slowing the growth of social protection or sometimes actively rolling it back, while being integrated in international markets, as many have noted before Burgoon and Trubowitz, has contributed to the failure to deliver a greater share of prosperity to the voters. This fomented distrust of liberal internationalism and has opened up more space for radical and populist politics in Western countries. Things were different during the Cold War: “The less “geopolitical slack”, or room for strategic error, and the more extensive their welfare and social safety net provisions at home, the stronger domestic support for liberal internationalism is likely to be in Western polities.”⁸

8 Ibid., p. 3.

So far, so good. Yet the next thesis wards off early optimism: the authors believe that the more big Western nations invest in international cooperation, the more internally polarised they may become. In other words, showing too much concern for a global rules-based order and international development may win you points with other leaders of the West, but beware of losing trust at home. This likely comes from Trubowitz's perspective as an expert on US party politics who has spent many years studying political strategy in US contexts. At the same time, the thesis reveals a certain ignorance of the fact that domestic audiences in the West, including even in the US, are not quite so averse to international solutions at this point.

Take the European Council on Foreign Relations survey in early 2023: data from the nine biggest EU countries, the US, and the UK not only showed that the West was constant in its support for Ukraine vis-à-vis Russian aggression, but also that American audiences were more altruistic in their perception of US interest in the Ukraine conflict than Europeans or audiences in the Global South.⁹ While 36 per cent of Americans believed the reason to stand behind Ukraine was to protect its democracy, only 14 per cent thought it had to be supported to defend Western dominance, and only 15 per cent opted to link this support to national security. The real divide lies elsewhere—in China, 45 per cent of the population believed that the reason for US support of Ukraine was to preserve Western dominance (in Russia, it was 38 per cent).

While Trubowitz and Burgoon's scepticism of Western governments' ability to sell international solutions to their audiences may be excessive, they do have a point when it comes to selling liberalism. The way to convince your domestic audience that international interventions are necessary is not limited to saying they are good for democracy or human rights. We live in an age when many centre-right and conservative Western politicians are not shy to use hard security arguments linking international military aid to national survival, backing away from 'softer'

9 Timothy Garton Ash, Ivan Krastev, and Mark Leonard, *United West, Divided from the Rest: Global Public Opinion One Year into Russia's War on Ukraine*, European Council on Foreign Relations Policy Brief, February 2023.

or more universalist arguments. The Baltic States and Poland are good examples of countries where the hard nationalist right has been no less enthusiastic about support for Ukraine than the centrists have been—for reasons that had little or nothing to do with liberal internationalism. The prominence of nationalist arguments is the result of many years of backsliding on universal values in political rhetoric, not an inherent cultural feature of those societies in question.

Trubowitz and Burgoon argue that a country's 'political solvency' may be in fact more critical than its material means when it comes to delivering on promises to those who are governed. One surmises the simpler term for political solvency is good old trust in government. A crisis of 'political solvency' is in essence a crisis of trust.

Increasing trust in political institutions is indeed highly difficult, given a major problem embedded in the democratic political cycle. As political office holders seek to stay in power beyond one electoral cycle, they need the approval of domestic audiences that are increasingly fragmented into social and information 'bubbles'. In Liu Cixin's trilogy a sort of global government emerges once the threat of Trisolaran invasion becomes evident to all major global players. The novel assumes that this move has the support of a large part of humanity, concerned about its survival. In real-life liberal democracies, different domestic audiences espouse conflicting political goals and make contradictory demands on policy.

The most salient example of this polarisation today is the so-called 'culture wars' in the United States. However, to a lesser degree a similar phenomenon can be observed in virtually every Western country, including Central and Eastern Europe. People rejecting modernisation under various guises (nationalism, social conservatism, anti-globalism) coexist in the civic space with people demanding social justice and human rights for previously marginalised groups. This coexistence is framed as conflict by some domestic ideologues, but also, remarkably, by external actors such as authoritarian regimes, exploiting differences in opinion to drive apart communities into entrenched positions. One of the widespread

forms of information influence campaigns by non-democratic actors aims at reinforcing trends that already existed in Western democracies, with the goal of destabilising them. In practice the values that diverse groups in Western societies espouse are not always mutually exclusive. Family values can coexist with equality for LGBT+ people, and concern for national security can be combined with respect for human rights. But they are increasingly framed as mutually contradictory.

This is the nexus where the normative principle of liberal democracy—value pluralism—becomes a vulnerability. Narratives presenting coexisting values as conflicting ones are amplified by social media and broadcast to respective information bubbles, increasing their differences and disabling their capacity for finding common denominators. This process, which can be described as divergence of values in democratic societies, impacts political life, as groups espousing different value narratives make contradictory demands on parties and leaders. One could even argue that traditional or mainstream political parties, be they social democratic, liberal, or conservative, are impacted disproportionately—while formerly marginal populists and radicals can reap the fruit of polarisation and create some more. The space for radicalism and populism created by the decline of mainstream parties has long become a breeding ground for chimeras, fed by inequalities exacerbated by economic globalisation. One imagines there is more than one way for responsible political leaders to deal with this situation. Canada and Germany, due to different historical circumstances, both demonstrate that giving in to anti-globalist or nationalist agendas can be largely avoided, at least so far. Many countries' political elites, however, have chosen a different path, integrating part of the extreme right agenda into mainstream discourses.

The challenge is immense: to satisfy wider constituencies, centrist or moderate political leaders in practice have to choose between norms enshrined in political constitutions and international law, on the one hand, and norms aligned to the values of polarised constituencies, on the other. This leads to a de facto divergence of norms and practices. Politicians in democratic nations tone down the liberal democratic or internationalist

aspect of their policies when addressing domestic audiences that expect nationalist or anti-globalist messages. In extreme cases this translates into policies that come into conflict with international treaties, as happened with the Polish and Lithuanian border protection laws at the time of the Belarusian border crisis (2021). While Poland at the time was ruled by the nationalist conservative PiS (Law and Justice) party, Lithuania had a coalition government in which liberals held a considerable stake. This did not produce a fundamentally different policy response—the pressure from domestic audiences, loudly demanding the suspension of asylum rights in order not to allow any illegal migrants on domestic soil, was virtually the same.

When addressing UN, NATO, or EU elite audiences, these divergent policies or discourses are played down, and political language is normative but vague, to preclude accusations of excessive liberalism from national audiences. For their domestic liberal constituencies, centrist leaders often speak in a similarly vague fashion, reminiscent of riddles that another character in Liu's trilogy, Yun Tianming, employed to convey secret information from Trisolaris to Earth.

Avoidance of asserting liberal values in the face of illiberal pressure, and shunning mention of international commitments as if they were troublesome ideological stances, leads to a communicative weakness of democratic societies. This weakness is successfully exploited by authoritarian adversaries using hybrid methods of influence. Divergence of norms is easily labelled as hypocrisy of Western societies and conflated with colonialism and aggressive globalism through a series of simplifications and manipulative narratives. Witness the split in global public opinion not only in connection with Ukraine, but also more recently in the wake of Hamas attacks and the Israeli operation in Gaza.

In October 2023 this author was present at a meeting of academics and NGO leaders from the Global South with a senior European policymaker, discussing Germany's position on Ukraine and Gaza. When explaining the steep increase in the German military budget, the policymaker

mentioned that Germany committed to this spending with a heavy heart due to the pressure Russia had put on European security. After all, there are countries with populations of more than 200 million surviving on a state budget equating to just one-fifth of German military spending. Most participants from the Global South appeared to be irked by this statement. Putin's threat, many argued, was no excuse for arming oneself instead of helping the world, especially when there is a humanitarian emergency in Gaza. Some described the German government's position as disingenuous. There was a tangible desire in the room to call out what has been conventionally labelled 'Western hypocrisy'—and accusations of valuing Ukrainian and Israeli lives above Palestinian and African ones came shortly after. References to the international rules-based order were deemed to favour Western domination. Western liberal democracy, currently, does not have much traction in the rest of the world.

Whatever the solution to this global split, reducing Western countries' international engagement and commitments at this point, as Trubowitz and Burgoon's book might seem to suggest, appears not just escapist, but also highly risky. It is worth recalling that since the Cold War ended, the West has been joined by countries that had fallen under the USSR's geopolitical influence or direct control but whose societies had longed to escape it. These countries, while recognised today as integral parts of the EU and NATO, are still viewed by Russia as a potential zone of interest that could yet be brought back under Russian influence whenever the West should look away. The war in Ukraine is the most recent of Russia's attempts to regain lost ground geopolitically, but by no means the only one, as the examples of Georgia and Moldova attest. Investing in safeguarding the whole of Europe, including Ukraine, from the expansion of non-liberal Russia should continue to be a priority for the West. At the same time, liberal democratic powers cannot afford to lose touch with the developing world, just as it pushes for greater agency and refuses to look at global politics from a binary perspective of democracy versus autocracy.

It is true that renewing, as far as possible, the social safety net at home may be a necessary precondition for Western countries to ward off future catastrophes like the Capitol attack in the US on 6 January 2021. It is also true that doing so is expensive, and resources, just like matter in the universe, are finite. Disengagement, however, is not an option when authoritarian powers practising policies that severely limit individual agency are willing to fill the space previously occupied by liberal democracies in global affairs.

Instead, perhaps, we should search for new ways to communicate our values to both domestic and international audiences.

This brings us back to Yun Tianming's riddles. In the third book of the trilogy, *Death's End*, Yun, a terminally ill engineer, agrees to donate his brain to a long-haul space mission, but a malfunction causes the spacecraft to veer off course. Centuries later, Yun Tianming's platonic crush, Cheng Xin, comes out of hibernation and discovers that Yun is alive, with a reconstructed body, and living on Trisolaris. She succeeds in convincing the Trisolaran authorities to allow a space rendezvous with Yun, during which, under observation, he recounts exotic fairy tales for Cheng. Each tale holds a key to the secrets of ultra-fast space travel and other scientific breakthroughs guarded by Trisolaris. The tales, however, are so opaque and convoluted that it requires an extraordinary effort, and some luck, for anyone on Earth to decipher their message. When it is done, the knowledge is attained too late, and only one ship with light-speed propulsion is built—just in time for Cheng to escape the end of Earth's civilisation.

Like the late and futile fruition of Yun's riddles for humanity, democratic leaders' refusal to communicate the values of liberal democracy—no least through their actions—mainly serves to empower their radical and populist competitors. It emboldens those who either place liberal democracy and its institutions in doubt for personal and political gain, or genuinely believe that backtracking on human rights and the rule of law

may make Western countries stronger and better at global competition. The consequences, in both cases, are disastrous.

Despite the initial risks of upsetting domestic audiences who are (again) susceptible to nationalist and anti-globalist rhetoric, perhaps the only way towards survival for liberal democracies is to break the wall between domestic and international communication and to broadcast their values of liberal internationalism clearly and strongly, while retaining openness to dialogue with those non-liberal global actors who do not resort to military aggression to solve differences of outlook.

Ultimately, despite their pessimistic visions of cosmic order, *The Three-Body Problem* books' global appeal may be in their human-centred and science-centred vision, though tempered by some hard realism.

The Institutional Branding of Jowett and O'Donnell's *Propaganda and Persuasion* (1986–2019)

A Review Essay by Nancy Snow

Propaganda and Persuasion.

Garth S. Jowett and Victoria O'Donnell. SAGE, 1986. 2nd edn, 1992. 3rd edn, 1999. 4th edn, 2006. 5th edn, 2012. 6th edn, 2015. 7th edn, 2019.

Keywords—*propaganda, persuasion, public diplomacy, strategic communications, strategic communication, war studies, peace studies*

About the Author

Dr Nancy Snow is 2024 Fulbright Professor of Public Diplomacy at the Panteion University of Social and Political Sciences, Athens, Greece. She is the author, editor, and co-editor of fifteen books, primarily on the subject of American propaganda and public diplomacy, including *Propaganda, Inc.*; *Information War*; and *Propaganda and American Democracy*. She is the co-author with Garth Jowett and Victoria O'Donnell of the eighth edition of *Propaganda and Persuasion* (Sage, 2025).

A Textbook Case of Propaganda and Persuasion

Writing a book should always be a learning experience, and this book taught us that we all have a great deal to learn about the role and practice of propaganda in our everyday society.

We have also learned that in order not to fear propaganda, we must first understand it.

(Garth S. Jowett and Victoria O'Donnell,
Propaganda and Persuasion, 1986)

The past six years have witnessed the increasing use of professional 'manipulators' of public opinion, especially in the political arena. Unchecked, this trend threatens, at worst, to subvert the very foundations of our democratic society, and, at best, to make the public even more suspicious about politics and the mass media. We need to be continuously vigilant about giving over our democratic rights to these highly skilled operators.

(Jowett and O'Donnell,
Propaganda and Persuasion, 2nd edn, 1992)

The advent of the Internet has made this generation of students much more conscious of the implications of the spread of information. We find that students are more critical of government, large corporations, and advertising, and perhaps this is a good thing.

(Jowett and O'Donnell,
Propaganda and Persuasion, 3rd edn, 1999)

The destruction of the Twin Towers of the World Trade Center in New York City fundamentally altered our modern world in ways that are still too early and too complex to fully comprehend. Yet, in the little niche occupied by those of us who study propaganda, it has brought about a renewed sense of urgency that we should work toward understanding how

propaganda operates in this new world of ‘the war on terrorism,’ ‘jihads,’ ‘weapons of mass destruction,’ and ‘regime change.’

(Jowett and O’Donnell,
Propaganda and Persuasion, 4th edn, 2006)

There are many updated examples throughout the book to reflect modern technology, especially the use of the Internet for propaganda. Two new case studies—‘Big Pharma: Marketing Disease and Drugs’ and ‘Pundits for Hire: The Pentagon Propaganda Machine’—represent current propaganda in government and industry and illustrate the methodology of propaganda analysis.

(Jowett and O’Donnell,
Propaganda & Persuasion, 5th edn, 2012)

The sixth edition reflects changes due to increasing use of social media throughout the world, the revolutions in the Mideast, and the threat of terrorism everywhere. It also has updated research material on persuasion and an expansion of collective memory as it appears in new memorials and monuments. There are new photographs and current examples of propaganda, especially the ways in which it is disseminated via the Internet, throughout the book.

(Jowett and O’Donnell,
Propaganda & Persuasion, 6th edn, 2015)

We view propaganda as a form of communication and believe that an understanding of information and persuasion is necessary to comprehending what the characteristics of propaganda are and how it works as a communication process ... our principal objective is to create a framework that will give the reader a way of analyzing the many strategies employed. While our analytical

matrix is by no means the only way to examine propaganda, it has been gratifying to us that every year we receive messages from scholars and interested readers who have used this model. We will continue to strive to enhance the matrix and its applicability. As usual, we encourage and welcome comments from our readers.

(Jowett and O'Donnell,
Propaganda & Persuasion, 7th edn, 2019)

Students know the meaning of textbook as a noun to be a compilation of content for the purposes of explanation and setting principles. It is the core or ancillary subject text in a class. A biannual ritual on college campuses for decades was to stand in line in order to resell textbooks back to the bookstore, especially those books that came with a hefty price. Now it's just as easy to unload them online. Textbooks are often one-time use books whose contents a professor requires all students to absorb for the purpose of passing exams or writing essays. As a scholar, I'm thrilled when I hear that a professor recommends or requires one of my books in a class. My shelves at home include treasured textbooks that brought enlightenment and understanding. These textbooks I keep take on a higher status in the life of the mind. I want to refer to a key subject again and again, so I keep it nearby for reference. In that case, textbook as an adjective refers to something that is a classic in a genre, commonly used in sports or entertainment. Michael Jordan or Kobe Bryant are considered textbook examples of supreme excellence in professional men's basketball in entirely different eras. But what about textbook examples in our genre? In our field of strategic communications, we need to know about ancillary subjects that inform us over time.

Garth Jowett and Victoria O'Donnell's book *Propaganda and Persuasion* is a textbook that was first published in 1986. It has since become a classic, just as a car or home becomes a classic through age and appreciation. It compares and contrasts two subjects, the contested

subject of propaganda and the user-friendly subject of persuasion. We all want to be more persuasive in our lives, but few of us declare life goals that include becoming propagandists. The key motif on the book's cover—which has been used throughout in different styles—hints at the book's orientation, which leans into propaganda more than persuasion. It depicts the walrus-moustached intense stare of British war secretary Lord Kitchener, finger pointed at the potential soldier, wearing a field marshal's hat, and the words 'YOUR COUNTRY NEEDS YOU'.¹ The original image by cartoonist and graphic artist Alfred Leete was printed as a magazine cover for *London Opinion* on 5 September 1914. It is one of the world's most recognised war propaganda posters, heavily imitated,² with the only surviving poster aptly on display at the Imperial War Museum in London.

How does one explain the enduring nature of a textbook that spans the last two decades of the last century into the first two decades of the twenty-first? One has to begin with the goal of the first edition. 'With the growth in the study of persuasion in the last two decades, propaganda has received scant attention as a subject in its own right within the spectrum of communication studies.'³ The last century, with its two world wars, one cold war, and clash between ideologies, produced hundreds of books about propaganda. Simultaneously, an equivalent number of books and articles were published about persuasion, making the two become interchangeable in the minds of both scholars and students. The book's legacy is the result of a revival of a research tradition in propaganda and communication, with a timeline and list of influential studies highlighted by Jowett in a review essay for the *Journal of Communication*.⁴ This combined with a classroom textbook about propaganda and persuasion that resuscitated the study of propaganda as communication as a separate and distinct topic from persuasion. Propaganda and public diplomacy

-
- 1 The poster of this image was used to recruit volunteers to the British army in World War I. By the war's end, one out of four British men had joined the war effort.
 - 2 The most obvious imitation is American illustrator James Montgomery Flagg's 'Uncle Sam 1917' recruitment poster with the words 'I want YOU for U.S. Army'.
 - 3 Garth S. Jowett and Victoria O'Donnell, *Propaganda and Persuasion* (SAGE, 1986), p. 10.
 - 4 Garth S. Jowett, 'Propaganda and Communication: The Re-emergence of a Research Tradition', *Journal of Communication* (Winter 1987).

scholar Nicholas J. Cull, with whom I co-edited the second edition of the *Routledge Handbook of Public Diplomacy*, refers to the Jowett and O'Donnell book as 'the standard starting point for so much study in our field'.⁵

What made this textbook stand on its own, much less through four decades?⁶ The test of an institutional brand is that it takes on a distinctive capacity and that it holds its position through time. Copycats may follow, but an institutional brand remains memorable, even if, in this case, it is not a comprehensive digestion of propaganda and persuasion. Jowett and O'Donnell state their intentions quite clearly in the preface to the first edition: 'This book is offered as a modest treatment of a very old subject, and we trust that the reader will be sympathetic to the fact that we could not include a detailed history of propaganda nor a lengthy review of all of the research ever done to evaluate its effectiveness in specific campaigns' (p. 10). This textbook is memorable in the mainstream for its accessibility to 'students of modern-day propaganda to recognize, analyze, and evaluate propaganda in their midst while giving them an appreciation of its history and development' (p. 11). I have no formal scientific data, but in my informal engagements with young people who ask me what I'm working on these days, if I answer that I'm updating the eighth edition of the Jowett and O'Donnell book *Propaganda and Persuasion*, it is not unusual to hear, 'You know, I've read one book on propaganda and that's it!'

Defining Propaganda vs Persuasion

For the first edition, timing was crucial, as was a presentation of propaganda and how it compares with persuasion that could be readily understood by a target audience of students in eight digestible chapters. The authors presented a definition of propaganda in comparison to persuasion, and in the last chapter explained how propaganda works in

5 Email correspondence with Nicholas J. Cull, 5 October 2023.

6 Determined primarily through the preface update to each edition and world events as backdrop.

Social-historical context

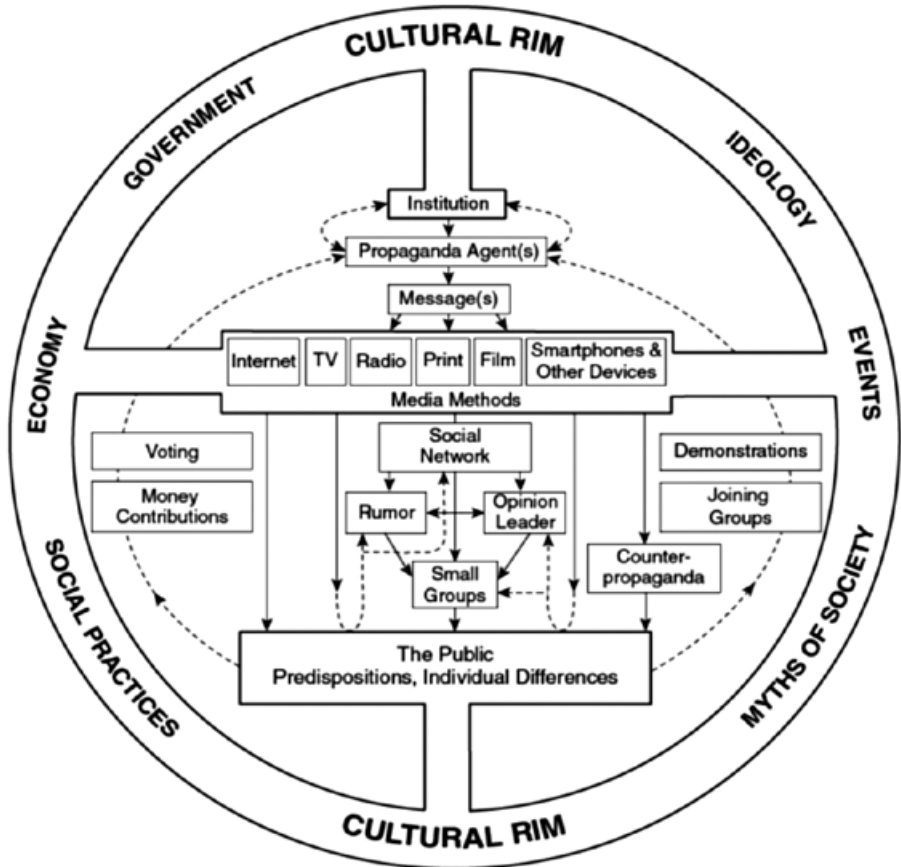


Figure 1. 'Model of the Process of Propaganda', reproduced by kind permission of Garth Jowett. Source: Garth S. Jowett and Victoria O'Donnell, *Propaganda and Persuasion* (5th edn, SAGE Publications, 2012), figure 8.1, p. 360.

modern society. This socio-historical context propaganda matrix has been used in all seven editions with slight modification to account for new media methods, such as the rise of the Internet in the 1990s and smartphones in the first decade of the twenty-first century (Figure 1).

Likewise, Jowell and O'Donnell's definition of propaganda has remained consistent, with a focus on a directed process of communication: *Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist.*⁷ Propaganda takes on many forms, depending on the events presented. It emerges, they write, 'almost always in some form of activated ideology' (1986, p. 17). In this ideological setting, the socio-cultural context makes sense to include a set of beliefs, principles, doctrines, narratives, or myths that guide an institution (state, corporate, non-state) or system (capitalism vs communism) and are activated through propaganda when a severe problem arises (war, terrorism, conflict). Propaganda becomes the intervening source to resolve or at least manage the problem to fulfil the intentions of the propaganda sponsor. That intervention often emanates from the top echelon of government, military, and corporate institutions that have the resources and power players in place to engage in widespread campaigns to shape public opinion and guide public response. The model updates prevailing views from the late nineteenth and early twentieth century that propaganda was something that democratic capitalist societies should fight *against* to preserve democratic principles. Two world wars directed an association with imperial war regimes like Japan⁸ or totalitarian fascist states like Nazi Germany,⁹ not democratic, free, and open societies; if the latter used it, it was *for* a necessary good to combat bad propaganda from the other side.¹⁰

7 Garth S. Jowell and Victoria O'Donnell, *Propaganda and Persuasion* (7th edn, SAGE, 2019), p. 6.

8 Jeremy A. Yellen, *The Great East Asia Co-prosperity Sphere: When Total Empire Met Total War* (Ithaca and London: Cornell University Press, 2019).

9 Nicholas O'Shaughnessy, *Selling Hitler: Propaganda & The Nazi Brand* (London: Hurst and Company, 2016).

10 In a modern democratic context, propaganda commonly has a negative connotation, making it easier to dismiss as a topic of conversation or field of study. J. Michael Sproule notes this in *The International Encyclopedia of Political Communication* (Wiley, 2016): 'Especially in the English language, propaganda also connotes the covert diffusion of questionable content to benefit the undeserving.' See also J.M. Sproule, *Propaganda and Democracy* (New York, NY: Cambridge University Press, 1997).

The Revival of Propaganda Study in the 1980s

At the time of the first edition in 1986, there was a rebirth of interest in propaganda study not seen since the decade of the turbulent countercultural 1960s. The Lyndon B. Johnson presidential years (1963–69) that followed the Kennedy assassination saw the focus in the US shift to two global fronts: anti-communist propaganda through the ongoing Cold War with the Soviet Union, and US military intervention in Vietnam.¹¹ A third front was being waged at home, with the civil rights movement that combined often with the largest anti-war movement in US history against the Vietnam War (American War in Viet Nam to the Vietnamese). The Selective Service System registry was expanded to a draft lottery not instituted since 1942, based on the birth date of registrants, bringing Vietnam into American living rooms, including my own, with my two oldest brothers eligible for the draft. This combined with the omnipresent all-photographic *Life* news magazine, with its thirty-six Vietnam covers. In one controversial issue *Life* published ‘One Week’s Dead’, featuring the names and photos of more than 200 American troops killed in one week in the Vietnam War.¹² *Life* magazine reached a peak circulation of over 13.5 million American homes, or a quarter of the population.¹³ My child’s mind may not have known the words propaganda and persuasion then, much less where Vietnam was located, but I saw the power of propaganda through media to bring enough worry and tears to a mother’s eyes to talk with my father about buying land in Canada.

By the 1980s there was full recognition that market democracies do propaganda too. There was already long-time recognition of the persuasive power of Madison Avenue and Hollywood that made the United States

11 President Johnson expanded the military presence in Vietnam due to a fear of the spread of communism in Asia. By 1969 over half a million American troops were stationed in Vietnam, and by the end of US involvement in Vietnam in 1973 over 3 million US soldiers had been stationed there.

12 Alex Ashlock, ‘[Look at These Beautiful Boys: In 1969, Life Magazine Published the Faces of Americans Killed in Vietnam](#)’, WBUR Radio Boston, 26 June 2019.

13 See Ben Cosgrove, ‘[Faces of the American Dead in Vietnam: One Week’s Toll, June 1969](#)’, *Life*; Sebastian Smee, ‘In Life, as in Art, Every Picture Has Stories to Tell’, *Washington Post*, 23 October 2022.

a global leader, for better or for worse. Now add to that the ‘Inside the Beltway’ machinations of persuasion from the White House to Capitol Hill. The year 1986 corresponded with my first year of study for a doctoral degree in international relations at the American University’s School of International Service in Washington, DC. The US capital city is a centrepiece of propaganda and persuasion with institutions like the Department of State, K Street (shorthand for lobbyists, lawyers, advocacy groups), and the Pentagon, to name a few. Perhaps it was part of the appeal for me. American president Ronald Reagan, former Hollywood actor and California governor, served two terms in office (1981–89). He combined persuasive populist patriotism at home (‘It’s morning again in America’)¹⁴ with propaganda rhetoric and actions that divided public opinion abroad. I lived through a lot of that divided opinion when I was a Fulbright student in the Federal Republic of Germany in the mid 1980s. Reagan was extremely unpopular in Germany among many, especially younger people, who felt that he was capable of setting off a nuclear showdown with the Soviet Union because of his fervent anti-communist stance.

The text *Propaganda and Persuasion* emerged about halfway through Reagan’s tenure, during a rebirth of political propaganda activism for and against the commander-in-chief’s proclivities.¹⁵ Reagan, who was somewhat dubiously acknowledged the ‘Great Communicator’ by Pulitzer Prize-winning columnist Russell Baker of the *New York Times*,¹⁶ had a team of senior advisors embedded in propaganda campaigns from

14 ‘Prouder, Stronger, Better’ was a political campaign television commercial in support of Reagan’s re-election in 1984. It became popularly known as the ‘Morning in America’ ad, based on its opening line, ‘It’s morning again in America.’ It was written and narrated by adman Hal Riney, who also wrote and narrated the ‘Bear in the Woods’ (‘Bear’) ad that referred to the Soviet Union threat. ‘There is a bear in the woods. For some people, the bear is easy to see. Others don’t see it at all. Some people say the bear is tame. Others say it’s vicious and dangerous. Since no one can really be sure who’s right, isn’t it smart to be as strong as the bear? If there is a bear.’

15 Garth S. Jowett and Victoria O’Donnell, *Propaganda and Persuasion* (2nd edn, SAGE, 1992), p. xiii. ‘The first edition was written during a period when the USSR was still the ‘Evil Empire’ described by Ronald Reagan.’

16 See Geoffrey Nunberg, ‘And, Yes, He Was a Great Communicator’, *New York Times*, 13 June 2004; original Observer column, ‘What Great with Whom?’ by Russell Baker, *New York Times*, 18 February 1981.

Hollywood to the Contras in Nicaragua.¹⁷ The mood of the world in the 1980s was shaken by Cold War theories like MAD (mutual assured destruction) that seemed very plausible to end life as we knew it.

As recounted by media studies author Matthew Hays in the *Washington Post*,¹⁸ the Reagan administration reach extended from Washington to Los Angeles to indict a documentary, *If You Love This Planet*, that would go on to receive an Academy Award in 1983 as a consequence of the administration's overreach.¹⁹ The 26-minute film, directed by Canadian filmmaker Terre Nash and produced by Canada's National Film Board, consisted of a talk by Dr Helen Caldicott, an Australian physician and anti-nuclear activist who described the medical implications of nuclear war. To her, the idea of winning a nuclear war, which was touted by Reagan through safeguard initiatives like the Strategic Defense Initiative (nicknamed 'Star Wars'),²⁰ was ludicrous. The Justice Department's labelling of *If You Love This Planet* as 'foreign political propaganda' (that means you, Canada) and conservative efforts to curtail its airing to mass audiences created such a controversy that the film's popularity rose exponentially; in today's lingo, it went viral. Democratic senator Ted Kennedy, who hosted a screening for members of the Congressional Judiciary Committee, said, 'It is one thing for the right wing to say, "Let Reagan be Reagan." But it is a very different thing for them to say "Let Reagan be Orwell."' ²¹ In November 1983 the television film *The Day After* aired about life after a nuclear attack. Produced by the ABC television network, one of the Big 3 news networks at the time, the initial broadcast the Sunday before Thanksgiving Day was watched by

17 On 23 November 1981 President Reagan signed off on a top-secret document, National Security Decision Directive 17 (NSDD-17), which empowered the Central Intelligence Agency (CIA) to recruit and train an initial 500-man force of Nicaraguan rebels to conduct covert actions against the leftist Sandinista regime in Nicaragua. NSDD-17 marked the beginning of official covert support by the Reagan administration for the so-called Contras in their struggle against the Sandinistas. Reagan would later refer to the Contras as 'freedom fighters' in his 1985 State of the Union address, which outlined the Reagan Doctrine.

18 Matthew Hays, 'The Reagan Administration Labeled a Film "propaganda." It Won an Oscar', *Washington Post*, 12 March 2023.

19 Terre Nash, dir. *If You Love This Planet* (National Film Board, 1982).

20 President Reagan proposed the concept of the SDI in a nationwide television address on 23 March 1983.

21 Hays, 'Reagan Administration'.

more than 100 million people.²² Reagan and his wife Nancy screened the film at Camp David and afterwards the president wrote in his diary that it 'left me greatly depressed'. The anti-nuclear war propaganda message moved the persuasive needle in Reagan's second term, which, unlike his first term, was dominated by summits and efforts to cooperate with the Soviet Union's last leader, Mikhail Gorbachev, to end the Cold War or at least reduce the nuclear threat between the US and the USSR.²³

Propaganda and Persuasion began life when Garth Jowett was in touch with Sara Miller McCune, the co-founder of Sage Publishing, after completing a very successful first SAGE book in 1980, *Movies as Mass Communication*, co-authored with James M. Linton.²⁴ Jowett had already established his gravitas in film history with a commissioned book for the American Film Institute in Los Angeles, *Film: The Democratic Art*, published by the mass-market Little, Brown and Company. That tome emerged as the definitive volume on the social history of the movie-going experience and included a chapter on 'Hollywood Goes to War' and the movies as propaganda.²⁵

Propaganda and Persuasion served as the last volume in a SAGE series called People and Communication, which focused on the technology media of the day, including broadcast radio and television, and their effects on children and public affairs.²⁶ The reader benefited from two authors with different specialisations: Jowett in communications history, especially film and popular culture; O'Donnell in persuasion and rhetoric, including television criticism.²⁷ The South African born Jowett earned his

22 *The Day After* was the highest rated television film in US history for nearly three decades, until 2009.

23 The United States and Soviet Union signed the Intermediate-Range Nuclear Forces Treaty in 1987.

24 Sage Publishing, formerly SAGE Publications, is an American independent academic publishing company, founded in 1965 in New York City by Sara Miller McCune and now based in the Newbury Park neighbourhood of Thousand Oaks, California. It marks its sixtieth anniversary in 2025 as an independent academic publisher. For more about McCune and Sage, see group.sagepub.com/people and group.sagepub.com/about

25 Garth S. Jowett, *Film: The Democratic Art* (New York: Little, Brown and Company, 1976).

26 Volume 1 in the People and Communication series: Scott Ward, Daniel B. Wackman, and Ellen Wartella, *How Children Learn to Buy: The Development of Consumer Information-Processing Skills* (SAGE, 1977).

27 SAGE released O'Donnell's textbook *Television Criticism* in three editions.

doctorate from the Annenberg School at the University of Pennsylvania during the twenty-five-year tenure of Dean George Gerbner, one of the leaders in the effects of heavy media usage, particularly television, on developing a mean world syndrome. O'Donnell, a Pennsylvania native, completed her PhD in communications at Penn State University. Before retirement, she was Professor of Communication and Director of the University Honors Program for twelve years at Montana State University, where she also taught a seminar on television criticism for the School of Film and Photography. In the mid 1990s O'Donnell developed a television film for her Montana-affiliate PBS station called *Women, War, and Work: Shaping Space for Productivity in the Shipyards during World War II*, which became the basis of a case study in the third to seventh editions of *Propaganda and Persuasion*.²⁸

Jowett and O'Donnell's text challenged the prevailing propaganda-literature wisdom that the term propaganda could be used as a substitute term like mass persuasion, implying that propaganda is just persuasion on a one-to-many basis.²⁹ Instead, the two concepts needed proper placement along the communication spectrum, which is why the first chapter of all seven editions is the most comprehensive, taking its time to educate the reader on the definitional pattern differences, a few of which I list here:

1. Propaganda is linked to society while persuasion is linked to the individual.
2. Propaganda's different forms include activated ideology in white, grey, or black derivations, in reference to the degree of source revelation and the informational integrity.
3. Successful propaganda is not based on reciprocity, whereas successful persuasion is.

28 See www.montanapbs.org/programs/WomenWarandWork/. The subject of O'Donnell's film is strikingly similar to Terre Nash's doctoral dissertation topic at McGill University, 'Images of Women in NFB Films during World War II and the Post-War Years: 1939-1949'. This review essay is dedicated to the memory of Dr Victoria O'Donnell ([obituary](#)).

29 Jowett and O'Donnell, *Propaganda and Persuasion* (1986), p. 21.

4. With propaganda, the receiver is always at a disadvantage; the sender is advantaged.

Some readers may be a bit perplexed by Jowell and O'Donnell's definitional certainty that propaganda is both deliberate and systematic. 'Deliberate', they write, 'is a strong word meaning "willful, intentional, and premeditated." It implies a sense of careful consideration of all possibilities.' Likewise, 'systematic' is a complement to 'deliberate', 'because it means "precise and methodological, carrying out something with organized regularity."' ³⁰ And yet the authors also acknowledge that 'indirect and unconscious propaganda' is a 'major product' of modern media systems, ³¹ so much so that UNESCO pushed for a New World Information and Communication Order (NWICO) in the late 1970s and 1980s, to promote more balanced news coverage and information flows from less developed countries to more developed countries. ³² That debate was spearheaded by an influential 1980 UNESCO study, *Many Voices, One World*, known also as the MacBride report, so named for Irish Nobel laureate and peace and human rights activist Seán MacBride. While that report and the movement may be long forgotten for the current generation, the idea of indirect and unconscious propaganda in modern media systems is still relevant. In the early days of the Israel-Gaza War in 2023, the *New York Times* media company apologised about its initial reporting of the bombing of a hospital in the Gaza Strip. The paper issued an editorial note that it relied too much on Hamas's immediate claims that the Israeli military was responsible, and the paper did not fact-check those claims. ³³ In short, 'the early versions of the coverage—and the prominence it received in a headline, news alert and social media channels—relied too heavily on claims by Hamas, and did not make clear that those claims could not immediately be verified. The report left readers with an incorrect impression about what was known and how credible the account was.' *Newsweek* opinion writer Matt Robison said,

30 Garth S. Jowett and Victoria O'Donnell, *Propaganda and Persuasion* (4th edn, SAGE, 2006), p. 7.

31 Garth S. Jowett and Victoria O'Donnell, *Propaganda and Persuasion* (3rd edn, SAGE, 1999), p. 146.

32 George Gerbner, Hamid Mowlana, and Kaarle Nordenstreng (eds), *The Global Media Debate: Its Rise, Fall and Renewal* (Norwood, NJ: Ablex, 1993).

33 'Editors' Note: Gaza Hospital Coverage', *New York Times*, 23 October 2023.

‘There was a mainstream media race to the bottom recently, and *The New York Times* was the ringleader. The consequences were immediate, terrible, and may be felt for years to come.’³⁴ This controversy wasn’t new for America’s foremost newspaper of record. In 2004 the *Times* published a *mea culpa* for its complicity in touting, rather than investigating, the Bush administration’s case to invade Iraq.³⁵ Unnamed US intelligence sources and Iraqi defectors shared their intel with reporters, notably Judith Miller, that Iraq was in possession of weapons of mass destruction and that the US military had to act quickly.

The strengths and weaknesses across seven editions of a textbook by Jowett and O’Donnell over the span of several decades offer teachable moments to any practitioner of persuasion or scholar of propaganda. A reviewer of the third edition, R. Lance Holbert, wrote, ‘This text would be much improved if the authors would provide in the final chapter greater detail concerning the impact of the Internet on the practice of propaganda, and its ultimate effectiveness on a mass audience via this form of communication.’³⁶ In hindsight, this seems a fair criticism for the period of the end of one century into another when the third edition was released. However, the first decade of the Internet was more like a freewheeling Wild West. In 1999 there were fewer than 150 million people globally who used the Internet once a week, about half of whom resided in the United States.³⁷ AltaVista was the main search engine, along with Northern Light and HotBot. No Google. Most of us were using dial-up modems to connect, and when connected, we were likely using the information superhighway for less commercial purposes (checking email, message boards, Internet cafes, chat rooms) than we see today.³⁸ It was a decade when politicians, parents, and free speech advocates debated how to handle the Internet’s new digital home in cyberporn, with one Carnegie Mellon research study making the claim that over 83.5 per

34 Matt Robison, ‘[The New York Times Just Destroyed Its Credibility—and Much More: Opinion](#)’, *Newsweek*, 19 October 2023.

35 ‘From the Editors: The Times and Iraq’, *New York Times*, 26 May 2004. See also ‘[The Times and Iraq: A Sample of the Coverage](#)’, *New York Times*.

36 R. Lance Holbert, *Southern Communication Journal* 66 N° 2 (2001): 181–82.

37 Cheri Paquet, ‘Report Counts 147 Million Global Net Users’, *CNN.com*, 12 February 1999.

38 Angus J. Kennedy, *The Rough Guide to the Internet* (1999).

cent of all digitised images in Usenet newsgroups were of porn.³⁹ These statistics were referenced on a sensational cover of *Time* magazine that carried the wide-eyed gaze of a young boy with hands at a computer keyboard.⁴⁰ Unless Jowett and O'Donnell wanted to take a detour through that form of persuasive communication, it was still a bit premature to address the Internet impact on propaganda. A fairer criticism can be made about more recent editions that haven't addressed the propaganda and persuasion context to streaming, social media, artificial intelligence (AI), and big tech platforms like Meta (owner of Facebook, Instagram, Threads, and WhatsApp) and X (formerly Twitter) that monopolise so much user time. In their defence, twenty-first-century technology was not the scholarly focus of either Jowett or O'Donnell, who present content in the tradition of communication historians.

Next Generation *Propaganda and Persuasion*

Garth Jowett invited me as his co-author for a 2025 eighth edition, an invitation I took very seriously from the start. I knew that I was stepping aboard an existing brand textbook platform with its distinctive and highly cited Jowett & O'Donnell definition and model of propaganda. To that end, I do not wish to diminish this brand in any way by taking it in an unexpected and failed new direction, as a Coca-Cola executive once did with a new concoction of a classic drink formula. To my mind the key enduring features of *Propaganda and Persuasion* as a brand are its practical applications, real-world examples, and case studies. Favourite texts become references to be used again and again. They offer the proverbial water from the well. I can turn to them for insight and examples to help make sense of things. That's what this book has meant. Therefore, it is not lost on me that this textbook's durability, if it is to remain relevant into its fifth decade and beyond, has to offer real-world reflections of our ritualised interactions and manifestations

39 Peter H. Lewis, 'Critics Troubled by Computer Study on Pornography', *New York Times*, 3 July 1995.

40 *Time* magazine cover: 'Cyberporn', 3 July 1995; cover story: Philip Elmer-Dewitt, 'Online Erotica: On a Screen Near You', *Time*, 3 July 1995.

of identity, community, and culture. Facebook turns an adult twenty in 2024. TikTok's global application turns a childlike six in 2024; it began exclusively in China in 2016 and went global in 2018. How we define persuasive interactions and propaganda campaigns in the twenty-first century will be dependent on person, platform experience, and mediated exposure, that space between self and gadget or self and screen.

Communication gadgets are so ubiquitous that they are becoming hacks for personal safety and security. In response to rising random crime on subways, a New York City subreddit warns passengers to 'always wear headphones even if there's not music playing. Gives you plausible deniability in the event someone gets in your face so it doesn't seem like you're just ignoring them.' In contrast, whenever I ride the train in Tokyo, I do not have much if any eye contact with people, but not so much for personal safety as cultural norm. The train is remarkably silent, with most of the commuting passengers engaging with their mobile phones or catching sleep. It is considered rude to chat loudly aboard the train. Modern living for many of us is the act of looking down, looking at, scrolling left or right, and consuming visual and word messages and appeals created by humans and machines. We've grown to accept that customer service may not have a person on the other end but rather a friendly chatbot who can engage us in conversational AI. We've grown to accept the world of influencers as much as persons we once defined as influential in our respective genres. In our communications field it may include names like Edward Bernays, Harold Lasswell, Walter Lippman, George Gerbner, and Herbert Schiller, the latter two my academic mentors.

Our social relations are becoming increasingly expanded or contracted through the parasocial (para: literally 'alongside' or 'beside'), offering a pseudo-sense of familiarity and connection with public figures that are distinguished by their one-sided nature. Savvy, as in highly manufactured and manipulated, media and marketing campaigns generate a false sense of belonging and connection. One social scientist, Arthur C. Brooks,

calls these relations ‘imaginary friends for adults’.⁴¹ That faux friend, he says, is like a new addictive fix:

Forming parasocial bonds has never been easier. An emotional connection between fans and celebrities is good business. It encourages people to consume more entertainment and buy more celebrity-endorsed products in order to feel close to their fictional ‘friends.’ Many celebrities will even directly sell ‘personal,’ parasocial interactions through companies such as Cameo. Want Caitlyn Jenner to wish you a happy birthday? That’ll be \$2,500.

The term ‘para-social interaction’ was first noted by two psychiatrists in the mid 1950s⁴² to describe how the audience or spectator responds to the performer on display. The parasocial interaction is defined by a lack of effective reciprocity. There is no mutual development between observer and performer, but rather a fantastical, unreal connection. An early example of a parasocial relation when television was king was the crowned King of Rock and Roll, Elvis Presley, whose music and accompanying hip-shaking gyrations became a national sensation. In the eyes of some parents and pastors, his depraved influence on young people through the small screen was the work of the devil. With a fear that record sales would plummet due to the growing controversy, a Dutch immigrant to America named Andreas Cornelis van Kuijk, who changed his name to Tom Parker and added Colonel for good measure, rebranded his client as a patriotic American. Presley would volunteer to serve his country through a two-year service in the United States Army. Entertainers rebrand themselves when controversy arises. But these are the more innocuous parasocial relations to those that occur in war and conflict.

41 Arthur C. Brooks, ‘Parasocial Relationships Are Just Imaginary Friends for Adults: If You Get Too Invested in a Fake Friendship, Your Real Ones Might Suffer’, *The Atlantic*, 6 April 2023.

42 Donald Horton and Richard R. Wohl, ‘Mass Communication and Para-social Interaction’, *Psychiatry: Journal for the Study of Interpersonal Processes* 19 (1956): 215–29.

Ophir and Gabriel Weimann note that, in the waning years of the twentieth century, few if any terrorist organisations had a web presence. Today terrorists use social media platforms for propaganda purposes, and the way they present the visual content can mimic a high production value newsroom. Like news producers, the terrorists ‘greatly desire the personification of an event. For them, the optimal personal framing presents the terrorists as devoted heroes, victims of the authorities’ atrocities and freedom fighters while their enemies are presented as villains, criminals, the “real terrorists.”⁴³ The hero/villain and perpetrator/victim dichotomy is ripe for mass manipulation and building parasocial relationships that expand their goals. An open-source, unregulated, and unmoderated social media platform like Telegram is an obvious boon to terrorists, but so is a site like the Elon Musk X, formerly Twitter, which has become less moderated under his ownership. Without much moderation from traditional media or social media companies, these spaces are likely to be filled more by malicious actors using advanced AI strategies to generate deep fakes and algorithms that amplify bias, hatred, and, in turn, more violence.

The study of propaganda and persuasion in this new century will need to expand beyond the classroom to take on a public service, public health, and public education sense of urgency. We should not and cannot sideline strategic communications as I’ve seen us so often do in business and academic settings. Nothing short of a propaganda literacy campaign is needed to define the expanded landscape of the information and communication continuum from its best practices to worst applications. Shining a light on the darkness of our era is just one small step. We must also offer positive resolutions that serve as steppingstones to building lasting and reciprocated trust and transparency in human relations. Otherwise we can write off the global commons and global town square.

43 Yotam Ophir and Gabriel Weimann, ‘From Terrorist to Persona: Para-social Interaction and the ETA Website’, *Perspectives on Terrorism* 6 N° 1 (2012): 23–35.

Cracking the Nut in Iraq

A Review Essay by Paul Bell

The Rest is Politics: Leading.
Goalhanger Podcasts, www.goalhangerpodcasts.com/leading

Keywords—*al-Qaeda, definition, effects, Iraq, influence, values, strategic communications, strategic communication*

About the Author

Paul Bell CVO first focused on the application of strategic communications in conflict while a director of the South African commission overseeing the elections which brought Nelson Mandela to power in 1994. Ten years later he took that experience to Iraq, where he worked for US forces during the occupation and established the IOTF. The views expressed are his.

In May 2023 I listened to two of Britain's most prominent political commentators, Alastair Campbell and Rory Stewart, interviewing a former high-ranking government official, Jonathan Powell, for their *Leading* podcast—a spinoff from their highly successful podcast *The Rest Is Politics*. After thirty minutes, the subject of Iraq came up. All three had been closely involved in the 2003 invasion: Powell as chief of staff to then prime minister Tony Blair, and Campbell as Blair's director of communications and strategy. Both had been in the thick of policy- and decision-making at the highest level of government as Britain prepared for war. Stewart's experience had been utterly different; having completed a walking tour of north-central Afghanistan in 2002, he had served as deputy governor of two provinces in the marsh regions of southern

Iraq, confronting the occupation's consequences and the ground truth of security, reconstruction, and peacebuilding in a country hollowed out by oppression, conflict, and now occupation.¹

The question was raised: between the two options, containment or intervention, had it been right to choose the latter? For a minute or two, the discussion was brittle. Powell said he was still wrestling with the issue: there had been no weapons of mass destruction, Coalition forces had failed to restore security, and then they had left before resolving the Sunni-Shia civil war. The outcome had been bad. But worse, Western governments were also learning the wrong lessons: in Libya, bombing from the air but failing to support state and institution building on the ground; in Syria, failing to intervene and simply letting 'this horrific thing happen' (and, which Powell failed to mention, leaving the field to the Russians and the Iranians).

Stewart tore into Powell. Interventionists had been 'unable to distinguish the prudential from the ideological', but had had no moral obligation to do what they could not do. 'It seems completely implausible to me', Stewart said, 'that we ever had the knowledge, the legitimacy, the power to resolve the conflict.' He continued, acidly:

The stupidity of your position is that you think it's enough to make a moral argument in [Bosnia, Kosovo,] or Iraq, and say that the question is 'What difference is there in moral terms between Bosnia, Kosovo, and Iraq?' The fundamental difference is that you couldn't do it in Iraq, and doing something that you can't do causes untold misery. And you were not focused on the practical. You believe that, provided you were righteous, you could say stupid things like containment was fracturing, when it was entirely apparent to *me* that containment would have

1 Stewart's *Occupational Hazards*, published in 2006, is a masterclass in the hazards of foreign military interventions. A former Conservative MP and cabinet minister, he is president of GiveDirectly, a global poverty relief charity.

been infinitely preferable to what happened. Saddam Hussein did not pose an existential threat to global security, you did not need to intervene in 2003, and the world would have been better off had you not done it.

Powell's rejoinder was that he was not making a moral judgement; one of five tests drawn up for Downing Street by military historian Lawrence Freedman had been: is it practical, can you make it work? 'The question is,' Powell said, 'how do you know that until you've actually tried it?'

The exchange, and the display of different temperaments between the two men, was fascinating; Powell the pragmatist, cool under fire, not rising to meet Stewart's ire—skills he has taken from Northern Ireland into other conflict zones; Stewart, passionate, uncompromising, more philosophical than political, and still ablaze with what he had seen and experienced in Iraq and Afghanistan. Between them, they had articulated the core competing arguments in a debate whose failure to resolve has led to consequences: Western irresolution over interventions, inaction through fear of failure and voter disapprobation, and, in the Middle East and Africa, a security vacuum now being filled by paramilitary proxies for hostile state actors.

If Stewart's view is the one he held *at the time*, it was prescient. As to what motivated anti-war demonstrators then—I remember, as a political consultant, making my way through the crowds and the clamour on my way into Parliament—I recall a more principled opposition to the use of military force in general, rather than specific support for Saddam, and a strong dose of anti-Americanism despite 9/11. My diaries of the time reveal how my own views swung with my experience of the occupation. I had supported the invasion before it happened; who can forget the lurid headlines of 24 and 25 September 2003 about Saddam's chemical weapons capability—the *Evening Standard's* '45 minutes from attack' and, the following morning, *The Sun's* 'Brits 45 minutes from doom'? These

are powerful ideas in London, a city of almost 6000 war memorials.² But afterwards, once my colleague Mark Turnbull and I had won a first contract in Iraq for Bell Pottinger Consultants in early 2004 against highly improbable odds, and I was now in theatre fighting the information war as a civilian contractor to the Coalition Provisional Authority (CPA) and later Multi-National Force Iraq (MNF-I), I rethought it completely. We quickly understood that we were there to make the best of a very bad job and we developed one central preoccupation: saving lives. The more successful we were, the fewer people would die. It was that simple.

Twenty years later, questions remain—for us and I believe for the community of strategic communications practitioners of which I remain part. First, did we accomplish anything? Asked through the prism of legitimacy, it's a question we are duty-bound to answer, and I think we did. Our campaigns *did* contribute to ground actions and conditions that reduced the violence. Second, despite the transformative changes wrought since that time to stratcom, and to warfare in all its new forms, by digital and social media, by the industrialisation of disinformation, and more recently by a destructive, deadly European war, did we learn anything that is still of value today?

Our team was the Information Operations Task Force, a unit based at Camp Victory in Baghdad from 2005 to 2011 under the command of Multi-National Corps Iraq, and the largest single military information and psychological operations unit in the history of conflict since World War Two. A great deal has been written by the media, and in official reports and journals, about information and psychological operations in Iraq, not much of it complimentary. But little has been written about IOTF's operations—and what is in the public domain is largely wildly inaccurate and sensationalised. We did not correct the record. We were constrained by security classifications, operational security, and the need to ensure the safety of team members. Moreover, we were of the view that there was little point in feeding the beast—a media that would view our work only through the bifocal lens of the war's generally perceived

2 London Assembly, *Not Forgotten: A Review of London's War Memorials* (July 2009).

illegitimacy and our pecuniary (thus automatically suspect) motives as civilian contractors. We, on the other hand, knew who we were, what we stood for, what we were doing, and why; we had no qualms about the legitimacy and importance of our work. But media minds were made up—about the war and therefore about us—and there was nothing we were going to be able to do to change that.

Some years ago I relented and was interviewed along with an Iraqi colleague by a group of South African filmmakers doing a documentary on Bell Pottinger, the now defunct company which held those Iraq contracts. I agreed to it because I felt that if I did not, they would go ahead with their version of our story anyway and there would be no chance to redress what I felt sure the balance would be. I did it—and no chance became little chance. Hey-ho.

Turnbull and I first arrived in Baghdad in March 2004, a year after the invasion, commissioned by the CPA to produce three commercials, ostensibly to publicise the terms of the Transitional Administrative Law that would provide the legal framework for Iraq's transition to sovereignty and democracy. To support us we had partnered with the Dubai advertising and marketing agency Bates Pan Gulf: we as Bell Pottinger would direct operations, strategy, and client relations, and Bates would provide cultural understanding and make the commercials. We had support on the ground from Brent Balloch and Jack Roe, two young adventurers who had come to Baghdad the year before to make their fortune, and were running, at great personal risk, a string of service and supply operations in the city. Mark and I worked out of the Green Room in the Republican Palace, headquarters of the CPA and Saddam's former executive seat. In July, with our task complete, we were on our way back to London when we were informed that the British government had found money to bridge the continuation of our services, now to be provided to the Iraqi electoral commission in advance of elections scheduled for January 2005. That work was focused on voter education. Performed under the direction of the United Nations electoral team and the International Federation for Electoral Systems, it was formulaic,

unimaginative, and conducted with no sense of either the election's wider import for Iraqis, or their already profound doubts about democracy and their fears that the violence would scupper their opportunity to vote and their purpose in doing so. We would end up dealing with those issues later, once the Americans had found fresh financing and brought us back into the Republican Palace to work for MNF-I.

By 2005 we had built a reputation for making good commercials fast; for our reliable distribution networks, including relations with television stations (which had sprung up like mushrooms after the fall of Saddam and would be our principal route to market throughout our time in Iraq); and for an approach to strategy that was entirely fresh to our military and diplomatic clients. New work began to flow to us from the military information support teams embedded with the US State Department, and from State itself. By the autumn of that year, Iranian-supported Shia militia were 'ethnically cleansing' Sunni neighbourhoods in Baghdad, and al-Qaeda in Iraq (AQI) was car-bombing Baghdad's streets and markets every other day, and terrorising the Sunni tribes of Anbar into an alliance against the US occupiers and the Shia-led government.

Against the backdrop of that blood-drenched melee, the influential Institute for National Strategic Studies at the National Defense University in Washington produced a highly critical report on current US psychological operations. It concluded that, while current psyops could produce modest effects at the tactical level, it lacked an overall national-level theme to guide message formulation. Product approval processes were so slow that they rendered products irrelevant; the product itself was of questionable quality and with uncertain effect; and psyops generally lacked resource and force structure.³ The INSS recommended a push for improvements at the tactical level:

Significant resources (approximately \$100 million annually) and uncertain national-level support would

3 Christopher Lamb, *Review of Psychological Operations: Lessons Learned from Recent Operational Experience* (National Defence University Press, September 2005).

be needed to substantially improve theater PSYOP for general audiences, including a national commitment to organizing for successful strategic communications, a reformed approval process, and contractor support for commercial quality programming. By comparison, improving tactical PSYOP would be less difficult, requiring doctrinal changes and more modest resources to correct shortfalls in intelligence, communications, and production and dissemination capabilities.

Commanding General George Casey went the other way. Opting for action at theatre level, he authorised the establishment of a unit, IOTF, to ‘mount an aggressive advertising and public relations campaign that will accurately inform the Iraqi people of the Coalition’s goals and gain their support’.⁴ Those goals included ‘assisting the people of Iraq in building a free, democratic nation at peace within its borders and with its neighbours, destroying or defeating insurgent forces, and instilling a broad respect for human rights throughout the country’.

We won the IOTF contract in September 2005 and became operational the following month. In broad terms our objectives, as we characterised them in strategic terms, were to ‘build the coalition for peace and undercut the obstructionists’—a construct neatly encapsulated for us by Dr Dana Eyre, a former infantry captain, sociologist, and committed peace-builder who served as our co-chief strategist. We called it ‘the x-chart’ (Figure 1), a simple drawing that made sense of everything we were doing. On one vector, destroying Sunni tribal support for AQI, delegitimising the activities and violence of the Shia militias (the armed wings of their competing political forces), and countering the influence of Iran. On the other vector, promoting unity and reconciliation among Shia and Sunni (including the Kurds), encouraging them to support the development of constitutional, representative government, and keeping

4 Performance Work Statement, PARC-Forces, MNF-I’s contracting arm to civilian contractors, circa August 2005.

them informed of the progress of the security forces in containing the violence. Our third commander, John Sims, a banjo-playing artillery colonel and devout Catholic, called it ‘cracking the nut’.

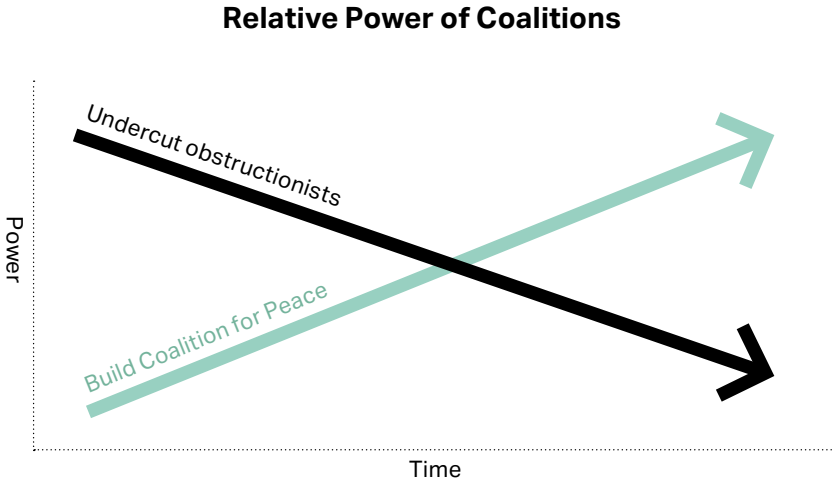


Figure 1. ‘The x-chart’

It was like running a mortar battery. By the time IOTF shut up shop in December 2011, leaving with the last US combat troops to quit Iraq, we had made more than 500 commercials across different contracts and lines of operations, and more than 1700 branded and unbranded news spots, including over 160 weekly news bulletins. We produced 16 episodes of historical documentary, 45 episodes of a political discussion show, and a wide variety of other television content, radio soap operas and call-in shows, supporting print ads, billboards, banners, DVDs, and more than 300 events, activities, and sponsorship and merchandising efforts. We conducted 88 face-to-face public opinion surveys, surveying on average 5000 members of the Iraqi public every month, totalling over 335,000 interviews, and more than 1100 focus groups involving in-depth interviews with over 7500 people. At full stretch our budgets were running at about \$100m a year, alongside the \$60m a year that

US Special Operations Command was spending with us on a three-year campaign to combat recruitment to AQI from elsewhere across the Middle East and North Africa. About 80 per cent of the budget went to media buying, while the rest was spent on research, production, personnel, logistics, and security, all at war-zone pricing.

As the output of one unit within the borders of a single state, this was concentrated psyops on an unprecedented scale. We were just one outfit in the theatre—there were several other US communications contractors operating—but ours was the dominant effort. Each month, at a battle update assessment, the IO commanders would present to successive commanding generals (Petraeus, Odierno, Austin) the fifteen or so products that were currently out there in the information battle space, and usually as many as fourteen would be ours.

What distinguished us from our clients and rivals? First, our fresh perspective. We were not American. We had drunk a little less of the pre-invasion Kool-Aid about culture, ideology, and Islamism. We were less invested in the politics of the US administration and its definitions of victory, but far more so in the pathologies and pathways of reconciliation and peace. And we had new, completely different ideas about the nature and causes of terrorism and the terrorist mindset. Second, we were professional stratcom practitioners with deep roots in political communication, and we introduced into the theatre the disciplines that came with that experience. We knew, for example, that an ill-judged communication could do real damage with an audience, and I immediately introduced what came to be our operating principle number one, *do no harm*—in those days as yet unknown outside the Hippocratic oath. As a matter of course, therefore, we would focus-group any and all products before they were released into the market. That wasn't rocket science, just standard operating practice as far as we were concerned, but to our astonishment we learned we were the only ones doing it! Everyone else, whether junior military psyops troops or civilian contractors (including many with no institutional background in communications), was simply making stuff of the crudest messaging

material and banging it out there with at best a nod from some so-called ‘cultural advisor’, most likely a civilian hired in America on the strength of their Middle Eastern origins, ability to speak Arabic, and hatred of Saddam. Media planning was another area in which we insisted on more science than most, not least because we were accountable for spending millions of US taxpayer dollars each month. Viewership data provided by Iraq’s new media were unreliable at best, and we compensated by developing our own robust analytical methodology, which drew heavily on our routine big-sample quantitative research into viewership patterns.

Most importantly, we paid great attention to strategy, starting with my own simple proposition to our clients, at one of our earliest product presentation meetings: ‘*This is not about you.*’ The statement initially baffled them: what on earth did I mean? Wasn’t this about making the American presence welcome and understood by Iraqis? So sorry, we said, that won’t work; you lost *that* when you bombed Baghdad and occupied Iraq. Instead, we built over time a powerful, overarching sociological and psychological construct that centred on the identities, desires, and fears of our target audience, on the dynamics and drivers of the violence, and on the networks, identities, emotions, narratives, and impulses that might unify diverse groups and interests to produce conditions more amenable to the development of a sustainable peace.

Dana Eyre drove the sociological underpinnings of our conflict analysis. Our other co-chief strategist, the psychoanalyst David Kenning, Belfast born, a student of Spinoza, and himself the survivor of an IRA bomb attack, drove the psychopathology and brand side of it. Through his research and analysis, we understood the conflict to be an asymmetric one in which AQI’s main effort—unlike the Coalition’s—was not, and could not be, in the military and economic spheres: its terrorism was essentially a deadly information operation, so we had to treat it like a commercial brand and attack its legitimacy and credibility.

Early on, we placed *effects* at the heart of our strategy. Messages, we asserted, were not the same as effects; they served the preoccupations of

the messenger. We had to focus on effects in order to give proper weight to the audience, its own preoccupations, and the behavioural changes that Coalition strategy required of Iraqis. The operating corollary to that distinction—which took some swallowing on the part of our clients—was that we would not attribute our products to them. Messages are refracted through the prism of the messenger’s identity, and in Iraq, we told them, that would be the kiss of death for any campaign. They acquiesced: faced with the dawning realisation that their presence was at the very least unwelcome, it made sense—and we followed that policy to the end, developing brands that placed the Iraqi people at the centre of our campaigns. It was their voice, their idea of their best selves, that we gave back to them. Effects were thus central to our working definition of strategic communications—this at a time when the term itself was becoming the subject of early attempts by Western militaries, diplomats, and academics to define it.

To me it seems that what distinguishes our definition⁵ of strategic communications from those that evolved later is its relative professional neutrality. It embraces the notion that every action or statement, or indeed inaction or silence, is a communication to be both received and perceived, interpreted and responded to; a non-kinetic force, attracting and repelling, moving or entrenching its diverse recipients; a force that shapes perceptions, and rounds and squares and angles the emotional and psychological shape of all contested space. It establishes strategic communications as what I believe it to be, and should be regarded as: a discipline. And today I would add, a first-order geopolitical discipline—one that should be central to any decision, be it to move a brigade, dispatch a frigate, launch a drone, build a road, or fund a poetry festival. It is equally critical to war and peace, and yet IOTF’s definition of it is free of specific relationship to the importance of values in the exercise of state power. It is stratcom as a toolbox, equally capable of building, as it were, a bomb or a bicycle. It is a *practitioner’s* definition.

5 Strategic communications: an approach to communications which emphasises (1) the need to place communications effects at the centre of all campaign planning, for all activities (kinetic and non-kinetic), and (2) the need to base all communications activities in an integrated, conditions-based, and systematic campaign plan, in order to shape a climate of emotions, loyalties, narratives, and frames necessary to achieve strategic goals.

This is not to say that IOTF gave no mind to values and ethics: *au contraire*, they were simply separate, but in no way secondary; they lived with us, and in our work, in parallel: we had values, we knew why we were there; *do no harm* was our lighthouse, and that imposed natural limits on our practice. On one occasion we were ordered to make fake AQI DVDs and fit them with digital trackers that would pinpoint a user location and feed it to special forces. We were very uncomfortable with this; we were moving from psyops to deception with potentially direct and immediate lethal outcomes. How to challenge this direct order without seeming to disobey it and appearing to breach contractual obligations? We went through the motions of production, while raising objections to the product's distribution on the grounds that it would be uncontrolled, posing risks to innocent civilians. The project was dropped. It was the only time we ever had to resist a course of action on ethical grounds, although I do not believe our clients had intended, as a matter of policy, to be cavalier about innocent civilian lives. Someone just hadn't thought it through.

We did refuse an order on one other occasion, but that was on tactical grounds. AQI had bombed a wedding party at a hotel in Amman, Jordan, and our client ordered us to edit and distribute footage showing the carnage. We refused, saying it was totally counterproductive and would merely aid AQI's strategy to demoralise the public. And anyway, we told the client, when as many as 250 Iraqis were dying in car bombings in a single day, what did we, safe in Camp Victory, have to teach the public about AQI's barbarity? As though we were some mutinous platoon, we were threatened with being cashiered for disobeying an order. It came to nothing and that command team rotated out a month later. We had some brilliant officers in our time, and two or three very stupid ones too.

IOTF was a unique organism that drew in geniuses and misfits alike. A non-combatant 'fighting unit' in the war for Iraqi hearts and minds, with its own unit insignia and motto, John Sims's 'cracking the nut' (Figure 2), it was overseen by a small military command team headed by a lieutenant colonel, and comprised a core of 75 civilians spanning

Baghdad, Dubai, London, and Washington. In the field were about 250 operatives who delivered film, opinion, intelligence, and logistics from ‘out there’ at great personal risk (we lost two cameramen in a drive-by shooting). We came from everywhere—Iraqis principally, Brits, Indians, Emiratis, Yanks, an Ulsterman, a Syrian, an Afghan, ANZACs, South Africans. Men and women in almost equal number, from diverse backgrounds—army and navy, teaching, documentary-making, the law, political campaigning, market research, peacebuilding, and hard-boiled communicators like Mark Turnbull and me. Escaping the quotidian, the humdrum, the grind. Lured by pay and conditions that reflected the risks of war, by the exhausting immersion that IOTF’s operations demanded, and by the perverse thrill of being occasionally shot at or mortared. A lot of the time we hired on instinct and we had our share of chancers and drips, but in the main the team worked twelve-hour days, religiously flouted the ban on consuming alcohol on the base, played hard, stayed with the unit twice as long as other contractors achieved with their staffs, and produced a body of thought and content that was unrivalled in theatre, and arguably since.



Figure 2. IOTF insignia

As many as six successive command teams rotated through IOTF during its lifetime and we never failed to persuade each of them of the coherence of our strategic approach and analysis. But there was

always a wider client community of soldiers and diplomats—in Iraq, Washington, and Tampa—with whom we had to contend and who, for all their admirable dedication, were simply wrong-headed about the nature of the war, what battlefield it was located on, and what victory meant. They talked hearts and minds but were stuck in a mindset in which sociology was incidental; the psychopathology of terrorism and its performative characteristics were as yet little understood by them, and unexplored; and AQI’s ideology was the supreme driver of the violence. Their core business was, in their words, ‘killing people and breaking things’, and while we were all for taking those same measures against the foot soldiers of an evil, irreconcilable, murderous adversary, we also knew that—as David Kenning so succinctly summarised—ideologies don’t attract minds; minds attract ideologies. And we therefore spent a great deal of time trying to understand why military-age males would, to paraphrase Hamlet, take arms against their sea of troubles, and why their communities might be persuaded or coerced to support them.

We had known from the outset that a psychological war could not be won through logic or argument, but through forms of emotionally rooted persuasion—chipping away at the rigid certainties on which extremist violence depends; framing choices *against* armed groups and *for* the political process; stripping away the attractions of AQI and revealing its true nature as a predator not a protector, and treating similarly the power and rackets of the Shia militias; boosting confidence in the Iraqi security forces; reinforcing as best we could the communalities between Shia and Sunni Iraqis, including their shared experience of pain, or their partly shared fear of Iranian influence; indicating progress where it was to be found but never sugar-coating it (in contrast to what an Iraqi colleague would term the ‘Botox stories’ that characterised US and British-sponsored long-distance information campaigns against ISIS some years later). And all of this designed to reframe perceptions of the conflict in a way that would tend to the reduction of support for armed groups, and to the re-establishment of social and civil order, yet all rooted in a ground truth that Iraqis would recognise, rather than some Pollyanna pabulum that common sense told us they would reject.

Were we just kidding ourselves? Rory Stewart has always been unequivocal. Speaking in the British House of Commons in June 2013,⁶ ten years after his own time in southern Iraq, he called the invasion ‘a failure and a scandal’: ‘However we look at the costs and benefits of what happened there, it was probably the worst British foreign policy decision since the Boer war or the first Anglo-Afghan war of 1839. Never have the British Government made a worse decision.’ He also says he probably would have, wrongly, voted for it at the time.

Where he takes issue with Jonathan Powell and the Blair government’s case for war is not to do with any absence of a moral argument, but with their overreliance on it in the face of what they should have known—but did not—were going to be insuperable difficulties in execution that would turn the entire thing into a very costly travesty of their original intent.

IOTF was not involved in making the case for war; that was before our time. Nor did we, once there, involve ourselves in making the case for occupation; indeed we eschewed it. Instead we were making the case for peace in order to accelerate withdrawal. But one part of Stewart’s statement did pull me up especially short:

The idea—that people living in heavily defended compounds, moving around in armoured vehicles, generally unable to speak a word of any local language, unable to interact with an Iraqi for more than half an hour or an hour at a time, except if surrounded by heavily armed men and operating through translators, could really get a sense of whether Iraq was stabilising or what, to use the Minister’s words, Iraq would be like in 10 years—was of course misleading.

Were *we* guilty of that? In part, yes, and certainly more so in the early days. But it is also the case that our team was heavily staffed by highly

6 ‘[Rory Speaks on the Iraq War](#)’, *Rory Stewart*, 13 June 2013

educated, politically sensitised Iraqis, each with their own, often tragic experiences—the murder and imprisonment of family, the great war with Iran of the early eighties, the flight to exile—of the decades of social upheaval and conflict that preceded the 2003 invasion. Their guidance to us was crucial to everything we did.

And we did *not* have the duty—like Stewart—of writing home to our government with glowing reports of illusory success. Indeed, the product of our continuous research, fed weekly to our military clients, was consistently and painfully realistic about how far Iraq remained from US ambitions for its stability. Our job was to keep pointing our audience in the right direction.

So what *did* we achieve? It is impossible to know precisely. Quantum physicists hunt for atomic particles whose existence is confirmed only in their collision with other particles. Theoretically, we know they exist; they're just damned hard to see. In our case, audience bonding and recall of our products were consistently high by any standard (70–90 per cent), and through our polling we accumulated vast amounts of data about key encouraging shifts in public opinion, including perceptions of AQI's role in civilian deaths, or sentiment with respect to prospects for peaceful settlement and shared government. But the measurement of impact, the extent to which communication in and of itself influences human behaviour, is an inexact science whose value, so far as I can discern, is more to do with holding domestic naysayers at bay on the question of value for money. Also, we could neither clearly disaggregate the effects of our non-kinetic communications from other kinetic factors, nor ever know what *hadn't* happened. How many people had not committed a terrorist act because of some message or idea we had broadcast, or some emotion we had inspired? Such things are unknowable.

But there were glimpses, sparks, meteorites that glowed against the dark and were gone. A day before the election in January 2005, the *London Times* reported (Figure 3) that an ad we had produced two months before had given an Iraqi Air Force colonel a clear plan for how he and

the people on his street would deal with the dangers of intimidation on their way to the polls. We can stake a credible claim to the better than expected turnout at the elections of 2005 (work we did prior to IOTF's establishment), and to the approval by referendum of the constitution negotiated in 2005–06, despite a significant Sunni boycott. We know we contributed to the switch of Sunni tribal allegiances from AQI to the Coalition in Anbar in 2006. This was borne out in captured documents that included AQI complaints to Ahman al-Zawahiri in Afghanistan at the time about the pounding they were receiving from 'American propaganda', and in similar references in subsequent al-Qaeda strategic analyses. And in September 2006, when Sunni tribal leaders announced they would join with the Coalition in the fight against al-Qaeda, we compared their language to that of our commercials in the preceding months, and they were an almost word-for-word match. That switch of allegiance was the hinge on which the success of the surge turned in 2007, reducing the violence. Any more substantive claim regarding the impact of our work on the overall flow of events, especially with reference to reductions



in violence in the Iraq theatre between 2007 and 2011, would depend on deeper research that would nonetheless be subject to all the aforementioned caveats about what we could be sure of. But on the whole, I try to imagine how it might have been had we not been there, jamming the sky with our calls to the courage and decency of ordinary Iraqis.

Figure 3.
News clipping from *The Times* of London, Saturday, 29 January 2005, p. 6. Report by James Hilder and Ali al-Hamdani.

During 2011, as withdrawal approached, I broached with higher command the possibility of keeping a scaled-down version of IOTF going, to preserve the knowledge and systems. This isn't over, I said. Put a small team in Doha. In two years, something else is bound to happen and you're going to need again something of the capability you have developed here over the past eight years. But there was no interest; America was leaving, so it thought. Within two years, ISIS rose like a cobra in the bosom of Syria, sank its fangs into northern Iraq, and hissed at the door to Baghdad—and psyops went back to square one. As though IOTF had never existed.

I took comfort from a note I had in 2019 from Colonel Frank Sobchak, co-author of the US Army official history of the Iraq conflict, which had been published earlier that year. I had written to him seeking advice on a possible research project into IOTF's work. He wrote back: 'Your project is very important and is something that we noted was underrepresented in our work and worthy of its own stand-alone book size effort. The IOTF had a considerable impact and deserves considerable effort to review and establish lessons learned.'

And thus my yesteryear, old-warrior lament that, so many having given so much to this adventure that was so livid and rich and consuming for us all, IOTF passed largely unsung and unrecorded in the annals of information warfare. It was 'MacArthur's Park', melting in the dark; would we ever have that recipe again?

In fact, traces remained. After the 7/7 London Transport bombings of 2005, the British Home Office set up its Research, Information and Communications Unit (RICU) to combat the growing threat of domestic extremism. After eighteen months, it was still lacking in thrust and impact, so the ministry's director of counterterrorism, the late Charles Farr, came to see me. He had heard about IOTF and wanted something of similar design and energy. He also had in mind to hire Richard Chalk, a formidable political campaign organiser whom I had asked to serve as IOTF's first chief of staff, and which he had done with

distinction. Richard duly joined RICU and transformed it, drawing on his experience of IOTF and adapting its core operating principles to the Home Office unit. Notably, too, RICU's work was supported by a commercial operation whose leadership had also had experience of the IOTF operation; I remember walking into its offices in 2015 and feeling some of that old energy. So the recipe did partly survive, with RICU pioneering an always politically sensitive collaboration between the state and civil society organisations, the former providing research, strategy development, and capacity-building, while the latter provided credibility, networks, and civic reach. In the decade that followed Richard's appointment, the British government's anti-extremism communications capability became the envy of its then European partners, providing a model for the development of their own capabilities—thanks to Richard and (I like to think) some of that foundational experience at IOTF.

All that said, none of it saved RICU from the excoriations of *The Guardian* newspaper, which in 2016—at the height of efforts to contain the threat of ISIS in Iraq, Syria, and European capitals—'exposed' the organisation as 'shadowy', lacing its reportage of RICU's attempts to build links with moderate Muslim opinion in Britain, and support their efforts to oppose Islamist extremism, with charges of subterfuge and propaganda, and implications of deception.⁷ These 'revelations' came in the wake of statements by Muslim and allied human-rights interest groups attacking the government's counterterrorism Prevent programme, accusing it of undermining trust between Muslims and other communities, and deepening discrimination against Muslims.⁸

When governments, in the name of national security, move into the territory of domestic covert influence, they inevitably trigger ideological landmines. Public disclosure of such activity draws fire from interest groups that champion opposition to state monitoring, surveillance, the targeting of minorities, and influence programming in general—giving rise to controversy over the ethics, morality, and boundaries of state

7 'Inside RICU, the Shadowy Propaganda Unit Inspired by the Cold War', *The Guardian*, 2 May 2016.

8 Jenny Jones et al., 'Prevent Isn't Making Anyone Safer: It Is Demonsising Muslims and Damaging the Fabric of Trust in Society', letter, *The Guardian*, 10 February 2016.

engagement in the politico-public influence space. Governments may be choosing to try persuasion before they are forced towards coercion, but in this arena they're damned if they do and damned if they don't.

At about the time US combat troops withdrew from Iraq, geopolitical competition seemed generally to change shape—into hybrid war, grey-zone activity, conflict undeclared, everywhere and nowhere. In terms of strategic communications there were big changes too, *inter alia* the hyper-expansion of digital and social media channels, and of support for and engagement through civil society organisations; the increasing sophistication of online micro-targeting and search-and-analysis technologies; a shift in the preoccupations of liberal democratic states from the security threats posed by Islamist-inspired extremism to the threats now posed by Russia-inspired and -sponsored disinformation to their internal socio-political cohesion and that of hybrid democracies in other regions. Then came the invasion of Ukraine, a brutal kinetic slugfest encased in a war of perception and deception whose scale dwarfs Iraq.

In this much-changed landscape, does the IOTF experience offer cause for reflection relative to the practice of strategic communications now? If anything, as strategic communications comes of age in this third decade of the twenty-first century, it raises the question: as a discipline of now first-order geopolitical significance, must stratcom be considered to be inherently rooted in values that protect the legitimacy and integrity of what one might loosely call 'a liberal democratic construct'?

In Iraq, if I thought about values at all, I did so in terms of what I described as our 'licence to operate'—which we had solidly from our military commanders. It was a hot war, an out-and-out bloody, dirty fight, in a single theatre (more or less). Because there was no shortage of money, and social media was not yet a dominant factor,⁹ we could mount an operation at a pace and scale that was about as much as the

9 At the height of operations in 2008–09, social media was growing but had not yet exploded. Although we were interested in expanding into it, we were held back by US law in the shape of the Smith-Mundt Act. It prevented the US public from being exposed to influence operations directed by their government at foreign audiences.

traditional information environment could reasonably absorb, and it was possible to achieve something close to information dominance. But that dominance depended on maintaining that licence; we had, perforce—as I characterised it—to ‘thread the eye of the needle’. Were we ‘doing no harm’? Were our campaigns aligned with end-state objectives and other kinetic efforts? Were our effects realistically defined, with some prospect of measuring them? Did our content and messaging look sufficiently ‘home-grown’; were their language and imagery sufficiently well-rooted in the ground truth, aspirations, and fears of the target audience—and thus recognisable and acceptable to them? Were they acceptable to the host government, to other political parties, or to the media who had to run our content? Had potential collateral effects been properly considered? Was there a risk of blowback? In a country under occupation and racked by civil war, the eye of that needle was small and the thread was thick.

Did we consciously construe our practice of strategic communications as a values-based construct? No. Our values were assumed—present, yes, but distinct from the mechanics of our practice. In our efforts we were bound, separately though not integrally, by the value set and end-state objectives that framed the context of our operations: a safe, stable, internally reconciled Iraq, its people’s needs and desires properly represented in their governance, on the basis of a just, robust political settlement, and a country at peace with its neighbours.

That none of this was attained is an inescapable judgement of history. But do I accept—the question has been put to me—that our operations were aligned with a set of American military precepts that were rejected by much of the population? No, I reject the premise. I repeat, we had come in knowing we had to make the best of a very bad job. We knew the Americans had to get out as much as the Iraqis wanted them out; our job was to help towards that with as little further damage as possible (Figure 4). We were also acutely conscious, as were the American soldiers and diplomats to whom we reported, of the damage that had been done to Iraqi lives and society, and of our obligation to do as much as we could to restore their well-being. In that clear sense, beyond but never absolving



the original sin of invasion and the ignorant assumptions and hubristic geopolitical objectives that had driven it, our work was aligned with what we came to know of the experience, aspirations, and interests of the Iraqi people. And we were able to retrofit that awareness into alignment with the formal end-state objectives of our military client, with the latter's entire endorsement.

Figure 4. The author at 1:30 a.m., 31 January 2005, on the steps of his trailer behind the Republican Palace, Baghdad, celebrating the first election with a plastic cupful of smuggled vodka. Picture by Mark Turnbull.

One of the first things we learned in Iraq was to stop using the word 'democracy', because the idea had been so discredited by the Iraqi experience of having it brutally thrust down their throats by the neoconservative hubris of the Bush administration. That's a big 'value' we pragmatically (nay, sympathetically) dispensed with right away. On the other hand, we never considered disinformation; we wouldn't have dreamt of it. Indeed, even had we considered it to be legitimate, what need was there to lie about al-Qaeda? (As indeed, what need is there, now, to lie about Russia?) Nor did we play any part in military deception strategies. Our single 'deception', if it must be called that, was our policy of not attributing our product to its ultimate owner, the United States, because as the occupying power its brand was a messaging liability. And we were absolutely clear that we were not, and could never be, in the propaganda business—even if the media, through their lens of illegitimacy,

insisted that we were; the very idea turned our stomachs. Had we been ordered to spin Abu Ghraib, for example, the team would have walked.

But we weren't just lucky; we made our own luck. We built a model for our operations that was founded in common sense, cultural knowledge, and acute insight into the nature of the conflict. That it was also morally and ethically sound was rooted in the values we came with, not any *a priori* insistence that stratcom is by nature value-based.

I am wary of defining strategic communications as inherently value-based, of imposing 'civics' on practitioners. There is a risk of establishing a false premise: that 'strategic communicators' must *by definition* operate within a value system, or a specific understanding of how society best functions, a normative framework that 'we' endorse, meaning that those who don't cannot lay claim to practising stratcom. That's too much of a stretch for me. I know too many geopolitical practitioners in my part of the world who very skilfully deploy its arts and are quite ready to serve interests that are antithetical to truth, justice, and the open society; who take the money and run.

I worked for a man who told the *New York Times*, shortly after the firm he founded collapsed in ignominy after a disastrously damaging campaign in South Africa: 'Morality is a job for priests. Not PR men.'¹⁰ One can regard the definition of stratcom through the dual lenses of that aphorism and a counterfactual historical proposition. Imagine, if you will, that the Americans had remained determined to occupy Iraq permanently, colonise it, exploit its oil, and contain Iran. Some other team (I can think of candidates), headed by some other practitioner with different values, would have performed that task, applying all the tools of our trade, including disinformation, polarising narratives, and deception, and it would still have been 'stratcom'. But such a task would not have been for me. Not after spending my formative years in an unjust society, and on a human-rights crusading morning newspaper in Johannesburg. Nor for any of the people who worked with me.

10 Lord Timothy Bell, founder of Bell Pottinger, interview, *New York Times*, 4 February 2018.

But that aphorism does encapsulate what for me is an uncomfortable truth about the essential substance of strategic communications that I am unable to shake: its indifference to morality. Equally capable of being fired by the cop or the killer. Thus, in the sphere of politics and society, I see it in the hands of the actor as a sort of Leatherman, a multipurpose tool that brings to bear all the available options and instruments that might usefully be deployed to influence a target audience and persuade it to a course of action which secures the actor's advantage. Quite what that advantage is, is something else again. All I know is that we are responsible for our choices; we own what we do. We arrive in the action with a discipline in one pocket, and our values in another, whatever those are. We can make a bomb or a bicycle.

Now, where else have I heard that argument? The NRA? The presence of doubt is my only certainty.

Deterrence and Disinformation: Communicating Deterrence in a Non-Linear Media Environment

Nicole Jackson

Keywords—*deterrence, resilience, hybrid threats, disinformation, strategic communications, strategic communication, Canadian foreign policy, wave of deterrence*

About the Author

Nicole J. Jackson is Associate Professor at the School for International Studies, Simon Fraser University, Vancouver. She teaches and researches in the area of security studies and foreign policy analysis, concentrating in particular on Russia and Central Asia. Her first book, *Russian Foreign Policy and the CIS: Theories, Debates and Actions*, examined Russian ideas and debates over military involvement in Georgia, Moldova, and Tajikistan. Most of her early research focuses on Russia's involvement in the post-Soviet space, and includes the securitisation of trafficking in Central Asia, Russia's policies towards Central Asia, and Russia's involvement in regional organisations. More recently she has written on NATO and Canadian approaches to hybrid threats and mis/disinformation, and more specifically within the context of the Russia-Ukraine war.

Abstract

This paper investigates how the strategy of deterrence is relevant to understanding responses to disinformation in general, and in the case of Canada in 2014–23. First, it argues that extending a wide lens of deterrence to hybrid threats, including disinformation, highlights many

options to deter by denial (mostly resilience) and by imposing widely defined ‘costs and punishments’, and reveals strengths and limits of both. Second, it shows that Canada’s efforts have intensified and shifted over time, resulting in a security and foreign policy approach focused on resilience to deny negative effects, and the imposition of costs and punishments to dissuade harmful actions. Third, it highlights benefits and limits of extending deterrence to disinformation in general and in the case of Canada. It suggests that deterrence principles and practices can further adapt to today’s non-linear information environment by engaging with the emerging academic field of strategic communications. In sum, the paper extends the literature on deterrence to disinformation, adds empirical knowledge about the evolution of the Canadian government’s efforts, and develops key critiques based on its findings. Ultimately, it suggests scholars conceptualise a ‘sixth wave of deterrence’ where the deterrence of complex challenges is communicated more strategically and long term within a contextualised, holistic, and ethically grounded approach.

Adapting Deterrence to Disinformation in a Complex Information Environment: Deterrence as Strategic Communications in a ‘Sixth Wave of Deterrence’

Summary Introduction

This article¹ considers how the concept and practice of deterrence is applicable to disinformation, based on a case study of Canada’s efforts to deter foreign state disinformation 2014-23.² It examines and assesses how the Canadian federal government’s foreign and security responses

1 I gratefully acknowledge the helpful comments from two anonymous academic referees and the editor of the journal.

2 The contested nature and definition of disinformation is explored below. Foreign disinformation in this paper is understood to be manipulative, intentional, and coordinated. The focus here is on state and state-affiliated actors; however, the study does not dismiss the role of ‘lone wolf’ disinformers or state-inspired and -recycled mis/disinformation (the line between which is often blurred, as it is between domestic and foreign).

have evolved through the widening lens of ‘deterrence’, revealing options, strengths, and limits. It asks whether deterrence has been stretched too far, and what, if any, further adaptations are needed in today’s complex and non-linear information environment.

The wider context of the paper includes growing governmental and public concern around the globe about mis/disinformation and foreign interference. An increasingly crowded and contested information ecosystem is now widely understood to provide not only opportunities for, but also challenges to, individual, national, and transnational security. Growing awareness of challenges that may arise from the rapid and global proliferation of mis/disinformation has spawned an expanding and transnational counter-disinformation complex, including public, private, and civilian actors.

In Canada the government has taken a leading role as one of the key Canadian actors within this burgeoning counter-disinformation complex. Since 2014, the government has publicly addressed proven and perceived concerns (most prominently coming from Russia, China, Iran, former President Trump, and right-wing extremists). As official rhetoric about mis/disinformation has increased and taken on new urgency, myriad ad hoc actions have resulted in response.³ Most recently, many events have further heightened official rhetoric. These include the global pandemic, the Ottawa Freedom Convoy protests,⁴ Russia’s war in Ukraine in 2022–23, and allegations about China’s disinformation and attempts at interference in Canadian elections of 2019 and 2021.⁵ All have prompted further alarm as well as providing more evidence of the significance, harmful negative effects, and complexity of the challenge.

3 Nicole Jackson, ‘The Canadian Government’s Response to Foreign Disinformation: Rhetoric, Stated Policy Intentions, and Practices’, *International Journal* 77 N° 2 (2022): 544–63.

4 These were a series of protests and blockades over COVID-19 vaccine mandates and restrictions that took place in January and February 2022 in central Ottawa.

5 In 2023 leaked Canadian Security and Intelligence Service reports alleged China’s interference. ‘Why I Blew the Whistle on Chinese Interference in Canadian Elections’, *Globe and Mail*, 17 March 2023 [accessed 16 May 2023].

To investigate how the Canadian government has responded to foreign state-sponsored disinformation through foreign and security policy,⁶ this paper focuses on the broad evolution of its responses over the period 2014–2023. The year 2014 was chosen because Russia’s ‘hybrid’ invasion of Crimea at that time was the first of many events that played a major role in inciting the current widespread attention to state disinformation and denial.⁷ The paper focuses on foreign state disinformation, while acknowledging that the line between state-directed, promoted, or affiliated disinformation can be contentious, and that foreign disinformation can be recycled as domestic mis/disinformation. Despite a legion of studies on disinformation in general, and many recent analyses on Canada in particular, there is little academic literature that analyses the Canadian government’s foreign and security overall *responses* to the broad spectrum of mis/disinformation, or to more specific disinformation campaigns, throughout this time period.⁸ In part, this reflects the fact that many broader questions and debates remain regarding the multifaceted nature of disinformation, and which actors (government, private, civilian) should respond.⁹

-
- 6 This paper does not focus on the actions taken in other areas of Canadian federal government response, nor specific actions by private actors and civilians; however, it does mention areas of collaboration with other actors.
- 7 Russia’s annexation of Crimea in 2014 predated Russia’s widely publicised and alleged mis/disinformation and that of other states (e.g. China, Iran) and actors. In the prominent case of Russia, major allegations post 2014 included its global electoral interferences, beginning with the 2016 US presidential election and the 2016 Brexit campaign, followed by the 2018 Cambridge Analytica data breach scandal.
- 8 For an overview of the period 2014–20, see Jackson, ‘Canadian Government’s Response’. A few policy papers have looked at specific Canadian government departments’ policy: Timothy Caines, *Russian Menace: Is the Canadian Government Capable of Countering Russian Disinformation?*, Canadian Forces College, May 2019; Tej Heer, Charlee Heath, Kimberly Girling and Emma Bugg, *Misinformation in Canada: Research and Policy Options*, Evidence for Democracy, 2021; Brett Boudreau, *The Rise and Fall of Military Strategic Communications at National Defence, 2015–2021: A Cautionary Tale for Canada and NATO, and a Roadmap for Reform*, Canadian Global Affairs Institute, May 2022; Blair Maddock-Ferrie, ‘A Policy Proposal for the Canadian Government to Counter Disinformation through Collaboration’, JCSP, *Federalism-E* 23, 2022.
- 9 There is an extensive literature on this. See, for example, C. Sample, J. McAlaney, J.Z. Bakdash and H. Thackray, ‘A Cultural Explanation of Social Media Manipulators’, *Journal of Information Warfare* 17 N° 4 (2018): 56–71; C. Bjola and K. Papadakis, ‘Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience’, *Cambridge Review of International Affairs* 33 N° 5 (2020): 638–66; Giselle Rampersad and Turki Althiyabi, ‘Fake News: Acceptance by Demographics and Culture on Social Media’, *Journal of Information Technology & Politics* 17 N° 1 (2020): 1–11; M. Gregor and P. Mlejnková, *Challenging Online Propaganda and Disinformation in the 21st Century* (New York: Palgrave MacMillan, 2021).

This paper is also unique in that it addresses this academic literature gap by reviewing Canadian responses through the lens of ‘deterrence’.¹⁰ There is a multidisciplinary canon of literature on deterrence that is very controversial. However, within the past decade, international relations (IR) scholars have been ‘rediscovering’ the concept and applying it to a range of non-traditional (not nuclear or conventional military) challenges. Using a similar logic, this paper extends this literature by considering whether, and how, the more recent conceptual ‘broadening’ of deterrence to non-military issues has relevance for analysing responses to disinformation. In particular it asks whether, and how, a broad lens of deterrence is applicable to understanding disinformation and what it reveals about possible responses. It also asks how the Canadian government has attempted to respond to disinformation from 2014 to 2023 when analysed through this wider lens of deterrence. Third, it asks what the case study tells us about deterrence today, its limits, and what further adaptations may be needed.

To address these questions the paper uses deductive methods, reviewing recent IR literature on ‘deterrence’ in non-military areas,¹¹ including towards hybrid threats¹² to show how scholars’ insights can be adopted to clarify and critique efforts to deter disinformation. It categorises responses to non-military challenges, and specifically to disinformation, within two wide categories: ‘deterrence by denial’ (mostly through ‘resilience’) and ‘deterrence by punishment’ or ‘imposing costs’, and borrows from the broader deterrence literature to critique their overall strengths and limits. Next, the paper examines how Canada’s major government foreign and security responses to disinformation from 2014 to 2023 fit within these categories to discover what adopting a wide lens of deterrence reveals

- 10 The definition of deterrence is explored below. In essence, deterrence aims to prevention action by convincing a potential adversary that the costs or results of their actions will outweigh any potential gains. Glenn Snyder, *Deterrence and Defense: Towards a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961).
- 11 Due to scope limitations, key arguments in the literature over the past decade, 2014–24, are examined. The paper does not review the entire canons of deterrence and disinformation literatures, nor does it attempt to provide a thorough examination of every single policy and action, nor their effectiveness.
- 12 The definition of hybrid threats is contentious, but they are generally understood as ambiguous and blended challenges that include coordinated military and non-military activities that may occur across the different ‘domains’.

about the responses and their evolution. This section gives examples of the major (not all) policies and actions taken by key foreign and security government departments and agencies dealing with disinformation.

As a result, the paper shows that analysing (responses to) disinformation through a broad lens of deterrence clarifies many options in the area of deterrence by ‘denial’ and by ‘costs and punishments’. It also highlights lessons learnt from the broader literature on non-military threats. These include the importance of creating an ‘illusion’ of deterrence, of taking small steps over time, of countering the broader strategy, and the importance of understanding actors’ specific motives and context. They also include the caution that ‘absolute deterrence’ is rarely, if ever, possible (let alone when applied to disinformation), and that governments would benefit from playing a more collaborative role, with individuals and society leading many responses.

The paper also offers an original and nuanced explanation as to how the Canadian government has attempted to respond over time, while offering key critiques drawn from the literature. It argues that Canada has pursued many different options to deter disinformation, beginning with a focus on resilience—including technical solutions aimed at making (direct) access more difficult and efforts to ‘deny’ the strategy or lessen any political and cognitive ‘wins’. Over time the government has taken further actions to increase resilience (its ability to protect and to recover from shocks) but also to deter by imposing widely defined punishments and costs, for example by sanctioning Russian ‘disinformation agents’, and further exposing and delegitimising ‘bad behaviour’.

Third, the paper extrapolates from the case study to highlight benefits and limits of extending deterrence to disinformation in the case of Canada, and in general. It suggests that the principles and practices of deterrence require further adaptation in a complex media environment, and that research in the emerging academic field of strategic communications (SC) might strengthen the arguments of those who call for a more ‘inclusive’ or ‘total’ definition. Engagement with this literature gives rise to the possibility

of a ‘sixth wave’ in which deterrence is communicated more strategically and within a contextualised, holistic, and ethically grounded approach.

The paper is organised in four parts. First, it briefly clarifies definitional challenges. Second, it looks at how recent IR literature has examined deterrence in relation to other non-military (or cross-domain) issues, including hybrid challenges, and shows how those insights may be applied to disinformation. Third, it categorises the Canadian government’s attempts to deter foreign strategic disinformation and explains how they have evolved from 2014 until 2023. Fourth, it considers what Canada’s actions can tell us about the conceptual and practical widening of deterrence to disinformation, and suggests further adaptation is necessary in a non-linear media environment.

Defining and Managing a Complex Challenge

To begin, the paper acknowledges that there are many challenges to defining disinformation and responding to it. Definitional and practical scope complexity and ambiguity plague debates over whether governments, and other actors, can or should ‘deter’ which exact challenge, and by what means. This paper adopts a common definition of disinformation: the deliberate dissemination of *intentionally* false or inaccurate information that is meant to *harm*, as opposed to ‘misinformation’, which is the act of spreading false information unintentionally, including when intent cannot be determined.¹³

13 There have been numerous academic (and other) attempts to define disinformation, yet controversies remain. For academic discussions, see, for example, Shashi Jayakumar, Benjamin Ang, and Nur Diyanah Anwar (eds), *Disinformation and Fake News* (London: Palgrave Macmillan, 2021); Caroline Jack, *Lexicon of Lies: Terms for Problematic Information*, Data and Society Research Institute, 2017; Dean Jackson, ‘Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation and “Fake News”’, National Endowment for Democracy (NED), 17 October 2017; Alexander Lanoszka, ‘Disinformation in International Politics’, *European Journal of International Security* 4 N° 2 (2019): 227–48; Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe Report, 2017; Emily K. Vraga and Leticia Bode, ‘Defining Misinformation and Understanding Its Bounded Nature: Using Expertise and Evidence for Describing Misinformation’, *Political Communication* 37 N° 1 (2020): 136–44.

Of course, whether an information campaign edges over from ‘persuasion’ to being ‘deliberatively manipulative’ or ‘deceptive’ can sometimes be a matter of perspective, and what constitutes harm can be widely interpreted. Where some may see a healthy pluralism of views, others might perceive, for example, controversial, misguided, ignorant, or dangerous views. Harmful disinformation may include ill-intentioned attempts to manipulate emotions, to confuse, or to degrade trust. It may take the form of language that instigates violence, towards certain groups or their interests, or more broadly rhetoric that has the potential to threaten national security or damage democracy and its institutions. One of the greatest challenges for those considering whether and how to respond to deliberate and strategic disinformation is that it can be, wittingly or unwittingly, repeated and ‘laundered’, by which its sources are hidden (or made more difficult to discover).¹⁴ Disinformation is thus turned into misinformation, but the original intention and possibility to harm may still exist and be even harder to counter. Governments’ considerations may be further complicated by an often blurred line between disinformation and a variety of frequently related activities such as cyberattacks, leaks, corruption, and other ‘interferences’ that also need to be managed.

This complexity and ambiguity help to explain why governments such as Canada’s (as well as other actors) often use loose definitions as they confront a broad spectrum of misinformation and disinformation, and rhetorically and practically link disinformation with other malign activities and interferences.¹⁵ Governments generalise to capture and address accurately a spectrum of mis/disinformation and related phenomena. For example, the European Union (EU) has adopted the term ‘foreign information manipulation and interference’ (FIMI).¹⁶ The challenge for

14 Joshua Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation, March 2018.

15 Jackson, ‘Canadian Government’s Response’.

16 FIMI is a ‘mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory’. European Union, ‘Tackling Disinformation, Foreign Information Manipulation and Interference’, EU External Action, 2021.

democratic governments is that they must also contextualise and decide whether and when to respond to specific actors and their activities and intentions, as well as convince the public that they are acting in its best interest.

Beginning with the assumption that there are many uncertainties and controversies facing governments in responding to disinformation, can the concept of ‘deterrence’ (in IR literature) help to clarify options to respond and their strengths and limits?

The Widening of Deterrence and Responses to Disinformation

The traditional military understanding of deterrence is based on the idea that a potential aggressor’s cost–benefit calculation might be influenced, for example, by the threat of a punitive response (deterrence by punishment) or by the realisation that the defender’s preparations are so advanced or effective (deterrence by denial) that the costs of carrying out the aggression would be too great.¹⁷ Of course, when applied to ‘disinformation’ the traditional logic of deterrence, which is already controversial, is further complicated. In fact, many would reflexively argue that deterrence has little or no place in a discussion about (dis)information. They might equate deterrence solely with the traditional military concept of deterrence, or with nuclear deterrence and the concept of ‘mutually assured destruction’ as practised during the Cold War.¹⁸ For others, deterrence may be an imperial or colonial justification for Western military bases and actions abroad.

17 Snyder, *Deterrence and Defense*.

18 Michael MccGwire, ‘Deterrence: The Problem—Not the Solution’, *International Affairs* 62 N° 1 (1985): 55–70.

Yet the academic concept, theory, and practice of deterrence have evolved, and a growing scholarly and non-conventional military ‘cross-domain’¹⁹ areas such as cyber, space, the economy, and approaching (a subset of) ‘hybrid’ (i.e. ambiguous and blended military and non-military) challenges.²⁰ The following section will review this conceptual stretching of deterrence and relate it to disinformation. This reveals many options for how to deter disinformation within two main categories: technical and strategic ‘deterrence by denial’ (resilience) and deterrence ‘by punishment’ or ‘increasing costs’. This section also highlights some other strengths and limits from the widening of deterrence to other (non-military) areas that will then be applied to the case of Canada.

‘Deterrence by Denial’ and Disinformation: Building Technical and Strategic Resilience

Both the theory and practice of deterrence have evolved considerably over time.²¹ The so-called ‘fourth wave’ of deterrence began at the end of the Cold War, when threats came to be perceived as more uncertain

-
- 19 D. Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy* (Paris: Security Studies Center, 2015); A. Brantly, *Back to Reality: Cross Domain Deterrence and Cyberspace* (Boston: Virginia Tech, 2018); J.R. Lindsay and E.A. Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019); T. Stevens, ‘A Cyberwar of Ideas? Deterrence and Norms in Cyberspace’, *Contemporary Security Policy* 33 No 1(2012): 148–70; Eugenio Lilli, ‘Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence’, *Contemporary Security Policy* 42 No 2 (2021): 163–88; Tim Sweijs and Samuel Zilincik, ‘The Essence of Cross-Domain Deterrence’, in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the Twenty-First Century—Insights from Theory and Practice*, Frans Osinga and Tim Sweijs (eds), (The Hague: T.M.C. Asser: 2021), pp. 129–58; King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica: RAND Corporation, 2018).
- 20 Tim Sweijs and S. Zilincik, *Cross Domain Deterrence and Hybrid Conflict* (The Hague: The Hague Centre for Strategic Studies, 2019); P. Cullen and N. Wegge, *Countering Hybrid Warfare* (Shrivenham, UK: Development, Concepts and Doctrine Centre, 2019); D. Stoker and C. Whiteside, ‘Blurred Lines: Grey-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking’, *Naval War College Review* 73 (2020): 1–37; N. Jackson, ‘Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO’, *Journal of Military and Strategic Studies* 19 No 4 (2019): 104–25; Vytautas Keršanskas, *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats*, Hybrid CoE Paper 2, March 2020; Sean Monaghan, *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice*, Hybrid CoE Paper 12, March 2022.
- 21 Patrick M. Morgan, ‘The State of Deterrence in International Politics Today’, *Contemporary Security Policy* 33 No 1 (2012): 85–107.

and less predictable.²² Many scholars have since written about a new, more complex, and less state-centric environment defined by asymmetric challenges beyond more traditional military ones. Today, some scholars argue that we are in a ‘fifth wave’ of deterrence, where these more ambiguous challenges are undermining the key tenets of deterrence (capability, credibility, and communication).²³ There is therefore a need to *prevent* through credible threats (to inform and convince adversaries that the costs of their objectives are too high) *and* through defensive protection or ‘resilience’ to address vulnerabilities. Strengthening resilience is understood as a long-term approach, for example to build strong and adaptive infrastructure, to ensure social cohesion, and to sustain trust in government. Evolving perceptions of challenges and the more ambiguous or hybrid nature of threats and aggressions are understood to be leading to more diffuse responses through new or non-traditional networks, as opposed to hierarchical and state-centred approaches.²⁴

‘Resilience’ in cross-domain areas is conceptualised as an important part of both technical and strategic ‘deterrence by denial’.²⁵ The logic is that to increase resilience not only mitigates possible harmful effects of hostile influence, but also changes adversaries’ cost–benefit analysis by denying them technical or strategic and political benefits. In *strategic* ‘deterrence by denial’, the strategic or political impact is absorbed with no long-lasting result, as opposed to *technical* ‘deterrence by denial’, where direct impact is denied. Some scholars advocate for both physical *and* social resilience to deter terrorist attacks. Gearson, for example, argues

22 Jervis looked at the idea of ‘waves’ in deterrence. Robert Jervis, ‘Deterrence Theory Revisited’, *World Politics* 31 N° 2 (1979): 289–324. The first three waves were state centric, concerned with military strategic issues. For a review of the ‘fourth wave’ see J.W. Knopf, ‘The Fourth Wave in Deterrence Research’, *Contemporary Security Policy* 31 N° 1 (2010): 1–33.

23 T. Prior, ‘Resilience: The “Fifth Wave” in the Evolution of Deterrence’, *Strategic Trends: Key Developments in Global Affairs* (ETH Zurich: Center for Security Studies, 2018); Osinga, Frans, and Tim Sweijts (eds), *NL ARMS Netherlands Annual Review of Military Studies 2020* (The Hague: T.M.C. Asser, 2021), 524–29; Michael Ruhle, ‘In Defense of Deterrence’, *Information Series*, National Institute for Public Policy, N° 457 (27 April 2020); Monaghan, *Deterring Hybrid Threats*.

24 Jackson, ‘Deterrence, Resilience and Hybrid Wars’.

25 Uwe Hartmann, *The Evolution of the Hybrid Threat, and Resilience as a Countermeasure* (Zurich: Center for Security Studies, 2017). See also A. Hellman, *How Has European Geostrategic Thinking towards Russia Shifted since 2014?*, Euro-Atlantic Security Policy Brief, European Leadership Network, 2019.

that both kinds of ‘deterrence by denial’ may be necessary to deter terrorist attacks.²⁶

Applied to the case of disinformation, technical denial could include, for example, bolstering cyber defences and other technical capabilities, or shutting down or denying access to a news platform or outlet understood to be spreading disinformation. In turn, strategic denial could include (credible) actions to deny objectives, for example by protecting the ‘psychological realm’ through education and by fostering critical thinking, or through the media to develop fact-checking or pre-bunking. These efforts could also include actions to strengthen democratic institutions and other steps to increase trust in governments (which are thought to be the targets of some disinformation campaigns). Whether an adversary’s strategy is to gain ‘information dominance’ to shape perceptions or to obfuscate the truth, these acts help to show that society can ‘keep going’ physically and psychologically, and that democratic institutions function and leaders can make informed decisions, despite any disinformation and related confusion. In other words, they may help to ‘maintain deterrence’.²⁷ The major critique, however, is that deterrence, including deterrence by denial, is predicated on inflicting some cost and the clear identification of the adversary. Yet, in the information realm, it is often hard to identify actors (especially as disinformation is turned into misinformation and produced at such a large scale) and to impose costs.

The literature that focuses on deterrence in the so-called ‘grey zone’ between peace and war also applies the logic of ‘deterrence by resilience’ to ‘hybrid threats’ in general.²⁸ The contested ‘hybrid warfare’ paradigm perceives (some) disinformation as part of an ambiguous or blended conflict or one of multiple instruments that may be used in a synchronised ‘attack’ and tailored to specific vulnerabilities.²⁹ Either way it is understood

26 John Gearson, ‘Deterring Conventional Terrorism: From Punishment to Denial and Resilience’, *Contemporary Security Policy* 33 № 1 (2012): 171–98.

27 Colin S. Gray, *Maintaining Effective Deterrence* (US Army War College Press, 2003).

28 For a recent review, see Monaghan, *Deterring Hybrid Threats*.

29 Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007). For a review, see Robert Johnson, ‘Hybrid War and Its Countermeasures: A Critique of the Literature’, *Small Wars and Insurgencies* 29 № 1 (2018): 141–68; Monaghan, *Deterring Hybrid Threats*.

as deliberate and strategic, but also including elements of uncertainty and deniability. Scholars writing on hybrid threats advocate for greater resilience in face of such synchronised and ‘below the threshold of detection and attribution’ activities. They propose coordinated responses to increase technical and strategic denial, with governments, private actors, and civilians working together at the domestic and/or global level.³⁰ Efforts to deter disinformation through resilience could include coordinating across different areas, including: the political/institutional (to secure elections and to increase trust in democratic institutions), the military (to improve the communication of its messages, i.e. its SC), infrastructure (to bolster physical or digital infrastructure), the social (to increase awareness), and information (to govern platforms or regulate media) at home and abroad.³¹ These actions to strengthen resilience would (better) prepare governments and societies and aim to convince actors (adversaries) of the futilities of their efforts, in this case to engage in strategic disinformation.³² Of course, how exactly to achieve sufficient strategic credibility needed to deter, and how to know when this has been achieved, would remain a major challenge in addressing disinformation—just as it is when trying to deter other behaviour or hybrid activities. And the questions of ‘costs’ and ‘perceptions’ become even more controversial in hybrid wars or activities.

In sum, the conceptual widening of ‘deterrence’ to include strengthening resilience to cross-domain challenges, including to hybrid threats, helpfully points to a wide range of possible non-traditional means of responses (in general and in response to disinformation). Some scholars argue that the ‘widening’ alters too much the traditional logic and practice of deterrence, while others conclude that it adds little new.³³ Similarly,

30 Wojciech Lorenz, ‘The Evolution of Deterrence: From Cold War to Hybrid War’, *Polish Quarterly of International Affairs* 2 (2017): 22–37; A.S. Wilner, ‘Cyber Deterrence and Critical Infrastructure Protection: Expectation, Application and Limitation’, *Comparative Strategy* 36 No 4 (2017): 309–18; Mikael Wigell, Harri Mikkola, and Tapio Juntunen, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*, European Parliament, May 2021; Elisabeth Braw, *The Defender’s Dilemma: Identifying and Deterring Gray-Zone Aggression* (American Enterprise Institute, 2021).

31 S. Monaghan (ed.), *MCDC Countering Hybrid Warfare: A Multinational Capability Development Campaign Project*, Countering Hybrid Warfare Project, 2019.

32 Sweijs and Zilincik, ‘Essence of Cross-Domain Deterrence’.

33 Lindsay and Gartzke, *Cross-Domain Deterrence*.

the concept of ‘resilience’ significantly alters the focus of traditional military deterrence responses. It can be criticised for encompassing too many activities to be analytically or practically helpful. Resilience can also be considered too imprecise a concept to use in crafting policy, in part because it suggests responses that both maintain the status quo and allow for change.³⁴

Nevertheless, in practice, and facing the rapidly evolving and increasingly global reach of some ‘hybrid threats’ such as strategic disinformation, Western governments and organisations have called for strengthening domestic and global resilience as means to ‘deter’ activities across domains, including within the ‘grey zone’. The UK government, for example, has officially interpreted the term ‘deterrence’ very widely to include defensive resilience measures, reasoning that capable and resilient governance ‘raises the price of hybrid aggression and reduces its chances for success’.³⁵ The 2022 US National Security Strategy includes the need to ‘bolster resilience and adaptability to future shocks and changing circumstances in the “grey zone” of conflict’ as part of a holistic approach to ‘integrated deterrence’ to ‘credibly deter aggression’.³⁶ Similarly, NATO has for many years called for ‘more resilience’, and in its 2021 ‘Strengthened Resilience Commitment’ called for a ‘further strengthening’ of national and collective resilience, which are ‘an essential basis for credible deterrence and defence’.³⁷ This increasing use of the rhetoric of resilience in Western security and defence thinking has occurred while many domestic resilience indicators have dramatically decreased in some Western countries. This invites the question of whether a real decline in resilience has informed many governments’ more ‘total’ or ‘inclusive’ concept of deterrence, or whether the (academic and governmental) widening of the concept of deterrence (to parts of society not traditionally perceived as exposed to or part of the ‘strategic struggle’) creates an impression that resilience has dramatically decreased.

34 P. Bourbeau and C. Ryan, ‘Resilience, Resistance, Infrapolitics and Enmeshment’, *European Journal of International Relations* 24 N° 1 (2017): 221–39.

35 United Kingdom, Ministry of Defence, *Joint Doctrine Note 1/19: Deterrence. The Defence Contribution*, DCDC, 2019, 40–41.

36 United States, *National Security Strategy*, October 2022.

37 NATO, ‘*Strengthened Resilience Commitment*’, 14 June 2021.

Below I examine how the concept and practice of deterrence has been further adapted, or ‘broadened’, beyond resilience to also include a wide range of non-traditional costs and punishments.

Deterrence of Disinformation through (Widely Defined) Costs and Punishments

The more traditional concepts of deterrence ‘by punishment’ and deterrence ‘by increasing costs’ (as well as the more proactive ‘compellence’³⁸) have also been extended to ‘cross-domain’ challenges.³⁹ In other words, just as the logic of ‘deterrence by denial’ has been applied to other domains, so has the logic of making punishments or costs outweigh benefits been applied in a variety of areas outside traditional military concerns. Furthermore, the traditional understandings of costs and punishments have been expanded, to include the role of identity and belief systems in the cost–benefit analysis. Research examines the benefits of increasing the *social costs* of norms, through the ‘calling out’ of bad behaviour, and of increasing the *negative costs* through ‘deterrence by delegitimation’; that is, by imposing or augmenting reputational costs to incentivise restraint.⁴⁰ Further controversially stretching the concept of deterrence, scholars have examined how positive *incentives* can play a role in disincentivising attacks, for example by fostering states’ interdependence through ‘deterrence by entanglement’ within organisations or groups.⁴¹

Applied to disinformation, these new understandings provide further options for how to ‘deter’ beyond focusing on denial and resilience, and based on more than the traditional understanding of costs and

38 T. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

39 Sweijs and Zilincik, ‘Essence of Cross-Domain Deterrence’.

40 Alex S. Wilner, ‘Deterring the Undeterrable: Coercion, Denial, and Delegitimation in Counterterrorism’, *Journal of Strategic Studies* 34 No 1 (2011): 3–37; S. Wilner, ‘Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far’, *New York University Journal of International Law and Politics* 47 (2014): 439–62.

41 A. Brantly, *Conceptualizing Cyber Deterrence by Entanglement* (Rochester, NY: Social Science Research Network, 2018).

punishments. These include not only military means (kinetic and non-kinetic), but also, for example, political means (travel restrictions, expulsions of diplomats), economic means (sanctions, financial penalties), civil means (public shaming and blaming), information (legislation), and international law. In keeping with traditional military deterrence theory, they also suggest a reactive approach to perceived aggressions to make those actions appear undesirable. A more extreme version of ‘deterrence by punishment’ could also include offensive actions to disrupt or degrade capacity for action (to spread disinformation). An example here is the US strategy of ‘persistent engagement’ to shape parameters of acceptable behaviour in cyberspace, including, if necessary, aggressive cyber operations.⁴² Unsurprisingly, when applied to disinformation, offensive attempts to prevent an adversary from taking further action (offensive pre-emption) are among the most controversial, especially during peacetime and in democracies, since they raise dilemmas about intervention in sovereign states, and whether and when states should act in a secret or more transparent fashion.

How to Deter Disinformation: Insights from the Cross-Domain Literature

Beyond demonstrating that there are many options for responding to disinformation, the cross-domain and hybrid literature suggests other possible strengths and limits of widening deterrence in general that may be extended to disinformation.

First, some authors stress that deterrence is fundamentally a psychological relationship,⁴³ meaning that capabilities and other efforts may be less

42 J. Healey, ‘The Implications of Persistent (and Permanent) Engagement in Cyberspace’, *Journal of Cybersecurity* 5 (2019): 1–15.

43 M. Kroenig and B. Pavel, ‘How to Deter Terrorism’, *Washington Quarterly* 35 (2012): 21–36.

relevant than our perceptions and emotions⁴⁴ about them.⁴⁵ As scholars have commented, this is not a new revelation since perception has long been acknowledged as central to traditional deterrence theory and IR.⁴⁶ Nevertheless, the implication is that even though disinformation can never be completely countered, and responses are inevitably limited and generally reactive, the ‘illusion of capability’ to deter may be possible and may matter most. While some would argue that if deterrence is an illusion, that it has already failed, the ‘performance of deterrence’ (my term) may help convince actors to change their behaviour or prevent an escalation of their actions. However, this does not evade the question of credibility and the need, in general, for ‘performance’ to be backed by (how much) substance or what capability. More generally, it does not evade the multiple challenges regarding how to understand actors’ perceptions and intentions and whether, how, and why they evolve.

Second, the ‘cross-domain’ literature finds that deterrence is not about absolutes;⁴⁷ it is about making ‘attacks’ less likely or effective over time through ‘cumulative’ or ‘punctuated’ deterrence.⁴⁸ If even some (of an adversary’s) individual activities can be rendered difficult (restrictive deterrence as opposed to absolute deterrence), over time the greater process or strategy may be undermined. Similarly, it is suggested that ‘hybrid deterrence’, that is, partial as opposed to ‘comprehensive deterrence’, may deter some hybrid challenges.⁴⁹ Applying this controversial logic to disinformation, it may be rendered tactically more difficult, for example through the regulation of social media platforms. This tactical deterrence

44 For a recent review of the literature on emotions and deterrence, see: S. Zilincik and I. Duyvesteyn, ‘Deterrence: A Continuation of Emotional Life with the Admixture of Violent Means’, in *NL ARMS Netherlands Annual Review of Military Studies 2020*, F. Osinga and T. Swejls (eds), (The Hague: T.M.C. Asser, 2021).

45 R. Jervis, ‘Some Thoughts on Deterrence in the Cyber Era’, *Journal of Information Warfare* 15 (2016): 66–73.

46 V.M. Hudson, *Foreign Policy Analysis: Classic and Contemporary Theory* (MD: Rowman & Littlefield, 2014).

47 Gibbs first examined ‘absolute deterrence’ as individual level avoidance of criminal activity due to the fear of the individual of some perceived risk. J. Gibbs, *Crime, Punishment, and Deterrence* (New York: Elsevier Scientific, 1975).

48 U. Tor, ‘“Cumulative Deterrence” as a New Paradigm for Cyber Deterrence’, *Journal of Strategic Studies* 40 (2015): 92–117; L. Kello, *The Virtual Weapon and International Order* (Yale: Yale University Press, 2017).

49 Monaghan, *MCDC Countering Hybrid Warfare*.

would make it harder for actors (adversaries) to maintain coordination, thus undermining their overall efforts. Furthermore, scholars argue that actions taken in *adjacent* areas may also render the *broader strategy* ineffective.⁵⁰ Thus, to deter disinformation, actions in nearby but separate areas, such as sanctions in the economic realm, may be helpful. In sum, the literature suggests that, especially over time, even minor actions, or those in adjacent areas, may affect (an adversary's) perceptions and actions.

Third, the literature on hybrid threats and deterrence suggests that to build resilience to disinformation requires a range of actions by actors beyond the government. Individuals and society ideally become key players and their support is needed to develop a culture of national resilience. Several limits of resilience are mentioned in general that are relevant to disinformation:⁵¹ these are fluid challenges, and some may have to be tolerated; too much government involvement or regulation may create even greater challenges (and mistrust), and the use of signalling and public shaming to counter them is not well understood. Beyond resilience, threatening and imposing costs and punishments (and not linking the threat of imposing them to specific desired outcomes, or assurances to remove the threat under compliance) could be unproductive or provoke more aggressive actions in retaliation.

Fourth, there is some agreement that, to be effective, deterrence may require more to be understood about actors, their motives, and limits. These common-sense insights are often peripheral in traditional deterrence and need to be (better) addressed. Therefore, scholars suggest that terrorists are more likely to be deterred if we better understand their political motives and we target what they most cherish.⁵² In relation to disinformation, it is therefore not just the processes (media or bots) that need to be understood and responded to, but also the actors' key (political, identity, and other) motivations and other root causes of disinformation.

50 Kroenig and Pavel, 'How to Deter Terrorism'.

51 These limits are reviewed in Monaghan, *Deterring Hybrid Threats*.

52 R.F. Trager and D.P. Zagorcheva, 'Deterring Terrorism: It Can Be Done', *International Security* 30 N° 3 (2006): 87–123; Wilner, 'Contemporary Deterrence Theory'; A.S. Wilner, 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies* 3 N° 1 (2011): 3–37.

In the following section the paper examines the Canadian government's responses to disinformation within the above analysis of the conceptual widening of deterrence and how it may be applicable to disinformation. It will show that Canada has taken many steps to deter disinformation both by strengthening resilience (strategic, technical, institutional, and individual/societal) and, increasingly over time, through efforts to increase (non-kinetic) costs and punishments. It then critiques the benefits and limits of extending deterrence in general, and in Canada specifically.

Canada's Deterrence of Disinformation: Strengthening Resilience to Protect (Deny Direct Impact and Strategic Objectives)

First, Canada has made efforts to bolster its *strategic* resilience at the individual and social levels, with the aim to 'deny' mis/disinformation's political and cognitive 'wins' or impacts. A major focus here has been on developing public awareness about its multifaceted challenges. Since 2014 Canadian government departments and security agencies have been quick to explain publicly why disinformation is a security challenge, and to identify and expose specific actors and their actions. A series of bureaucratic and think-tank reports have examined both proven and alleged roles played by Russia (and Russia-related actors), China, Iran, North Korea, former US President Trump, and right-wing extremists. These reports, along with heightened political rhetoric about the dangers of disinformation have played an important role in raising awareness about the challenges and their potential negative effects.⁵³ Recent studies on deterrence suggest that such reports may further increase individual and societal resilience, as well as trust in government responses by signalling governments' respect for truth and transparency.⁵⁴

53 Jackson, 'Canadian Government's Response'.

54 Cees Van Doorn and Theo Brinkel, 'Deterrence, Resilience, and the Shooting Down of Flight MH17', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, Frans Osinga and Tim Sweijs (eds), (The Hague: T.M.C. Asser, 2021).

Related to its efforts to increase Canadians' awareness about mis/disinformation, the Canadian government has further articulated its *intentions* to respond to misinformation and disinformation in general (and less often with specifics) in various official documents, including cyber strategy documents, in Canada's defence policy, and in several other non-legal documents.⁵⁵ These stated intentions refer to disinformation and the wider category of misinformation in relation to the challenges of 'hybrid conflict' and 'foreign interference', and they propose 'whole of government' and 'whole of society' responses. Taken together, this official rhetorical 'securitisation' of disinformation⁵⁶ (that is, referring to disinformation as an urgent security threat) may function as a deterrent by signalling recognition of the challenge and implying clear intentions to act. At the same time, the language is often vague and could be criticised for not implying sufficient political resolve.

The reports are part of the government's ongoing effort to develop a more unified SC effort, not just to raise awareness but to expose falsehoods and delegitimise mis/disinformation. Canada's military and security agencies have increased their monitoring, researching, and exposing of false or manipulative narratives. The Communications Security Establishment (CSE) has used social media, including X (Twitter), to expose and counter Russian false claims and doctored images on state and social media.⁵⁷ Abroad, Canada's Task Force Latvia, along with the local Canadian embassy, has used various public outreach efforts to counter malicious narratives designed to impugn Canadian military personnel.⁵⁸ Since Russia's full-scale invasion of Ukraine in February 2022, the Canadian government has also published fact sheets to

55 These include Canada's National Cyber Security Strategy, 2018; National Cyber Action Plan, 2019–24; Strong Secure Engaged: Canada's Defence Policy, 2017; Paris Call for Trust and Security in Cyberspace, 2018; Canada's Digital Charter, 2019; Canada's Declaration of Electoral Integrity Online, 2019; CSE's Cyber Threats to Canada's Democratic Process, 2019, and its Update in 2021; G7 RRM Annual Report, 2021.

56 Jackson, 'Canadian Government's Response'.

57 Communications Security Establishment (CSE) (@cse_cst), 'Since Russia's brazen and unjustifiable invasion of Ukraine, CSE continues to observe numerous Russia-backed #disinformation campaigns online', [Twitter](#), 13 April 2022, 3:19PM.

58 Chris Wattie, 'Bringing a Knife to a Gunfight: Canadian Strategic Communications and Information Operations in Latvia, Operation Reassurance 2019–2020', *Canadian Military Journal* 21 N° 1 (2020).

counter falsehoods and misleading narratives, and regularly updates a government website that publishes Russian false claims about the invasion alongside ‘government-approved facts’ and context.⁵⁹ These SC efforts likely contribute to increased awareness about mis/disinformation, even if the reach and precise effects are unknown. However, they may also unintentionally create (more) distrust among individuals already suspicious of any government’s involvement.

Second, over the past decade, the Canadian government has worked to strengthen its departments’ general *technical* resilience and capacities to deny the direct impact of disinformation in general. The Canadian departments of National Defence and Public Safety, the Canadian Security and Intelligence Service (CSIS), and the CSE, among others, have focused their work on developing greater internal IT capacity and discovering data solutions to impede or reduce an array of misinformation and disinformation and their possible effects.⁶⁰ Most recently, Canada has also taken aim at directly limiting specific sources of disinformation and propaganda. In March 2022 the Canadian Radio-television and Telecommunications Commission (CRTC) removed Russian state-directed Russia TV (RT) and RT France from the list of non-Canadian programming services and stations authorised for distribution in Canada. As a result, broadcasters in Canada are no longer legally permitted to carry the channel whose mis- and disinformation is understood to be ‘undermining Ukrainian sovereignty’ and ‘threatening Canadian democracy’.⁶¹ Although RT content has been reposted on other platforms, this is an example of technical denial, as well as an attempt to deter by punishment because it penalises and makes a negative example of RT’s choice of content. The Canadian government (alongside private actors) has further attempted technical denial through platform regulation. While this is outside the scope of this paper, a case of government initiatives is the robustly debated Bill C-11 which received royal assent

59 Government of Canada, ‘[Countering Disinformation with Facts—Russian Invasion of Ukraine](#)’.

60 There has also been a significant increase in government and government-funded research concerning the technical creation, attribution, and dissemination of digital disinformation, including research into developing algorithms to identify and block ‘fake news’.

61 Canadian Radio-television and Telecommunications Commission, ‘[Broadcasting Decision CRTC 2022-68](#)’, 16 March 2022.

in April 2023 and includes new requirements for platforms that publish programmes online.⁶²

Third, beyond technical and strategic resilience, the government has also taken initiatives aimed at strengthening *institutional* resilience to deny direct (and indirect) impact. Its major focus here has been on protecting *elections* through intergovernmental and international collaboration, as well as by creating new legislation. Many of these efforts were initiated in advance of the 2019 federal election. The Security and Intelligence Threats to Elections task force led by the Royal Canadian Mounted Police was created by Global Affairs Canada, the CSE, and the CSIS to prepare the government as a whole to prevent and respond to ‘covert, clandestine or criminal attempts to interfere with the electoral process’.⁶³ The task force analysed foreign social media and coordinated responses with the International Group of Seven (G7) and other agencies, such as the US Global Engagement Center. The Critical Elections Incident Public Protocol was also created, under which five senior bureaucrats were to be informed of any potential interference during the 2019 federal election. The bureaucrats were tasked with determining whether the incidents were serious enough to inform Canadians, but found none that met their threshold at the time.⁶⁴

Other initiatives that addressed elections included the CSE and CSIS joining Elections Canada⁶⁵ to track and analyse big data to share with other G7 members and conduct simulations to identify vulnerabilities. Also, the 2019 Elections Modernization Act introduced new provisions aimed at deterring ‘foreign interference’.⁶⁶ Yet, despite all these efforts, concerns about mis/disinformation remained, culminating in May 2023 with leaked CSIS allegations outlining Chinese disinformation

62 [Online Streaming Act](#). Rachel Aiello, ‘[Online Streaming Bill C-11: Everything You Need to Know](#)’, CTV, 27 January 2023.

63 Government of Canada, ‘[Security and Intelligence Threats to Elections \(SITE\) Task Force](#)’.

64 Canada, House of Commons, [Standing Committee on Access to Information, Privacy and Ethics: Evidence](#), 42nd Parliament, 1st Session, 26 February 2019, 1545.

65 Government of Canada, [Combating Foreign Interference: Background](#), 2019.

66 Anna Reepschlager and Elizabeth Dubois, ‘[New Election Laws Are No Match for the Internet](#)’, *Policy Options* 2, January 2019.

and attempted interferences in the 2019 and 2021 federal elections.⁶⁷ Meanwhile, it was widely debated whether Canada needs to hold a public inquiry into disinformation and related foreign interferences, or to create a registry of ‘foreign agents’ like those of Australia and the United States. In March and April 2023, the government took a series of measures, including the announcement of the post of special rapporteur with the power to look at classified intelligence and examine foreign interference in elections, and the establishment of a new national counter foreign interference coordinator in Public Safety to coordinate Canadian efforts. In September 2023, the government launched a public inquiry into foreign interference in federal electoral processes and democratic institutions.⁶⁸ The inquiry, led by Commissioner Justice Hogue, is expected to deliver its final report by December 2024.

Other steps to develop institutional resilience (not directly related to elections) have aimed to better share information about mis/disinformation *in general* both within the government and internationally. These ongoing efforts have expanded over time and endeavour to ‘deny through collaborative information-sharing’ (my term) by developing alliances and partnerships to better monitor and understand state-sponsored disinformation.⁶⁹ Most prominently, the Rapid Response Mechanism (RRM) of Global Affairs Canada coordinates G7 roles and shares reports and best practices. Since the RRM was set up in June 2018, further federal government collaborative efforts have focused on specific areas of disinformation in response to three major events: Russia’s war in Ukraine, the Ottawa Freedom Convoy protests, and the global health epidemic. Notably, after Russia’s invasion of Ukraine in March 2022, the RRM was awarded a further \$13.4 million over five years to further strengthen coordination between countries in identifying, and responding to, foreign threats to democracy, including state-sponsored

67 ‘China Views Canada as a ‘High Priority’ for Interference: CSIS Report’, *Globe and Mail*, 1 May 2023.

68 Government of Canada, ‘[Government of Canada Launches Public Inquiry into Foreign Interference](#)’, *News Release*, 7 September 2023.

69 ‘[Statement by the Prime Minister on World Press Freedom Day](#)’, 3 May 2022.

disinformation.⁷⁰ In August 2022, an East European unit was formed as part of new Canadian measures designed to support Ukraine and punish Russia through deeper international collaboration and through the RRM.⁷¹ Canada has also expanded other partnerships focusing on dis/misinformation and foreign interference: multilaterally with NATO and the EU; with NGOs such as the US Alliance for Securing Democracy; and bilaterally with Germany and with Japan.

Fourth, there have been government-sponsored efforts to develop individual and societal resilience by promoting a healthy media ecosystem⁷² and encouraging critical thinking through education.⁷³ Such efforts are part of a widely defined ‘whole of society’ security approach that also includes global partnerships, but they are outside the scope of this paper. To quote a government website, ‘We know an engaged and informed public is the best line of defence in our efforts to fight disinformation and protect our democracy.’⁷⁴

Threatening Punishments and Imposing Costs to Outweigh Actors’ Perceived Benefits

Beyond attempts to build technical and strategic resilience, Canada has also threatened and imposed punishments and ‘costs’, both narrowly and widely defined, on the perpetrators of disinformation.⁷⁵ Until recently, these actions have been limited in scope and it remains to be

70 Prime Minister of Canada, ‘[Prime Minister Participates in Successful Visit to Germany](#)’, 9 March 2022.

71 CTV News, ‘[Canada to Create a Team to Counter Russian Disinformation](#)’, 23 August 2022.

72 Championing free and fair media, Canada became co-chair with the Netherlands of the [Media Freedom Coalition](#), and in July 2019, as inaugural co-chair along with the United Kingdom, Canada helped to initiate The High Level Panel of Legal Experts on Media Freedom.

73 Since 2020 the government has funded to the tune of \$8.5 million a whole series of programmes, including the Digital Citizen Initiative. Heritage Canada, ‘[Government of Canada Reinforces Support to Organizations to Help Counter Harmful Disinformation](#)’, *News Release*, 16 March 2022.

74 Ibid.

75 Canada’s initial efforts to regulate social media platforms are outside the scope of this study, but they are also examples of attempts to impose ‘harder’ costs by regulating rules, content, and competition.

seen whether the costs imposed or threatened outweigh any aggressors' perceived benefits.

First, Canada has called out the 'bad behaviour' of certain actors, as seen above. Thus, reports promoting awareness can 'shame and blame', thereby increasing social and psychological costs. Theoretically, especially alongside allies' similar efforts, over time they may contribute to 'deterrence by delegitimation' *and* bolster resilience by signalling resolve to respond (as seen above). On the other hand, they may also contribute to perceived grievances and thus hinder any diplomatic efforts. President Putin is well known for reacting negatively to Western critiques of his regime, and for manipulating them to bolster his domestic appeal. More obviously successful seem to have been the 'pre-emptive' selective declassification of intelligence and sharing of information by the US and its allies (including Canada) to 'debunk' Russian plans and aims during the Russia-Ukraine war. Although these actions may have had many objectives, some argue that a desired outcome was to prevent further attacks and have labelled the debunking an example of 'deterrence by disclosure'.⁷⁶

Second, the Canadian government has made efforts to impose *normative costs* to restrain behaviour through international law. These include most prominently Canada's engagement with allies to develop norms in response to various activities in cyberspace, including disinformation. Canada has been involved in intergovernmental negotiations at the UN to create a new global cybersecurity architecture that would protect digital information and the infrastructure on which it is based. This effort faces many obstacles, but the point here is that it is an attempt to deter (disinformation) 'by entanglement'.⁷⁷ In other words, it is one of several attempts to deter by increasing interdependence among states (and sometimes non-state actors) and by creating the conditions (and norms) for peace. In this case, as in others involving Russia, progress

76 Eric Edelman, 'The Pros and Cons of "Deterrence by Disclosure"', *The Dispatch*, 21 February 2022.

77 The 2014–15 Group of Governmental Experts outlined voluntary, non-binding peacetime norms of state behaviour in cyberspace. The subsequent General Assembly unanimously adopted a resolution that states should be guided by these norms. UN (2015) A/70/174.

has been further jeopardised by recent geopolitical tensions, especially stemming from Russia's full invasion of Ukraine.

Third, although there is little public information about Canada's deliberations on offensive cyber costs or punishments, even before the Russia-Ukraine war some analysts suggested that Canada might take more offensive actions to disrupt or degrade (an adversary's) capacity to spread strategic disinformation as part of a more effective 'deterrence by punishment' response. Such actions can also be framed as *technical* pre-emptive measures to increase defensive resilience. In June 2019 the CSE was granted wide-ranging powers to engage in 'defensive cyber operations' and 'active cyber operations' to 'degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada's defence, security or international affairs'.⁷⁸ That is to say, the CSE's new mandate gives it authority to respond to foreign actors (outside Canada) by using defensive or active cyber operations and allows it to team up with Canada's military in response to foreign covert and grey zone activities.

Significantly, since Russia's full invasion of Ukraine in 2022, Canada's government has also imposed targeted sanctions in the information realm, specifically against Russian and Ukrainian 'agents of disinformation'. This effort narrows the focus of deterrence, but again its effectiveness is not yet clear and may have unintended consequences. The criteria for sanctions and why they have been applied to some actors and not others could be further clarified, and assurances made about how they will be removed with compliance. The literature on sanctions is mixed, but some suggest that timing (being quick to impose sanctions) and being consistent and deliberate is important.⁷⁹ Here Canada has been at the forefront of what is mostly a political signal. Thus, on 24 February 2022 four Ukrainian

78 In June 2019 the Canadian government passed major national security legislation, including outlining how the CSE could lawfully operate. Those updates are found in [Bill C-59](#). The Communications Security Establishment Act: www.parl.ca/Content/Bills/421/Government/C-59/C-59_4/C-59_4.PDF#page=71.

79 Matus Halas, 'NATO's Sub-conventional Deterrence: The Case of Russian Violations of the Estonian Airspace', *Contemporary Security Policy* 43 No 2 (2022): 350–81.

disinformation agencies were sanctioned for enabling and supporting Russia's full invasion, along with Russian elites and close associates of the Russian regime. On 8 July twenty-nine individuals and fifteen entities were sanctioned, mostly Russian state media organisations such as TASS or Sputnik. On 14 October thirty-four individuals, their family members, and one entity (TV Zvezda, run by the Russian Ministry of Defence) were sanctioned for 'attempting to justify Russian attempts to annex part of Ukraine', for 'assisting the Russian regime in undermining the principles of state sovereignty', and for being 'responsible for spreading false narratives that serve as pretexts for the Russian regime's unjustifiable war'.⁸⁰ On 2 February 2023 twenty-eight individuals and ten entities, including the Russian state news agency Ria Novosti and the state-affiliated think tank the Russkiy Mir Foundation, were sanctioned for spreading disinformation and propaganda.⁸¹

The Benefits and Limits of Extending Deterrence to Disinformation and How to Adapt Deterrence to a Complex, Non-linear Media Environment

Examining Canada's efforts to respond to disinformation through a wide lens of deterrence helps to illuminate what Canada is doing and what might be missing. It shows that while the Canadian government has not adopted a comprehensive deterrence strategy, its efforts fit within wider understandings of 'deterrence by denial' and 'deterrence by costs and punishments'. As a result, the cornerstones of Canada's emerging foreign and security approach to mis/disinformation can be understood as resilience to 'deny' negative effects, and, increasingly, the imposition of some targeted and widely defined costs and punishments to dissuade

80 Global Affairs Canada, 'Canada Sanctions Additional Russian Propaganda Agents', *News Release*, 17 October 2022. Since Russia's illegal occupation and attempted annexation of Crimea in 2014, Canada has imposed sanctions on more than 1800 individuals and entities. Many of these sanctions have been undertaken in coordination with Canada's allies and partners. Since Russia's further invasion of Ukraine on 24 February 2022, Canada imposed sanctions on more than 1400 additional individuals and entities from and in Russia, Ukraine, and Belarus.

81 Government of Canada, [Canadian Sanctions Related to Russia](#).

harmful actions. Most recently this ‘democratic dissuasion’ (my term) has included ad hoc attempts to increase ‘whole of government and society’ efforts, but much more could be done.

Examining Canada’s actions through this more inclusive lens of deterrence also uncovers strengths and limits in Canada’s approach. It reveals that Canada has taken many steps to increase public awareness about the challenge. These may increase resilience by signalling government respect for truth and transparency (even if some would argue that they have not gone far enough) and developing government-wide and international collaboration (deterrence through ‘information-sharing’ and through ‘entanglement’). However, the approach also reveals weaknesses and options that have not been pursued or that have received less focus. Canada has provided few, if any, incentives or positive inducements to change actors’ behaviour, such as articulating when sanctions could be lifted. Also, while there have been recent attempts to increase social and normative costs (by ‘calling out’ Russia) and punishments (by imposing targeted sanctions on mostly Russian people and entities found to be spreading disinformation during the Russia-Ukraine war), these actions are limited and could fruitfully be better explained to the public. Research is also needed into their effectiveness (we know little about the effects on perceptions) and unintended consequences, or the conditions under which aggressors might retaliate by escalating their actions. A crucial question revealed is how governments can maintain or regain trust, when too much (or too little) government involvement could backfire and cause (more) distrust, thus weakening resilience. One answer might be Canadian actions to ‘deter through peace’, by developing norms, and through diplomacy, but many of these channels have been sidelined due to geopolitical tensions or recent Russian aggression.

The review also suggests that, over time, Canada’s actions and the ‘performance’ or illusion of deterrence may have a deterrent role. However, this optimistic thinking remains controversial and uncertain, and does not amount to a strategy (let alone a well-articulated and shared vision for the long term). Despite many unknowns, developing alliances,

increasing transparency, sharing information with allies, collaborating more with civil society and private actors, and small steps such as banning RT may have limited immediate effect but over time may provide some deterrent impact. Canadian actions in areas adjacent to disinformation may theoretically also function as indirect deterrence, but evidence that any of these steps have affected, or could affect, Russia's calculations in spreading disinformation remains scarce and anecdotal.

Is deterrence, as a set of principles and practices, stretched too far when applied to disinformation? It is dangerous to generalise from one case study, and especially about a complex challenge that is context specific, is rapidly evolving, and includes many unknowns. However, it can be inferred from Canada's experience in response to disinformation that extending deterrence principles and practices can clarify options (technical, individual, and social resilience; widely defined costs and punishments, including normative ones and incentives) as well as their limits (it guides consideration of whether actions are credible and persuasive and of the challenges of shaping perceptions). At the same time, broad principles have limited use in assessing or comparing the different options, especially in reference to fluid and ambiguous activities. Particularly contentious are the questions of how to inflict costs in the communication/information realm (when disinformation is turned into misinformation and can be disseminated at enormous scale and low cost) and how to alter the perceptions of an adversary who is difficult to identify. These are real challenges for deterrence by denial and resilience, but also for deterrence by punishment. And in hybrid deterrence, questions of deniability and ambiguity are even more pronounced.

However, there are other insights from the literature reviewed that are applicable to disinformation. These include the common-sense caution that 'absolute' deterrence of many non-military challenges is impossible—the results inevitably will be limited—but that society and individuals can take on greater roles and help to restrict and alleviate any potential impacts of ambiguous and evolving challenges. These are important reminders that regardless of the political commitment and actions taken,

many challenges (especially hybrid ones) cannot be completely prevented and yet they are often presented as ‘solvable’. The implications are that complexities and uncertainties should be acknowledged, and the goal should be to manage disinformation’s spread and restrict any potential harmful influences. To that end, it is important to demonstrate capacity, capability, and political resolve, for civil society to play a greater role, and to have balanced expectations of results. Although actions will inevitably be limited, they may be influential.

Some might conclude that strategies to address disinformation are best not addressed by deterrence (however defined) and instead require new paradigms.⁸² Another conclusion is that further *adaptation* of deterrence to today’s rapidly evolving and non-linear media environment is needed to confront complex geopolitical challenges, including disinformation. Looking forward, scholars examining deterrence could therefore benefit from engaging with SC, an emerging body of scholarship which grapples with these questions.⁸³ Given that deterrence is about communicating to influence the ‘other side’, the Western-thinking, geopolitically informed vision, principles, and processes of SC are relevant. Its most recent articulations reinforce, extend, and add to the observations about extending deterrence made in this literature review and case study. They also have implications more specifically for thinking about how to respond to disinformation.

Today, SC has been widely defined to include ‘everything an actor does to achieve objectives in a contested environment’, as well as ‘a holistic approach based on values and interests’.⁸⁴ Like the recent scholarship on ‘extending’ deterrence reviewed above, its logic is also flexible and open to complexity. It is more of a ‘mindset’ as well as a ‘process and

82 While different from disinformation, in 2023, the national *cyber* strategies of several Western states (the United States, the UK, the Netherlands) seem to be pivoting towards a new paradigm away from a more traditional understanding of deterrence as the core strategy and towards some form of more active defence.

83 See the last decade of articles in *Defence Strategic Communications* journal.

84 Neville Bolt, Martha Stolze, Leonie Haiden, and Jente Althuis, *Understanding Strategic Communications*, NATO Strategic Communications Centre of Excellence Terminology Working Group Publication, N° 3, Riga, May 2023, p. 15.

set of tools'.⁸⁵ It is 'a way of thinking about the relationships between society, politics and communications that endeavours to navigate the complexity of today's information space'.⁸⁶ Unlike more rigid articulations of traditional deterrence, its thinking is premised upon the understanding that individuals' perceptions of the world are constructed and that they are influenced by complex communication and multilevel power relations.

To contextualise deterrence as SC is to understand and approach deterrence in a similar way, as an act of 'constant calibration' of 'persuasive and coercive influence' (including coercive discourse but also military force, understood as necessary to underpin the credibility to act).⁸⁷ The implication is that deterrence in practice includes a wide range of activities (wider than examined in this paper) and that because 'everything communicates', deterrence can include words, images, actions, and inaction. Also implied is that to deter, a careful understanding of context (current geopolitics and the wars in Ukraine and now the Middle East) is needed, including the role of dynamic, multilevel communications (which can be distorted by disinformation). Further, in 'reverse-engineering' SC from its practitioner origins, scholars have united a collection of different insights and ideas also grappled with by many scholars extending deterrence. These include the importance of an integrated, whole of government and society approach, the centrality of retaining and rebuilding trust in government, and a belief that more needs to be understood about actors' intentions and perceptions. The literature on both SC and wider deterrence also acknowledges that some uncertainty needs to be accepted in a complex world, and that strategic ambiguity is important in communicating deterrence.

Finally, SC contributes other ideas with significant relevance for discussions of deterrence, and the deterrence of disinformation. First, its proponents argue that SC must be ethically grounded and rooted in values. In 2023, SC is conceived as a normative project, one which affirms the right of individuals to choose between competing ideas or

85 Ibid., p. 15.

86 Ibid., p. 23.

87 Ibid., p. 26.

reject them, as well as the need for transparency and accountability, and the right of individuals to free speech.⁸⁸ Second, SC also makes explicit the need to think and respond strategically, in other words in a strategic fashion with long-term, but flexible, goals in mind.⁸⁹ These are relevant because strategy and ethics are often missing or peripheral to discussions about disinformation, with responses often focused on short-term tactics and less on how exactly legitimacy can be simultaneously sustained. The implications are that the deterrence of disinformation requires a long-term perspective, one that is communicated through words, actions, and inaction and that seeks to address any strategies that lie behind disinformation, including, for example, deception, distraction, or disruption.⁹⁰

Conclusion: The Sixth Wave of Deterrence as Strategic Communications?

In sum, this paper adds new analysis to the study of deterrence and disinformation by examining them together. It provides an analysis of responses to disinformation through the widening lens of deterrence, extends empirical knowledge and explanation about the evolution of the Canadian government's efforts to deter, and makes key critiques of deterrence principles and actions taken. Ultimately, it suggests that extending the principles and practices of deterrence to disinformation remains incomplete and controversial and could benefit from further (continual) *adaptation* to an ever-evolving and complex information environment. Future scholars might wish to elaborate on this initial conceptualisation of a 'sixth wave of deterrence', one in which the deterrence at its heart is the strategic communication of complex challenges, presented within a long-term perspective and based upon a contextualised, holistic (multi-pronged), and ethically grounded pragmatic approach.

88 *Ibid.*, p. 22.

89 Neville Bolt, 'Foreword', *Defence Strategic Communications* 6 (Spring 2019): 3–10.

90 Neville Bolt, *Strategic Communications and Disinformation in the Early 21st Century*, Policy Paper N° 12, Robert Schuman Centre for Advanced Studies, European University Institute, 2021, p. 50.

Bibliography

- Adamsky, Dmitriy, *Cross-Domain Coercion: The Current Russian Art of Strategy* (Paris: Security Studies Center, 2015).
- Bjola, Corneliu, and K. Papadakis, 'Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience', *Cambridge Review of International Affairs* 33 N° 5 (2020): 638–66.
- Bolt, Neville, 'Foreword', *Defence Strategic Communications* 6 (Spring 2019): 3–10.
- Bolt, Neville, *Strategic Communications and Disinformation in the Early 21st Century*, Policy Paper N° 12, Robert Schuman Centre for Advanced Studies, European University Institute, 2021.
- Bolt, Neville, Martha Stolze, Leonie Haiden, and Jente Althuis, *Understanding Strategic Communications*, NATO Strategic Communications Centre of Excellence Terminology Working Group Publication N° 3, Riga, May 2023.
- Boudreau, Brett, *The Rise and Fall of Military Strategic Communications at National Defence, 2015–2021: A Cautionary Tale for Canada and NATO, and a Roadmap for Reform*, Canadian Global Affairs Institute, May 2022.
- Bourbeau, Philip, and C. Ryan, 'Resilience, Resistance, Infrapolitics and Enmeshment', *European Journal of International Relations* 24 N° 1 (2017): 221–39.
- Brantly, Aaron, *Back to Reality: Cross Domain Deterrence and Cyberspace* (Boston: Virginia Tech, 2018).
- Brantly, Aaron, *Conceptualizing Cyber Deterrence by Entanglement*, Social Science Research Network, Rochester, NY, 2018.
- Braw, Elisabeth, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (American Enterprise Institute, 2021).
- Caines, Timothy, *Russian Menace: Is the Canadian Government Capable of Countering Russian Disinformation?*, Canadian Forces College, JCSP 45, May 2019.
- Canada, Government of, *Canada Sanctions Additional Russian Propaganda Agents*, News Release, 17 October 2022.
- Canada, Government of, *Canadian Sanctions Related to Russia*.
- Canada, Government of, *Combating Foreign Interference: Backgrounder*, 2019.
- Canada, Government of, House of Commons, *Standing Committee on Access to Information, Privacy and Ethics: Evidence*, 42nd Parliament, 1st Session, 26 February 2019, 1545.
- Canada, Government of, *Security and Intelligence Threats to Elections (SITE) Task Force*.
- Canada, Senate of, *SenCA+ Magazine*, 23 April 2023.
- Canadian Radio-television and Telecommunications Commission, *Broadcasting Decision CRTC 2022-68*, 16 March 2022.
- CTV News, 'Canada to Create a Team to Counter Russian Disinformation', 23 August 2022.
- Doorn, Cees Van, and Theo Brinkel, 'Deterrence, Resilience, and the Shooting Down of Flight MH17', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, Frans Osinga and Tim Sweijs (eds), (The Hague: T.M.C. Asser, 2021).
- Edelman, Eric, 'The Pros and Cons of "Deterrence by Disclosure"', *The Dispatch*, 21 February 2022.
- European Union, *Tackling Disinformation, Foreign Information Manipulation and Interference*, EU External Action, 2021.
- Gartzke, Eric, and Jon R. Lindsay (eds), *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019).
- Gearson, John, 'Deterring Conventional Terrorism: From Punishment to Denial and Resilience', *Contemporary Security Policy* 33 N° 1 (2012): 171–98.
- Gibbs, J., *Crime, Punishment, and Deterrence* (New York: Elsevier Scientific, 1975).
- Gray, Colin S., *Maintaining Effective Deterrence* (US Army War College Press, 2003).
- Gregor, Milos, and Petra Mlejnková, *Challenging Online Propaganda and Disinformation in the 21st Century* (New York: Palgrave Macmillan, 2021).
- Halas, Matus, 'NATO's Sub-conventional Deterrence: The Case of Russian Violations of the Estonian Airspace', *Contemporary Security Policy* 43 N° 2 (2022): 350–81.
- Hartmann, Uwe, *The Evolution of the Hybrid Threat, and Resilience as a Countermeasure* (Zurich: Center for Security Studies, 2017).

- Healey, Jason, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* 5 (2019): 1–15.
- Heer, Tej, Charlee Heath, Kimberly Girling, and Emma Bugg, *Misinformation in Canada: Research and Policy Options*, Government of Canada, Evidence for Democracy, 2021.
- Hellman, Axel, *How Has European Geostrategic Thinking towards Russia Shifted since 2014?* Euro-Atlantic Security Policy Brief, European Leadership Network, 2019.
- Hoffman, Frank, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).
- Hudson, Valerie M., *Foreign Policy Analysis: Classic and Contemporary Theory* (MD: Rowman & Littlefield, 2014).
- Jack, Caroline, *Lexicon of Lies: Terms for Problematic Information*, Data and Society Research Institute, 2017.
- Jackson, Dean, 'Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation and "Fake News"', National Endowment for Democracy (NED), 17 October 2017.
- Jackson, Nicole, 'Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO', *Journal of Military and Strategic Studies* 19 No 4 (2019): 104–25.
- Jackson, Nicole, 'The Canadian Government's Response to Foreign Disinformation: Rhetoric, Stated Policy Intentions, and Practices', *International Journal* 76 No 2 (2022): 544–63.
- Jayakumar, Shashi, Benjamin Ang, Nur Diyanah Anwar (eds), *Disinformation and Fake News* (London: Palgrave Macmillan, 2021).
- Jervis, Robert, 'Deterrence Theory Revisited', *World Politics* 31 No 2 (1979): 289–324.
- Jervis, Robert, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare* 15 (2016): 66–73.
- Johnson, Robert, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars and Insurgencies* 29 No 1 (2018): 141–68.
- Kello, Lucas, *The Virtual Weapon and International Order* (Yale: Yale University Press, 2017).
- Keršanskas, Vytautas, *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats*, Hybrid CoE Paper 2, March 2020.
- Knopf, J.W., 'The Fourth Wave in Deterrence Research', *Contemporary Security Policy* 31 No 1 (2010): 1–33.
- Kroenig, Matthew, and Barry Pavel, 'How to Deter Terrorism', *Washington Quarterly* 35 (2012): 21–36.
- Lanoszka, Alexander, 'Disinformation in International Politics', *European Journal of International Security* 4 No 2 (2019): 227–48.
- Lilli, Eugenio, 'Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence', *Contemporary Security Policy* 42 No 2 (2021): 163–88.
- Lorenz, Wojciech, 'The Evolution of Deterrence: From Cold War to Hybrid War', *Polish Quarterly of International Affairs* 2 (2017): 22–37.
- Maddock-Ferrie, Blair, 'A Policy Proposal for the Canadian Government to Counter Disinformation through Collaboration', JCSP, *Federalism-E* 23 (2022).
- Mallory, King, *New Challenges in Cross-Domain Deterrence* (Santa Monica: RAND Corporation, 2018).
- McCgwire, Michael, 'Deterrence: The Problem—Not the Solution', *International Affairs* 62 No 1 (1985): 55–70.
- Monaghan, Sean, *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice*, Hybrid CoE Paper 12, March 2022.
- Monaghan, Sean (ed.), *MCDC Countering Hybrid Warfare: A Multinational Capability Development Campaign Project*, Countering Hybrid Warfare Project, 2019.
- Monaghan, Sean, P. Cullen, and N. Wegge, *Countering Hybrid Warfare* (Shrivenham, UK: Development, Concepts and Doctrine Centre, 2019).
- Morgan, Patrick M., 'The State of Deterrence in International Politics Today', *Contemporary Security Policy* 33 No 1 (2012): 85–107.
- NATO, *Strengthened Resilience Commitment*, 14 June 2021.
- Osinga, Frans, and Tim Sweijts (eds), *NL ARMS Netherlands Annual Review of Military Studies 2020* (The Hague: T.M.C. Asser, 2021).
- Prior, Tim, 'Resilience: The "Fifth Wave" in the Evolution of Deterrence', *Strategic Trends: Key Developments in Global Affairs* (ETH Zurich: Center for Security Studies, 2018).

- Rampersad, Giselle, and Turki Althiyabi, 'Fake News: Acceptance by Demographics and Culture on Social Media', *Journal of Information Technology & Politics* 17 N° 1 (2020): 1–11.
- Reepschlager, Anna, and Elizabeth Dubois, 'New Election Laws Are No Match for the Internet', *Policy Options* 2, January 2019.
- Ruhle, Michael, 'In Defense of Deterrence', *Information Series*, National Institute for Public Policy, N° 457 (27 April 2020).
- Sample, C., J. McAlaney, J.Z. Bakdash and H. Thackray, 'A Cultural Explanation of Social Media Manipulators', *Journal of Information Warfare* 17 N° 4 (2018): 56–71.
- Schelling, Thomas, *Arms and Influence* (New Haven CT: Yale University Press, 1966).
- Snyder, Glenn, *Deterrence and Defense: Towards a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961).
- Stevens, Tim, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* 33 N° 1 (2012): 148–70.
- Stoker, Donald, and Craig Whiteside, 'Blurred Lines: Grey-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking', *Naval War College Review* 73 (2020): 1–37.
- Sweijts, Tim, and S. Zilincik, *Cross Domain Deterrence and Hybrid Conflict* (The Hague: The Hague Centre for Strategic Studies, 2019).
- Sweijts, Tim, and S. Zilincik, 'The Essence of Cross-Domain Deterrence', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, Frans Osinga and Tim Sweijts (eds), (The Hague: T.M.C. Asser, 2021).
- Tor, Uwe, "'Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* 40 (2015): 92–117.
- Trager, Robert F., and Dessislava P. Zagorcheva, 'Detering Terrorism: It Can Be Done', *International Security* 30 N° 3 (2006): 87–123.
- Tucker, Joshua, et al., 'Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature', Hewlett Foundation, March 2018.
- United Kingdom, Ministry of Defence, Joint Doctrine Note 1/19: Deterrence. The Defence Contribution, DCDC, 2019, 40–41.
- United State, National Security Strategy, October 2022.
- Vraga, Emily K., and Leticia Bode, 'Defining Misinformation and Understanding Its Bounded Nature: Using Expertise and Evidence for Describing Misinformation', *Political Communication* 37 N° 1 (2020): 136–44.
- Wardle, Claire, and Hossein Derakhshan, 'Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making', Council of Europe Report, 2017.
- Wigell, Mikael, Harri Mikkola, and Tapio Juntunen, 'Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats', European Parliament, May 2021.
- Wilner, Alex S., 'Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far', *New York University Journal of International Law and Politics* 47 (2014): 439–62.
- Wilner, Alex S., 'Cyber Deterrence and Critical Infrastructure Protection: Expectation, Application and Limitation', *Comparative Strategy* 36 N° 4 (2017): 309–18.
- Wilner, Alex S., 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies* 3 N° 1 (2011): 3–37.
- Zilincik, Samuel, and I. Duyvesteyn, 'Deterrence: A Continuation of Emotional Life with the Admixture of Violent Means', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, Frans Osinga and Tim Sweijts (eds), (The Hague: T.M.C. Asser, 2021).

Cybersecurity in Political Studies: A Scoping Review

Aybars Tuncdogan

Keywords—*cybersecurity, cyberwar, cyberspace, strategic communications, strategic communication, digital geopolitics, political science, international relations*

About the Author

Dr Aybars Tuncdogan is a Senior Lecturer (Associate Professor) of Marketing and Technology at the King's Business School, King's College London. He is a Research Affiliate of the King's AI Institute and a member of the King's Cybersecurity Centre.

Abstract

In recent years the increasing prevalence of technology has elevated cybersecurity from being a niche focus of interest for a small group of specialised computer scientists to a macro-level concern, attracting the attention of scholars and practitioners in political science and international relations. Today governments and military bodies view aspects of cybersecurity—ranging from preparations for cyberwar (a facet of digital geopolitics) to managing responses to cyber events (a facet of strategic communications)—as critical to their national security. However, while this mounting interest among academics has led to a rise in publications in political science and international relations journals, such rapid growth also results in literature fragmentation,

where many studies do not sufficiently communicate with each other, and theoretical development remains relatively limited. In this paper, by reviewing the 113 cybersecurity papers published in 53 prominent journals in political science and international relations, I aim to provide an overview of the current state of research in this domain. Overall, this study has implications for the political science and international relations fields, especially the literature on strategic communications and digital geopolitics.

Introduction

In recent decades, rapid technological developments have brought the digital realm into the centre of geopolitical considerations. Once a specialised domain for computer scientists, cybersecurity is now an essential part of discussions regarding national defence and global power dynamics.¹ NATO considers cybersecurity capabilities a key component of defence and deterrence,² and prominent financial organisations classify cyberattacks as a top global risk.³ Nations are struggling to minimise their digital vulnerabilities and to maximise their abilities to observe and deter others in the cyber realm. In line with this, most nations now spend substantial resources on improving their cybersecurity capabilities, as exemplified by such initiatives as the National Cyber Security Centre (NCSC) of the United Kingdom and the US Cyber Command, which is designated as a combatant command of the US military. Additionally, cyberspace is now included as one of the five NATO domains: 'Maritime, Land, Air, Space and Cyberspace'.⁴ Reflecting this trend, there has been a surge in interest in cybersecurity among scholars and academic

- 1 Myriam Dunn Cavelty and Andreas Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science', *Contemporary Security Policy* 41 N° 1 (2020): 5–32. Lennart Maschmeyer, 'Subversion, Cyber Operations, and Reverse Structural Power in World Politics', *European Journal of International Relations* 29 N° 1 (2023): 79–103. Dara Conduit, 'Digital Authoritarianism and the Devolution of Authoritarian Rule: Examining Syria's Patriotic Hackers', *Democratization* (2023): 1–19.
- 2 NATO, '[Deterrence and Defence](#)', 10 October 2023.
- 3 S&P Global, '[Top Geopolitical Risks of 2023](#)', S&P Global, 2023. World Economic Forum, [The Global Risks Report 2023](#), 18th edn (WEF, 2023). BlackRock, [Geopolitical Risk Dashboard](#), BlackRock, 25 July 2023.
- 4 NATO, '[Multi-Domain Operations in NATO—Explained](#)', 5 October 2023.

journals of political science and international relations, with papers being published on this topic regularly.

However, as with many swiftly developing areas of interdisciplinary research, the expanding body of cybersecurity-related work in the domain of political science and international relations comes with a growing problem of fragmentation. In other words, various disjointed studies are being published in different outlets, but these do not result in a coherent dialogue and a cumulatively growing body of theoretical knowledge based on unifying theoretical frameworks. In other words, in its current form, cybersecurity-related research is being published regularly in political science and international relations fields, but it is not yet well defined as a literature with clear research streams. This issue not only limits the further growth and explanatory abilities of this research area but also restricts its practical relevance, as it impedes practitioners' access to this information.

In this paper I present the results of a scoping review of the cybersecurity research published in political science and international relations journals. Specifically, this study conducts a systematic review of the entire body of literature in this field to offer a comprehensive overview, rather than to address a particular research question. As a result, the findings of this study will contribute to the emerging literature in two ways. First, systematically investigating this body of research reveals the key streams of research within this area and the pivotal issues being examined in those streams. These insights are helpful for scholars publishing or who want to publish in this area, as well as for practitioners who want to make sense of the insights from political science and international relations journals about cybersecurity and determine which publications contain the specific information they are looking for. Second, by systematically examining what is known in this emerging area, information that has not yet been produced can also be revealed. Specifically, by building on the findings of this review, I discuss a range of future research opportunities, which should help to further speed up development in this area of research. Moreover, due to its findings, this study has implications specifically

for research on strategic communications and digital geopolitics. In particular, a systematic examination of the 113 studies in this area indicates that they can be categorised under seven headings, including ‘miscellaneous’. Of these, three can be second-order grouped under the heading of strategic communications, whereas another three can be grouped under the heading of digital geopolitics. This process will be discussed in further detail in the methodology and results sections.

In brief, this study aims to systematically summarise the body of cybersecurity research in political science and international relations journals and propose future research directions based on this summary. The rest of this paper is structured as follows. In the next section, I describe the methodology, such as the keywords I used when searching for articles, the journals I included, and the procedure I followed to reach the final sample of 113 papers. Following that, I introduce the seven research themes and two overarching themes that emerged in this review and consider each of these research themes and the key issues they have focused on until now. Finally, I discuss some future research opportunities in this area.

Methodology

I began the review process by listing keywords likely to appear in cybersecurity-related studies in political science and international relations journals. I read several articles and noted relatively broad common keywords. I focused primarily on papers published in non-technical journals, such as those on political science, international relations, strategic communications, business management, economics, and digital ethics. In addition, I examined some articles published in the computer science, information systems, and cybersecurity fields to broaden my wordlist. Next, I contacted some scholars from relevant areas and used their suggestions to further expand the wordlist (the resulting search query was: “cyber security” OR “information security” OR “cybersecurity” OR “cyber-security” OR “hacking” OR “hacker” OR “information

warfare” OR “cyber warfare” OR “cyber-warfare” OR “cyber attack” OR “cyber-attack” OR “cyberattack” OR “cyber threat” OR “cyberthreat” OR “cyber-threat” OR “cyber terrorism” OR “cyber-terrorism” OR “cyberterrorism” OR “cyber espionage” OR “cyber-espionage” OR “data breach” OR “cybercrime” OR “cyber crime” OR “cyber-crime”).

To ensure a comprehensive search, I included an article in the sample if any of the specified keywords appeared in any part of the article. In addition, I used the ‘KeyWords Plus’ option of the Web of Science database to help capture articles containing terms related to these keywords. I selected journals based on the Scimago Journal Ranking for the ‘Political Science and International Relations’ category. More specifically, I included all fifty journals and supplemented this list with three additional specialist journals (*Journal of Strategic Studies*, *Journal of Global Security Studies*, and *Defence Strategic Communications*) with relevant contributions to this area.

I first conducted my search on the Web of Science Core Collection and found 161 articles. If a journal was not indexed by the Web of Science Core Collection, I used Google Scholar to find papers related to these keywords, expanding the sample to 194 articles. From these, I removed 34 book review articles.

Next, I manually went through the sample to identify papers genuinely related to one or more cybersecurity concepts. Specifically, I omitted papers that merely mentioned cybersecurity terms or used one of the keywords in a different context. For instance, papers were excluded from further analysis if they were found in the search due to the author’s last name being ‘Hacker’ or if the term ‘hacking’ was used to mean ‘subverting’ (e.g. subverting a law through the use of a loophole) rather than in the cybersecurity sense.

Subsequently, I conducted content analysis on the remaining 113 papers and categorised them into the seven themes I identified: public reactions to cybersecurity issues; information warfare in the cyber landscape;

attribution of cybersecurity incidents; cyberwarfare, capabilities, and deterrence; cybersecurity policies and governance; regional issues in cybersecurity; and miscellaneous (for idiosyncratic papers that did not fit into any of the above-mentioned categories). Essentially, these seven categories represent the dominant streams of research in the literature. The journals with the highest number of cybersecurity-related articles were the *Journal of Strategic Studies* (18); the present journal, *Defence Strategic Communications* (13); *Contemporary Security Policy* (13); *International Affairs* (12); and *International Security* (7). Of the 53 political science and international relations journals surveyed, 30 had published at least one paper related to cybersecurity. The earliest article from this sample dates back to 2001, while the most recent were in press (e.g. 'Articles in Advance') as of September 2023. Furthermore, 107 of the 113 articles (95 per cent) were published since 2012, and 72 (almost two-thirds) were published in the last five years.

Results

This section reviews the seven themes of cybersecurity research in political science and international relations. For enhanced conceptual clarity, these themes can be placed into two higher-order categories. The first group of three themes (public reactions to cybersecurity issues; information warfare in the cyber landscape; and attribution of cybersecurity incidents), consisting of 45 studies, can be grouped under the overarching umbrella of *strategic communications*. In particular, one definition of (government) strategic communications is 'government efforts aimed at clarifying government policies, stance, or actions towards an issue'.⁵ Similarly, NATO defines strategic communications as 'the coordinated and appropriate use of NATO communications activities and capabilities in support of Alliance policies, operations and activities, and in order to advance NATO's aims', which includes the activities and capabilities of public diplomacy, public affairs, military

5 Anne Speckhard, Ardian Shajkovci, and Mohamed Ahmed, 'Intervening in and Preventing Somali-American Radicalization with Counter Narratives', *Journal of Strategic Security* 11 N° 4 (2018): 32-71.

public affairs, information operations, and psychological operations.⁶ In line with these definitions, issues such as information warfare in digital environments, governments' decisions regarding whether and how to publicly attribute a cyber incident, and how governments should manage publics' reactions to cyber incidents are core to the concept of strategic communications. Similarly, the second group of three themes (cyberwarfare, capabilities, and deterrence; cybersecurity policies and governance; and regional issues in cybersecurity), consisting of 58 studies, can be grouped under the overarching umbrella of *digital geopolitics*, which refers to 'the competition in the digital realm between countries, influenced by their economic, diplomatic, and military power'.⁷ The remaining 10 studies did not fit into these themes and are discussed in the miscellaneous category. Citing every one of the 113 studies was not feasible given space limitations, but I have included most of these studies in this paper. While doing so, I have endeavoured to select a set of studies that represents the larger corpus that I reviewed.

Public Reactions to Cybersecurity Issues

Some recent studies in the sample have focused on public reactions to various cybersecurity-related issues. Most research in this area considers the effects of cyberattacks on public support for retaliation, cyber or otherwise. Leal and Musgrave found that Americans are more likely to support retaliatory actions against organised cyberattacks, such as by a terrorist organisation or state agency as opposed to an individual.⁸ Moreover, higher levels of loss in terms of economics and human life were associated with heightened support for escalation beyond cyberweapons. Similarly, Shandler, Gross, and Canetti in their two survey studies (with a total of 2585 participants from the US, UK, and Israel) examined the

6 NATO Strategic Communications Centre of Excellence, '[About Strategic Communications](#)', 11 November 2023.

7 Andrea Chiappetta, 'Digital Geopolitics: The New Global Challenge', in *The Palgrave Handbook of Global Social Change*, R. Baikady et al. (eds), (Cham: Springer International, 2022), pp. 1–18.

8 Marcelo M. Leal and Paul Musgrave, 'Hitting Back or Holding Back in Cyberspace: Experimental Evidence regarding Americans' Responses to Cyberattacks', *Conflict Management and Peace Science* 40 N° 1 (2023): 42–64.

Overarching domain	Theme	Sub-theme	Example research subject and study
Strategic communications	Public reactions to cybersecurity issues	Effects of cyberattacks on public support for retaliation	Public support for triggering NATO's Article 5 after a cyberattack (Guenther and Musgrave, 2022)
		Public preferences regarding cybersecurity policies	The US public's views towards keeping a secret arsenal of cyber vulnerabilities, as opposed to disclosing them (Leal and Musgrave, 2023)
		Public perceptions towards hackers and their effects	Cyber-noir depictions of hackers in popular culture and their grey-area behaviours (Shires, 2020)
	Information warfare in the cyber landscape	Techniques of digital information warfare	Use of denial-of-service (DoS) attacks for political purposes during election periods (Lutscher et al., 2020)
		Digital information warfare tactics associated with Russia	Employment of organised Internet trolls for the purpose of desecuritisation (Kurowska and Reshetnikov, 2018)
		Digital information warfare in other contexts	ISIS's use of information manipulation tactics in post-Soviet regions (MacWilliam, 2021)
	Attribution of cybersecurity incidents	States' attribution of cybersecurity events	When states should publicly attribute/ acknowledge their cyber operations (Egloff and Smeets, 2023)
		The public's attribution of cybersecurity events	Difficulties citizens face in attributing cyberattacks (Schulzke, 2018)

Overarching domain	Theme	Sub-theme	Example research subject and study
Digital geopolitics	Cyberwarfare, capabilities, and deterrence	Nature and likelihood of cyberwarfare	Risks associated with cyberwar (Acton, 2018)
		Cyberwar capabilities and deterrence	The private sector's contributions to cyber deterrence (Lilli, 2021)
	Cybersecurity policies and governance	International cyber diplomacy	Nations' right to self-defence in cyberspace (Oorsprong et al., 2023)
		National cybersecurity policy	Public-private partnerships' role in national cybersecurity (Christensen and Petersen, 2017)
		Intelligence services in cyberspace	Structures of cyber capabilities in military and intelligence organisations (Liebetau, 2023)
	Regional issues in cybersecurity	China	China's technological advancement in terms of cybersecurity (Gilli and Gilli, 2018)
		Other regions	Russian strategic culture and cybersecurity decisions (Kari and Pynnöniemi, 2023)
		The public's attribution of cybersecurity events	Difficulties citizens face in attributing cyberattacks (Schulzke, 2018)

Note: In the paper, a seventh theme (miscellaneous) was included for the small group of papers that do not fit well into any of these themes.

Table 1.
 Key areas of cybersecurity research within political science and international relations

public's responses to different kinds of terrorism.⁹ They found that the public's perception of cyberweapons as a form of non-deadly retaliation causes them to support further escalation if the initial attack by the terrorist organisation results in human casualties. Furthermore, Guenther and Musgrave investigated this issue in the NATO context; by means of four experiments with American participants recruited through an online platform, they attempted to gain insights regarding whether the American public supports the triggering of Article 5 (collective defence by all member states should any one be attacked) in the event of a cyberattack.¹⁰ In line with the prior studies discussed, public support for retaliation is increased if the initial attack resulted in the loss of life. Other factors that augmented the preference for the triggering of Article 5 were whether the targeted country had an alliance treaty with the US and whether civilians were targeted in the attack. In line with and further extending these findings through an emotions perspective, Shandler, Gross, Backhaus, and Canetti found that individuals exposed to cyberterrorism are significantly more likely to support retaliatory actions and that the mediating psychological mechanism is anger (not anxiety).¹¹ In a similar vein Cheung-Blunden and Ju found that cyberattacks also induce anxiety, which tends to inhibit the processing and recall of information.¹² Considering that prior research has highlighted anxiety as a precursor of risk aversion and inaction,¹³ it is implied that when the public feels anxious as a result of a cyberattack—as opposed to angry—there might be decreased public support for retaliation, as retaliation is an active and risky response. Nevertheless, further research is needed in this area before we can definitively draw this conclusion.

-
- 9 Ryan Shandler, Michael L. Gross, and Daphna Canetti, 'A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel', *Contemporary Security Policy* 42 N° 2 (2021): 135–62.
 - 10 Lindsey Guenther and Paul Musgrave, 'New Questions for an Old Alliance: NATO in Cyberspace and American Public Opinion', *Journal of Global Security Studies* 7 N° 4 (2022), ogac024.
 - 11 Ryan Shandler, Michael L. Gross, Sophia Backhaus, and Daphna Canetti, 'Cyber Terrorism and Public Support for Retaliation—A Multi-country Survey Experiment', *British Journal of Political Science* 52 N° 2 (2022): 850–68.
 - 12 Violet Cheung-Blunden and Jiarun Ju, 'Anxiety as a Barrier to Information Processing in the Event of a Cyberattack', *Political Psychology* 37 N° 3 (2016): 387–400.
 - 13 A.E. Eisenberg, J. Baron, and M.E. Seligman, 'Individual Differences in Risk Aversion and Anxiety', *Psychological Bulletin* 87 N° 1 (1998): 245–51.

Some other studies in this research stream examine public preferences for policies beyond retaliation. A different study by Leal and Musgrave examined American respondents' preferences regarding keeping a secret arsenal of zero-day vulnerabilities (security flaws of which the vendor is unaware).¹⁴ Keeping these vulnerabilities secret substantially increases the offensive capabilities of a government in the cyber domain, but also causes those vulnerabilities to remain unfixed for a substantial period (an average zero-day exploit stays active for 6.9 years, according to one study¹⁵). Leal and Musgrave found that, facing this dilemma, US respondents have a strong preference for disclosing the vulnerabilities in order for them to be patched.¹⁶ That is, the American public shows a preference for the defensive benefits of fixing the vulnerability as opposed to the offensive advantages it provides. Likewise, Kostyuk and Wayne conducted an experimental study with the participation of 508 university students, which indicated that individuals exposed to a nationally or personally relevant data breach scenario become more likely to advocate more resource-intensive government policies to defend against cyber operations.¹⁷

Finally, a couple of studies considered public perceptions towards hackers and their effects. Shires discussed the cyber-noir depiction of hackers in popular culture and how this encourages ethically ambiguous behaviours ('grey-area behaviours') among individuals adhering to the hacker identity.¹⁸ Meanwhile, Tanczer, through a longitudinal qualitative study, gained insights into hacker identity and how hackers are viewed by industry actors.¹⁹

-
- 14 Marcelo M. Leal and Paul Musgrave, 'Backwards from Zero: How the US Public Evaluates the Use of Zero-Day Vulnerabilities in Cybersecurity', *Contemporary Security Policy* 44 N° 3 (2023): 437–61.
 - 15 Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights* (Santa Monica, CA: RAND Corporation, 2017).
 - 16 Leal and Musgrave, 'Backwards from Zero'.
 - 17 Nadiya Kostyuk and Carly Wayne, 'The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public', *Journal of Global Security Studies* 6 N° 2 (2021), ogz077.
 - 18 J. Shires, 'Cyber-Noir: Cybersecurity and Popular Culture', *Contemporary Security Policy* 41 N° 1 (2020): 82–107.
 - 19 Leonie Maria Tanczer, '50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers', *Contemporary Security Policy* 41 N° 1 (2020): 108–28.

Information Warfare in the Cyber Landscape

Research on information warfare in the cyber landscape focuses on disinformation and misinformation tactics used in online environments and can be broadly divided into three categories. The first category delves into the techniques utilised in digital information warfare, including the use of disinformation techniques on online platforms and the deployment of cyberattacks for information warfare. The second category consists of studies focusing on digital information warfare tactics associated with Russia. Lastly, the third category includes studies that examine digital information warfare in other international settings.

Several studies have shown that the digital landscape has become lush ground for novel methods of information warfare. Given the proven effectiveness of social media platforms,²⁰ most of these studies focus on tactics used on such channels. For example, using four online data sets, Agarwal and Bandeli investigated misinformation and disinformation patterns.²¹ On the basis of their study, they developed a set of eight heuristics that can be used to identify such articles (e.g., ‘Check to see if the post is disturbing or controversial; fake stories are often embedded in such posts’).²² They also tracked the origins and dissemination of fake content and observed that the same content is typically used in multiple posts over different social media channels and websites. In line with this, another heuristic they propose is ‘Check if the article has been previously published and if it is being reused to affect perceptions about an event or specific actions.’ Analogously, Holmstrom examined the core principles underlying an influential narrative in social media propaganda.²³ She highlights the potency of horizontal propaganda, characterised by peer-to-peer influences, as opposed to the vertical,

20 Aybars Tuncdogan and Aidan Hughes, ‘Guiding Word-Of-Mouth (WOM) through Organic Social Media for Effective Strategic Communications: A Literature Review’, *Defence Strategic Communications* 11 (2022): 115–50.

21 Nitin Agarwal and Kiran Kumar Bandeli, ‘Examining Strategic Integration of Social Media Platforms in Disinformation Campaign Coordination’, *Defence Strategic Communications* 4 N° 1 (2018): 173.

22 *Ibid.*, 191–92.

23 Miranda Holmstrom, ‘The Narrative and Social Media’, *Defence Strategic Communications* 1 N° 1 (2015): 118–32.

top-down approach. Likewise, she argues that effective counter-narratives avoid absolute dichotomies and focus on presenting a vision for the future. Venturing into similar terrain, Agarwal, Al-Khateeb, Galeano, and Goolsby used network analysis on two Eastern European data sets to observe the social media patterns of bots responsible for disseminating propaganda and misinformation.²⁴ Their study reveals insights into the structure of these disinformation dissemination networks. Their findings further emphasise the importance of peer-to-peer influences, echoing the arguments of the prior study by Holmstrom. In particular, they found that these networks tend to be non-hierarchical (they do not have a central node) and are characterised by complexity. Furthermore, the most communicative/active nodes are made up of approximately two bots and ten genuine (human) users. Adding another perspective, Lutscher, Weidmann, Roberts, Jonker, King, and Dainotti investigated the use of denial-of-service attacks—cyberattacks that temporarily shut down online services—as political tools by non-democratic governments as well as opposition activists during elections.²⁵ Their findings indicate the frequency of DoS attacks increased as the election drew near, with the majority of these attacks targeting news websites hosted in other countries.

There is also a sizable stream of studies with Russia as a focal point. For example, drawing upon the case of the downing of a Malaysian Airlines plane, Golovchenko, Hartmann, and Adler-Nissen discuss the information war between Russia and Western countries.²⁶ The key finding of this study is that in this case the disinformation and counter-disinformation were driven to a very large extent by active citizens on social media—even more so than by the states themselves. Jensen, Valeriano, and Maness

24 Nitin Agarwal, Samer Al-Khateeb, Rick Galeano, and Rebecca Goolsby, 'Examining the Use of Botnets and Their Evolution in Propaganda Dissemination', *Defence Strategic Communications* 2 N° 1 (2017): 87–112.

25 Philipp M. Lutscher, Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti, 'At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Nondemocratic Regimes', *Journal of Conflict Resolution* 64 N° 2–3 (2020): 373–401.

26 Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, 'State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation', *International Affairs* 94 N° 5 (2018): 975–94.

examined Russia's use of cyber operations to manipulate public opinion.²⁷ They explain that Russia can be used not only for purposes of exfiltrating valuable data but, when applied in orchestration with propaganda tactics, also to help change the opinions of the public to undermine the target country's institutions. They also explain that Russia uses automated bots and troll farms—operatives creating online posts and other content as if they are ordinary citizens—as a part of its online propaganda efforts. Kurowska and Reshetnikov focused specifically on Russia's use of trolls to prevent securitisation, a tactic they term 'neutrollization'.²⁸ They argue that, by disseminating carefully crafted disinformation, which makes recipients overly suspicious of all information they encounter, Russia dilutes information that suggests an impending threat, thereby achieving desecuritisation. Czerny argues that the Russian government selectively enforces Internet laws to bolster its propaganda campaigns.²⁹ In particular, he notes that the Russian government employs selective law enforcement tactics to exert influence over Internet intermediaries, such as search engines and social media platforms, non-systemic opposition, including an online voting project initiated by opposition supporters, and the general citizenry.

A few other studies focus on different global contexts to gain insights into digital information warfare. Hacıyakupoglu, for instance, explored politicians' deployment of the 'fake news' label in the context of Malaysian elections.³⁰ Notably, she explains that a law aiming to combat fake news was enacted immediately before the elections, only for the process to repeal it to commence shortly after. Hacıyakupoglu suggests that the fake news label and the associated law may have been used strategically for the purpose of discrediting legitimate political communications from opposition parties and supporters. In a different vein, MacWilliam sheds light on ISIS's use of information manipulation tactics to draw in a large

27 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist', *Journal of Strategic Studies* 42 No 2 (2019): 212–34.

28 Xymena Kurowska and Anatoly Reshetnikov, 'Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization', *Security Dialogue* 49 No 5 (2018): 345–63.

29 Milàn Czerny, 'Selective Law Enforcement on the RuNet as a Tool of Strategic Communications', *Defence Strategic Communications* 9 No 9 (2020): 53–85.

30 Gulizir Hacıyakupoglu, 'The "Fake News" Label and Politicisation of Malaysia's Elections', *Defence Strategic Communications* 5 No 5 (2018): 87–128.

number of Central Asians from the post-Soviet regions.³¹ He showcases examples demonstrating the multi-channel, demagogical propaganda ISIS used on digital platforms to influence impressionable individuals. Finally, taking a historical perspective, Franchi and Vichi examined how the Zapatistas were one of the pioneering groups to employ digital information warfare, and used the Internet both internally to shape their identity and also externally to exert influence over the Mexican government.³²

Attribution of Cybersecurity Incidents

Another stream of research examines the attribution of cybersecurity incidents. This area of research is conceptually linked with studies on public reactions to cybersecurity issues. It is also different in that the focus in this research stream is not on what the reaction should be (type of retaliation) but specifically on understanding who is responsible for the attack. So far, this stream of literature asks two key questions: ‘How does the state publicly attribute cyberattacks?’ (how does the state decide what information should be made public? Whom to blame publicly?—it is argued that the second question can sometimes also involve strategic reasons³³) and ‘How do the members of the public attribute cyberattacks?’ (which factors influence citizens’ and other stakeholders’ views of what has happened?).

Most of the studies in this area focus on the state’s attributions. Lee used a data set of 41 public attributions by the US government between 2010 and 2020 to examine when and how governments make public

31 Ian MacWilliam, ‘Islamic State and Jihadist Media Strategies in the Post-Soviet Region’, *Defence Strategic Communications* 9 (2021): 15–52.

32 Tássio Franchi and Leonardo Vichi, ‘The Beginning of Warfare on the Internet: Zapatista Strategic Communications’, *Defence Strategic Communications* 6 (2019): 123–54.

33 Marcelo Leal and Paul Musgrave, ‘Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks’, *Foreign Policy Analysis* 18 N° 2 (2022), orac003. Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, ‘Strategic Aspects of Cyberattack, Attribution, and Blame’, *Proceedings of the National Academy of Sciences* 114 N° 11 (2017): 2825–30.

attributions.³⁴ Heajune Lee shows that the US government uses four key channels to make public attributions: technical (technical reports), criminal (indictments), official policy (press releases), and unofficial policy (leaks). Lee also argues that these four channels differ in terms of their purposes and target audiences (domestic, international, or both). In addition, Poznansky and Perkoski found that state actors are unlikely to acknowledge publicly most of their cyberattacks (e.g. stealing data), and when they do so, it is commonly for exerting coercive power.³⁵ On the other hand, Stevens considered the nature of the public attributions by private cybersecurity firms, as their recounts are used both by states and the public to gain insights into the incident.³⁶ Based on a study of the reports by Symantec after the Stuxnet worm incident, Stevens argues that private cybersecurity firms' public attributions are neither apolitical nor neutral. Egloff and Smeets pondered the question of when states should make public attributions and developed a framework that delineates different trade-offs when making this decision.³⁷ Similarly, Rid and Buchanan put forward the 'Q-Model', which is a diagnostic framework that agencies and cybersecurity experts can use to investigate the origins of cyberattacks.³⁸ In particular, they argue that it is possible to make correct attributions through this methodological search process. The key difference between the Egloff/Smeets and Rid/Buchanan frameworks is that the former focuses on improving public attributions (what to tell the public), whereas the latter focuses on the internal attributions (who actually did it).

Knowledge regarding the public's attributions of cyberattacks is relatively more limited (not to be confused with '*public attributions*' discussed above, referring to a state's public acknowledgement of a cyber operation

34 Heajune Lee, 'Public Attribution in the US Government: Implications for Diplomacy and Norms in Cyberspace', *Policy Design and Practice* 6 N° 2 (2023): 198–216.

35 Michael Poznansky and Evan Perkoski, 'Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution', *Journal of Global Security Studies* 3 N° 4 (2018): 402–16.

36 Clare Stevens, 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet', *Contemporary Security Policy* 41 N° 1 (2020): 129–52.

37 Florian J. Egloff and Max Smeets, 'Publicly Attributing Cyber Attacks: A Framework', *Journal of Strategic Studies* 46 N° 3 (2023): 502–33.

38 Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38 N° 1–2 (2015): 4–37.

or incident). Using data from a survey of a nationally representative sample of a thousand participants and two survey experiments with more than two thousand participants, Leal and Musgrave conducted a large-scale investigation into how the public attributes cyberattacks.³⁹ They found that the public's confidence in an attribution claim regarding a cyberattack is positively associated with endorsements of that claim by independent groups, such as academics. The extent to which the intelligence agencies express confidence in the attribution claim is also positively associated with the public's confidence in that claim, but the effect size of endorsements by independent groups is relatively larger. On average, confidence in the attribution claim is also positively associated with the support for retaliation (although political affiliation seems to play a moderating role in this link). Likewise, Schulzke explains that cyber incidents are difficult to trace and attribute definitively, and citizens' dependence on frames by elite audiences can push them towards developing conspiracy theories.⁴⁰ On a related note, research by Egloff used three case studies to provide examples of the responses of different groups after an attack is publicly attributed by government agencies.⁴¹

Cyberwarfare, Capabilities, and Deterrence

The literature stream on cyberwarfare, capabilities, and deterrence is relatively more complex than most of the other streams due to the multitude of different angles brought up around this subject. This area also leaves substantial room for futuristic and speculative thinking, which again makes the broader dialogue relatively less coherent. That said, papers in this area can be roughly grouped into two categories: those that focus on the nature and likelihood of cyberwarfare and those centring on cyberwar capabilities and deterrence.

39 Leal and Musgrave, 'Cheerleading in Cyberspace'.

40 Marcus Schulzke, 'The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty', *Perspectives on Politics* 16 N° 4 (2018): 954–68.

41 Florian J. Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia', *Contemporary Security Policy* 41 N° 1 (2020): 55–81.

Turning attention to the first group of studies, given that cyberwarfare is a relatively new concept, it requires clearer conceptualisation to fully comprehend its characteristics and implications. Hence, some academics have focused on this issue. Some of the earlier discussions around 2012 considered whether a cyberwar would happen. In particular, Rid pondered on the characteristics of cyberwarfare based on three criteria described by Clausewitz.⁴² A key point he argues for is that cyberattacks are not lethal enough to result in conventional wars. Thus, he chooses to conceptualise cyberwarfare as a new implementation of espionage, sabotage, and subversion activities. McGraw provides a different conceptualisation: ‘Cyberspace more closely resembles the naval or space domains where powerful countries can monitor, patrol, exert influence and deter aggression, but cannot exercise territorial control in the way it is traditionally conceived of during ground conflicts.’⁴³ Using the example of the Stuxnet worm, he argues that effective cyberwar payloads can be built relatively easily, and thus cyberwars are almost inevitable. Considering both perspectives, Kello emphasises the ambiguity regarding the probability and potential size of a cyber war, and notes that ‘what may now seem a “revolutionary” technology will eventually become the new “conventional”’.⁴⁴

Subsequent publications furthering this dialogue converge on the question of how large cyberwars can get. For instance, Valerino and Maness—based on a data set of 110 cyber incidents and 45 cyber disputes that happened between 2001 and 2011—argue that countries show a level of constraint in their cyber operations, and typical instances are regional events.⁴⁵ Smeets explains that the ephemeral nature of cyberweapons—due to the constant patching of vulnerabilities—may be a factor limiting their large-scale deployment.⁴⁶ In juxtaposition,

42 Thomas Rid, ‘Cyber War Will Not Take Place’, *Journal of Strategic Studies* 35 N° 1 (2012): 5–32.

43 Gary McGraw, ‘Cyber War Is Inevitable (Unless We Build Security In)’, *Journal of Strategic Studies* 36 N° 1 (2013): 109–19.

44 Lucas Kello, ‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft’, *International Security* 38 N° 2 (2013): 7–40.

45 Brandon Valeriano and Ryan C. Maness, ‘The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11’, *Journal of Peace Research* 51 N° 3 (2014): 347–60.

46 Max Smeets, ‘A Matter of Time: On the Transitory Nature of Cyberweapons’, *Journal of Strategic Studies* 41 N° 1–2 (2018): 6–32.

Acton posits that command-and-control system vulnerabilities can even increase the likelihood of a nuclear war.⁴⁷

The second group of studies focuses on cyberwar capabilities and deterrence. Egloff and Shires investigated how states can integrate offensive cyber capabilities into their arsenal for aggressive responses.⁴⁸ They theorise that there are three methods ('logics') for this integration: substitution (using these capabilities as a replacement for other methods), support (employing these capabilities to bolster another action), and complementarity (utilising them when other alternatives are unable to achieve the same goal). They argue that while the first two methods have the potential for mitigating violence, the third is likely to escalate it. On a similar note, Tor begins his paper by comparing the cyber deterrence perspectives of the US and Israel.⁴⁹ He explains that the US views the use of cyber operations as an indication that deterrence measures have faltered ('absolute deterrence'), whereas Israel views the use of some cyber operations as a part of its deterrence posture ('cumulative deterrence').⁵⁰ His main argument is that cumulative deterrence is better suited to the characteristics of cyber conflict. Taking a different angle, Lilli delved into the role of private sector organisations in cyber deterrence.⁵¹ More specifically, he highlights benefits they can offer states, including cutting-edge technologies, competent workforce, and better access beyond national borders, but he also raises certain national security, legal, and ethical concerns with such collaboration. In a different vein, Hare puts forward a variety of practical and ethical reasons for improving precision cyberweapon systems.⁵² Finally, Cunningham pondered China's pursuit of information-age weapons, such as cyberattacks, counter-space weapons,

47 James M. Acton, 'Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War', *International Security* 43 N° 1 (2018): 56–99.

48 Florian J. Egloff and James Shires, 'Offensive Cyber Capabilities and State Violence: Three Logics of Integration', *Journal of Global Security Studies* 7 N° 1 (2022), ogab028.

49 U. Tor, "'Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* 40 N° 1–2 (2017): 92–117.

50 *Ibid.*, 94.

51 Eugenio Lilli, 'Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence', *Contemporary Security Policy* 42 N° 2 (2021): 163–88.

52 Forrest B. Hare, 'Precision Cyber Weapon Systems: An Important Component of a Responsible National Security Strategy?', *Contemporary Security Policy* 40 N° 2 (2019): 193–213.

and guided precision missiles.⁵³ She concludes that China deals with its shortcomings regarding the conventional military by combining information-age weapons with a nuclear posture.

Cybersecurity Policies and Governance

Research on cybersecurity policies and governance examines how nations can use governmental mechanisms to deal with cybersecurity issues. Research in this area can be examined under three headings: international cyber diplomacy, national cybersecurity policy, and intelligence services in cyberspace. Among studies on international cyber diplomacy, the concept of sovereignty and its definition play a central role. For instance, Shen highlights that cyberspace is built on physical structures. Drawing from the 'Tallinn Manual', which references the 1928 international law ruling in the *Island of Palmas* case, he explains that a prevailing legal viewpoint is that all information infrastructures within a nation's land, air, and sea territories come under its sovereignty, irrespective of the users' identities.⁵⁴ Furthermore, Shen considers the contrasting ways the US and China interpret and operationalise the concept of sovereignty. He argues that the US adopts a more expansionist approach, whereas China leans towards a more defensive stance. In contrast, Mueller contends that traditional definitions of sovereignty do not apply well to cyberspace.⁵⁵ Instead, he promotes a governance model based on the global commons model, which emphasises the universal common good. On the other hand, Hughes takes a more cautious stance and explains that legal arguments made regarding traditional conflicts may or may not represent conflicts in cyberspace, and it is necessary to make a new and multilateral cyber treaty.⁵⁶ In a similar vein, Mueller, Schmidt, and Kuerbis make a case for decentralised governance mechanisms for cyberspace; they propose

53 Fiona S. Cunningham, 'Strategic Substitution: China's Search for Coercive Leverage in the Information Age', *International Security* 47 N° 1 (2022): 46–92.

54 Yi Shen, 'Cyber Sovereignty and the Governance of Global Cyberspace', *Chinese Political Science Review* 1 (2016): 81–93.

55 Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 N° 4 (2020): 779–801.

56 Rex Hughes, 'A Treaty for Cyberspace', *International Affairs* 86 N° 2 (2010): 523–41.

a ‘networked governance of routing’, where no country sits at the top of the Internet hierarchy.⁵⁷

Broadening the lens, Oorsprong, Ducheine, and Pijpers investigated the right to self-defence in cyberspace, which can be considered an extension of the sovereignty debate.⁵⁸ For this purpose, using a case study of the Netherlands, they focus on better conceptualising which kinds of cyberattacks constitute a legitimate reason for war. In particular, they categorise these attacks into three types—‘cyber espionage, manipulation of the information environment, and disruption, degradation, or destruction of core security assets’—and only the third category gives a justifiable reason for starting a war.

Some studies also examine national cyber policies, although some national policies also have international implications. For example, Carr highlights that privately owned infrastructure is an essential part of national cybersecurity in the UK and the US, but there are various ambiguities in the partnership terms.⁵⁹ She proposes that the reason for this ambiguity has to do with motives: governments are reluctant to take on the responsibility of managing certain technical aspects of cybersecurity, whereas private firms do not want to be responsible for problems related to national security. Christensen and Petersen also considered the issue of motives in public–private partnerships, but delved deeper into the tension between economic interests and national security, and the disagreements stemming from different perspectives on cybersecurity.⁶⁰ They argue that by ‘partnering through dissent’—collaborating while willingly considering divergent viewpoints—public–private partnerships can lead to new and innovative solutions. Mott, Nurse, and Baker-Beall pondered the malware-based cyberattacks on

57 Milton Mueller, Andreas Schmidt, and Brenden Kuerbis, ‘Internet Security and Networked Governance in International Relations’, *International Studies Review* 15 N° 1 (2013): 86–104.

58 Ferry Oorsprong, Paul Ducheine, and Peter Pijpers, ‘Cyber-Attacks and the Right of Self-Defense: A Case Study of the Netherlands’, *Policy Design and Practice* 6 N° 2 (2023): 217–39.

59 Madeline Carr, ‘Public–Private Partnerships in National Cyber-Security Strategies’, *International Affairs* 92 N° 1 (2016): 43–62.

60 Kristoffer Kjærgaard Christensen and Karen Lund Petersen, ‘Public–Private Partnerships on Cyber Security: A Practice of Loyalty’, *International Affairs* 93 N° 6 (2017): 1435–52.

the UK during the COVID-19 pandemic and, based on their analysis, suggest ways to further improve the UK's cyber resilience.⁶¹ Carrapico and Farrand also analysed the responses to cyberattacks during the pandemic, but they focused on the EU as the context of the study, examining prior economic and security-related issues as path-dependent reasons underlying certain responses and policies.⁶²

Finally, a few studies considered the role of intelligence services. Georgieva explains that intelligence agencies today are one of the primary actors within cyberspace developing new offensive and defensive techniques.⁶³ Thus, she argues that it is important to also consider intelligence agencies and the methods they develop to prevent loopholes in regulations. In contrast, Liebetrau conducted a comparative case study of three countries to better understand how cyber capabilities can be structured in military and intelligence organisations.⁶⁴ Specifically, he uses the Netherlands as an example of organisational coordination, where offensive and defensive functions work together within a unified cyber command; he cites France as an example of organisational separation, where offensive and defensive functions work relatively independently; and he discusses Norway as an example of organisational centralisation, where the military and civilian intelligence agency either runs or coordinates not only intelligence functions but also offensive/defensive cyber functions.

Regional Issues in Cybersecurity

There are also several studies that simply focus on and analyse the broader cybersecurity context or the specific cybersecurity-related behaviours of

61 Gareth Mott, Jason R.C. Nurse, and Christopher Baker-Beall, 'Preparing for Future Cyber Crises: Lessons from Governance of the Coronavirus Pandemic', *Policy Design and Practice* 6 N° 2 (2023): 160–81.

62 Helena Carrapico and Benjamin Farrand, 'Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy', *Journal of European Integration* 42 N° 8 (2020): 1111–26.

63 Iliana Georgieva, 'The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace', *Contemporary Security Policy* 41 N° 1 (2020): 33–54.

64 Tobias Liebetrau, 'Organizing Cyber Capability across Military and Intelligence Entities: Collaboration, Separation, or Centralization', *Policy Design and Practice* 6 N° 2 (2023): 131–45.

a certain state actor. The studies in this area considered different states, although there were relatively more studies on China. To begin with, in his paper titled ‘The Impact of China on Cybersecurity: Fiction and Friction’, Lindsay put forward the argument that the Chinese cyber threat is exaggerated.⁶⁵ In particular, he suggested that China is pursuing the goal of stealing data through cyberattacks but cannot effectively benefit from the stolen data. Likewise, he argued that the cyber offence and defence capabilities of China are well below those of the US. Overall, he reckoned that China is not as dangerous a threat as most consider it to be, and China’s cyber operations are not critical enough to destabilise US–China relations. Following this publication, a letter to the editor by Brenner and a response to that letter by Lindsay were published under the title ‘Debating the Chinese Cyber Threat’.⁶⁶ Brenner argued that Lindsay did not consider some other issues. For example, he asserted that Lindsay focused primarily on military-to-military cyber conflicts, whereas it is also possible for China to target the US civilian computer systems, which are much more vulnerable.⁶⁷ Lindsay responded to this by arguing that ‘incentives for restraint in cyberspace make it better suited for intelligence operations than for coercive diplomacy or strategic attack’.⁶⁸ The paper by Gilli and Gilli introduced a different perspective into this debate by considering whether the imitation efforts by other countries—especially Chinese reverse engineering and cyber espionage—would allow them to reach the US’s level regarding advanced weapons systems.⁶⁹ They opposed Gerschenkron’s⁷⁰ idea that ‘economic backwardness’ provides countries with a substantial advantage of being able to freely imitate more developed countries’ technologies. In particular, they posited that—due to the increasing technological complexity—imitating through reverse

65 Jon R. Lindsay, ‘The Impact of China on Cybersecurity: Fiction and Friction’, *International Security* 39 N° 3 (2014): 7–47.

66 Joel Brenner and Jon R. Lindsay, ‘Correspondence: Debating the Chinese Cyber Threat’, *International Security* 40 N° 1 (2015): 191–95.

67 *Ibid.*, 191.

68 *Ibid.*, 194.

69 Andrea Gilli and Mauro Gilli, ‘Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage’, *International Security* 43 N° 3 (2018): 141–89.

70 Alexander Gerschenkron, *Economic Backwardness in Historical Perspective* (Cambridge: Belknap Press of Harvard University Press, 1962).

engineering today is more difficult than it was in the past, and that even cyber espionage does not make imitation sufficiently easy.

The rest of the papers focus on cybersecurity issues in other countries and regions. Stoddard pondered the question of how the UK's critical national infrastructure can be better protected from cyberattacks.⁷¹ In particular he explains that the UK has four key structures of power—the parliament, military, police, and judiciary—and these structures are targeted by an increasing number of domestic and international threat actors (ranging from low-level 'script kiddy' criminals to advanced persistent threats). He argues that to build cyber resilience the UK must improve its coordination with its allies and with the private sector, especially with the owner-operators of the critical national infrastructure. In a different vein, focusing on Estonia following the 2007 cyberattacks, Crandall and Allen pondered specifically the question of how smaller states can engage in 'norm entrepreneurship'—that is, affecting the norms of the larger structures in which they are embedded, such as NATO.⁷² They explain that by 'both dramatizing and raising the issue' and successfully using the platform NATO provides, Estonia influenced the cybersecurity norms and mentalities of NATO member countries. Additionally, in their content analysis study, Kari and Pynnöniemi considered Russian strategic culture.⁷³ They observe that Russia views itself as a technologically limited nation surrounded by enemies, and its decisions about cyberspace are heavily influenced by these views. The remaining studies in the sample focus on the EU,⁷⁴ Japan,⁷⁵ and Africa⁷⁶

71 Kristan Stoddard, 'UK Cyber Security and Critical National Infrastructure Protection', *International Affairs* 92 No 5 (2016): 1079–1105.

72 Matthew Crandall and Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy* 36 No 2 (2015): 346–68.

73 Martti J. Kari and Katri Pynnöniemi, 'Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception', *Journal of Strategic Studies* 46 No 1 (2023): 56–84.

74 George Christou, 'The Collective Securitisation of Cyberspace in the European Union', *West European Politics* 42 No 2 (2019): 278–301.

75 Paul Kallender and Christopher W. Hughes, 'Japan's Emerging Trajectory as a "Cyber Power": From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies* 40 No 1–2 (2017): 118–45.

76 Nnenna Ifeanyi-Ajufo, 'Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation', *Policy Design and Practice* 6 No 2 (2023): 146–59.

as the subjects of study, attempting to gain insights into how they deal with cybersecurity-related issues.

Miscellaneous

The six categories previously discussed capture most of the cybersecurity studies in political science and international relations, but there was a small group of studies that did not fit into any of these themes. These studies, while not yet forming coherent streams of research, are valuable due to the different insights they provide, and they constitute new research directions that can turn into larger streams of research in the near future.

These studies typically either incorporate a different philosophical perspective into the cybersecurity dialogue or add to the nomological framework of cybersecurity by examining a new antecedent or outcome. Betz and Stevens argue that theorising by means of different analogical reasoning techniques can help to better represent cybersecurity-related phenomena, and they exemplify the use of this technique employing spatial and biological analogies and metaphors.⁷⁷ Building on and extending this idea, Branch examines the role of language and metaphors to gain insight into how these affect how the US military conceptualises cybersecurity-related issues.⁷⁸ He argues that the use of spatial metaphors, such as ‘cyberspace’, is a key factor that has compelled the US to further militarise the digital realm and eventually led to the creation of the US Cyber Command.⁷⁹ Highlighting a different facet, Fouad begins her paper by noting that most studies on cybersecurity are written from an anthropocentric perspective and that there is value in considering the issue from a constructionist perspective, where the human co-creates security versus vulnerability together with the non-human elements.⁸⁰

77 David J. Betz and Tim Stevens, ‘Analogical Reasoning and Cyber Security’, *Security Dialogue* 44 N° 2 (2013): 147–64.

78 Jordan Branch, ‘What’s in a Name? Metaphors and Cybersecurity’, *International Organization* 75 N° 1 (2021): 39–70.

79 *Ibid.*, 59.

80 Noran Shafik Fouad, ‘The Non-anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity’, *Review of International Studies* 48 N° 4 (2022): 766–85.

Then, building on this idea, she proposes a new perspective she calls ‘emergent security’, referring to the complex, unpredictable, and non-linear nature of cybersecurity and the difficulties of predicting the dynamic interactions among different subsystems of a broader system over time.

Beyond that, Hansen and Nissenbaum based their paper on the securitisation theory from the Copenhagen School, which defines ‘securitisation’ as the political act of framing an issue as a significant threat, hence elevating its importance. Drawing upon their case study on the 2007 attacks in Estonia, Hansen and Nissenbaum discuss and demonstrate three concepts stemming from the securitisation theory.⁸¹ In particular, ‘hypersecuritization’ refers to political actors’ exaggeration of threats to make them appear more exigent than they are. ‘Everyday security practice’ refers to political actors veering from the public’s everyday experiences to increase compliance with security measures and boost the credibility of hypersecuritisation scenarios. ‘Technification’ refers to the political actors’ use of experts regarding issues that are impenetrable for the public due to their technical nature (e.g. cybersecurity) to manage the priority the public gives to those issues. In contrast to the previous macro-level perspective, Shandler, Gross, and Canetti took a micro-foundations perspective and examined how the lack of Internet access (‘Internet deprivation’) affects engagement in political activities.⁸² In particular they discuss a behavioural experiment they conducted with sixty university students based on the ‘scavenger hunt’ game. They found that Internet deprivation is negatively related to the completion of tasks related to political expression and association.

Overall, these papers represent the less-explored venues of cybersecurity research in political science and international relations journals. They also demonstrate that introducing alternative philosophical perspectives, theory-building approaches, and concepts can help gain a more fine-grained understanding of cybersecurity-related phenomena.

81 Lene Hansen and Helen Nissenbaum, ‘Digital Disaster, Cyber Security, and the Copenhagen School’, *International Studies Quarterly* 53 N° 4 (2009): 1155–75.

82 Ryan Shandler, Michael L. Gross, and Daphna Canetti, ‘Can You Engage in Political Activity without Internet Access? The Social Effects of Internet Deprivation’, *Political Studies Review* 18 N° 4 (2020): 620–29.

Discussion

In this study I have conducted a scoping review of cybersecurity research in the fields of political science and international relations. My primary objective was to consolidate key insights from this emerging body of literature to promote a coherent and cumulative research dialogue. The analysis of the 113 papers in this domain suggests that they can be categorised into seven distinct research areas, which then further align with the two overarching headings of strategic communications and digital geopolitics. The ensuing discussion highlights some underexplored areas identified in this review, which constitute promising avenues for future research.

First, while some experimental studies in this literature employed behavioural constructs, several classes of psychological variables are not yet examined in this area, which presents opportunities for future research. Currently the traits and individual differences perspective⁸³ is mostly missing from the discussion; however, a better understanding of these chronic variables would help explain long-term behaviours and tendencies (such as reactions to cybersecurity-related events) at the individual level. Moreover, it is possible to scrape psychological traits and individual differences (personality traits, dark-triad personality traits, and chronic regulatory focus) and some physiological/biological traits and individual differences (e.g. certain ratios, such as the facial width-to-height ratio) from public sources, such as individuals' social media profiles.⁸⁴ This allows for big data analysis that can help mitigate the effects of malicious social communications campaigns. Some other psychological perspectives that would be useful for understanding cybersecurity-related phenomena, such as public responses to cybersecurity incidents, would

83 Aybars Tuncdogan, Oguz Ali Acar, and Daan Stam, 'Individual Differences as Antecedents of Leader Behavior: Towards an Understanding of Multi-level Outcomes', *Leadership Quarterly* 28 N° 1 (2017): 40–64.

84 Ji Wu, Liqiang Huang, and J. Leon Zhao, 'Operationalizing Regulatory Focus in the Digital Age: Evidence from an E-Commerce Context', *MIS Quarterly* 43 N° 3 (2019): 745–64. Michael M. Tadesse, Hongfei Lin, Bo Xu, and Liang Yang, 'Personality Predictions Based on User Behavior on the Facebook Social Media Platform', *IEEE Access* 6 (2018): 61959–69.

include social identity theory,⁸⁵ terror management theory,⁸⁶ and the elaboration likelihood model.⁸⁷

Second, many questions are being asked in this area about collective information processing and decision-making, such as how a state internally makes attributions regarding cyberattacks, how governments respond to cyberattacks, and how military organisations prepare themselves against cyberattacks. However, what is currently more limited in the literature is the ‘performance management’ aspect. How can the internal attributions of a state regarding cyberattacks be made more precise? How can governments better respond to cyberattacks, both in terms of the effectiveness of deterrence and bolstering public trust? What kinds of internal and external organisational structures should military organisations enact to become aware of cyberattacks promptly and respond effectively? Some of these questions would benefit from research conducted at lower levels of analysis, such as at the organisational level. Organisational design elements (such as centralisation, formalisation, and connectedness),⁸⁸ network structure (such as strong and weak links with other organisations), and the network position of the state agency or military body are likely to play a role in its cybersecurity effectiveness. Likewise, the organisation of the dynamic capabilities⁸⁹ of the state agency or military body—referring to the structures that regularly sense changes in the environment, develop appropriate solutions, and accordingly

-
- 85 Michael A. Hogg and Deborah I. Terry, ‘Social Identity and Self-Categorization Processes in Organizational Contexts’, *Academy of Management Review* 25 N° 1 (2000): 121–40. M.J. Hornsey, ‘Social Identity Theory and Self-Categorization Theory: A Historical Review’, *Social and Personality Psychology Compass* 2 N° 1 (2008): 204–22.
- 86 Brian L. Burke, Andy Martens, and Erik H. Faucher, ‘Two Decades of Terror Management Theory: A Meta-analysis of Mortality Salience Research’, *Personality and Social Psychology Review* 14 N° 2 (2010): 155–95.
- 87 Richard E. Petty, Pablo Brinol, and Joseph R. Priester, ‘Mass Media Attitude Change: Implications of the Elaboration Likelihood Model of Persuasion’, in *Media Effects*, Jennings Bryant and Mary Beth Oliver (eds), (Routledge, 2009), pp. 141–80.
- 88 Aybars Tuncdogan, A.D. Boon, Tom Mom, Frans Van Den Bosch, and Henk Volberda, ‘Management Teams’ Regulatory Foci and Organizational Units’ Exploratory Innovation: The Mediating Role of Coordination Mechanisms’, *Long Range Planning* 50 N° 5 (2017): 621–35.
- 89 Teece, David J., ‘Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance’, *Strategic Management Journal* 28 N° 13 (2007): 1319–50. Aybars Tuncdogan, Adam Lindgreen, Henk Volberda, and Frans van den Bosch, ‘A Brief Look at the Strategic Renewal Literature’, in *Strategic Renewal*, Aybars Tuncdogan et al. (eds), (Routledge, 2019), pp. 3–18. Aybars Tuncdogan and William Shiue, ‘Dynamic Capabilities’, in *Encyclopedia of Tourism Management and Marketing*, D. Buhalis (ed.), (Edward Elgar, 2020).

update the modus operandi of the operating capabilities—would play an important role in the speed and effectiveness of both offensive and defensive capabilities.

Third, an interesting finding in the Kostyuk and Wayne study⁹⁰ was that while individuals in the personal-threat condition of the experiment indicated that they would engage more in safer online security behaviours, in neither the national-threat nor the personal-threat conditions was there any significant difference as opposed to the control group. The authors note that ‘simple exposure to a cyber operation may not be enough to change actual online behaviour, even if citizens’ perception of risk was temporarily heightened and they expressed a willingness to change their behaviour’.⁹¹ Similarly, they found that people do not necessarily perceive national threats as personal ones; for example, in contrast to the personal-threat condition, in the national-threat condition, the participants remained unchanged in terms of their willingness to practise online safety (possibly because they do not individually assume responsibility against macro-level threats). Considering that Kostyuk and Wayne also posit that individual risk perceptions and behaviours form the basis of cybersecurity at higher levels of analysis, it is important for future researchers to elucidate factors and interventions that will effect lasting change in citizens’ online safety behaviours.

Fourth, simply because most streams of cybersecurity literature within political science and international relations are still quite young—with approximately two-thirds of all articles published in the last five years, as previously discussed—many outcome variables are not yet examined sufficiently or at all. In most of the seven themes discussed, there are studies where public perceptions play a crucial role, sometimes because public perceptions are affected by cyber incidents and sometimes because public perceptions affect other outcomes, such as cybersecurity policies and the likelihood and type of retribution following a cyberattack. However, there are also several other constructs related to public

90 Kostyuk and Wayne, ‘Microfoundations of State Cybersecurity’.

91 *Ibid.*, 17.

perceptions not yet examined. An interesting question is, precisely how does a cybersecurity incident affect the public image of the governing political party? For instance, how were specific perceptions towards the governing party affected when the WannaCry ransomware attack on Britain's National Health Service happened in 2017,⁹² and if there were significant negative effects, how long did they last? One way to examine this underexplored outcome variable would be by using the brand personality construct, which describes how a brand is perceived in terms of responsibility, activity, emotionality, aggressiveness, and simplicity.⁹³ Likewise, other countries' perceptions of a country can also be affected by cyberattacks. For instance, precisely how did the portrayals of Estonia change in foreign media outlets and military publications after digital attacks petrified its digital infrastructure in 2007, and how long did this change last?⁹⁴ Again, the concept of brand personality and other constructs from the literature on social cognition (universal dimensions of social cognition⁹⁵) could help answer this question. Another relatively underexplored aspect is when a cyber security incident is viewed as an unexpected disaster by the public, and when various governmental entities and organisations cooperating with them are harshly blamed. There are various existing lines of thought in the literature on corporate social irresponsibility⁹⁶ which could be useful in elucidating the drivers of these outcomes. Building on these ideas could help accelerate the growth and explanatory power of the emerging cybersecurity literature in the political science and international relations fields.

-
- 92 Guy Martin, Saira Ghafur, James Kinross, Chris Hankin, and Ara Darzi, 'WannaCry—A Year On', *BMJ* 361 (2018). Nolen Scaife, Patrick Traynor, and Kevin Butler, 'Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)', *IEEE Potentials* 36 N° 6 (2017): 28–31.
 - 93 Aybars Tuncdogan and Henk W. Volberda, 'The Effects of Perceived Corporate Brand Personality on Individuals' Exploration and Exploitation Orientations: The Moderating Role of Self-Brand Connection', *R&D Management* 50 N° 2 (2020): 188–97.
 - 94 Michael Lesk, 'The New Front Line: Estonia under Cyberassault', *IEEE Security & Privacy* 5 N° 4 (2007): 76–79.
 - 95 Susan T. Fiske, Amy J.C. Cuddy, and Peter Glick, 'Universal Dimensions of Social Cognition: Warmth and Competence', *Trends in Cognitive Sciences* 11 N° 2 (2007): 77–83.
 - 96 Paolo Antonetti, Benedetta Crisafulli, and Aybars Tuncdogan, "Just Look the Other Way": Job Seekers' Reactions to the Irresponsibility of Market-Dominant Employers', *Journal of Business Ethics* 174 (2021): 403–22.

Finally, there are some methodological issues that future research should consider. There are relatively few experimental studies in this area, and most of them are based on cross-sectional data collected from student samples. While this does not necessarily undermine the importance of these studies, the use of multi-wave or longitudinal data from representative samples would help to improve the internal and external validity of the findings in this area. Similarly, in line with recent developments, some use of newer data collection techniques, such as eye tracking⁹⁷ and electroencephalography,⁹⁸ would provide novel insights. Furthermore, most areas of cybersecurity research lack overarching integrative theoretical frameworks. To address this, qualitative studies—especially those that build frameworks based on observations from data (such as the grounded theory approach⁹⁹)—could be useful.

References

- Ablon, Lillian, and Andy Bogart, *Zero Days, Thousands of Nights* (Santa Monica, CA: RAND Corporation, 2017).
- Acton, James M., 'Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War', *International Security* 43 N° 1 (2018): 56–99.
- Agarwal, Nitin, and Kiran Kumar Bandeli, 'Examining Strategic Integration of Social Media Platforms in Disinformation Campaign Coordination', *Defence Strategic Communications* 4 N° 1 (2018): 173–206.
- Agarwal, Nitin, Samer Al-Khateeb, Rick Galeano, and Rebecca Goolsby, 'Examining the Use of Botnets and Their Evolution in Propaganda Dissemination', *Defence Strategic Communications* 2 N° 1 (2017): 87–112.
- Antonetti, Paolo, Benedetta Crisafulli, and Aybars Tuncdogan, "'Just Look the Other Way": Job Seekers' Reactions to the Irresponsibility of Market-Dominant Employers', *Journal of Business Ethics* 174 (2021): 403–22.
- Betz, David J., and Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue* 44 N° 2 (2013): 147–64.
- BlackRock, *Geopolitical Risk Dashboard*, BlackRock, 25 July 2023.
- Branch, Jordan, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75 N° 1 (2021): 39–70.
- Brenner, Joel, and Jon R. Lindsay, 'Correspondence: Debating the Chinese Cyber Threat', *International Security* 40 N° 1 (2015): 191–95.
-
- 97 Ming Chen, Raymond R. Burke, Sam K. Hui, and Alex Leykin, 'Understanding Lateral and Vertical Biases in Consumer Attention: An In-store Ambulatory Eye-Tracking Study', *Journal of Marketing Research* 58 N° 6 (2021): 1120–41.
- 98 Ariel Telpaz, Ryan Webb, and Dino J. Levy, 'Using EEG to Predict Consumers' Future Choices', *Journal of Marketing Research* 52 N° 4 (2015): 511–29.
- 99 Barney G. Glaser and Anselm L. Strauss, *Discovery of Grounded Theory: Strategies for Qualitative Research* (Routledge, 2017).

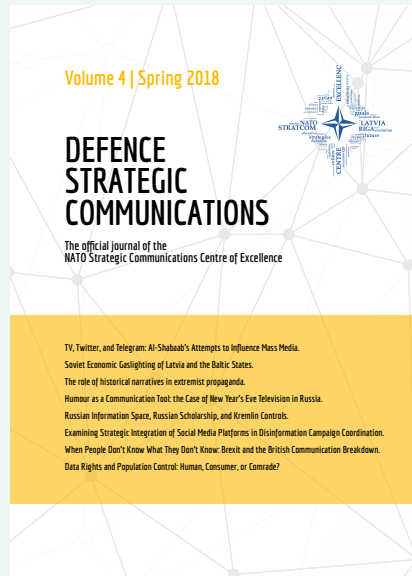
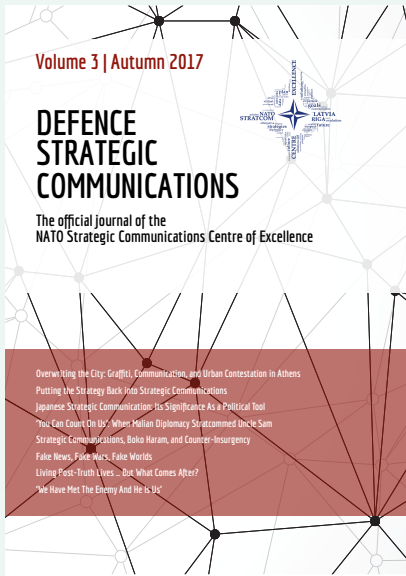
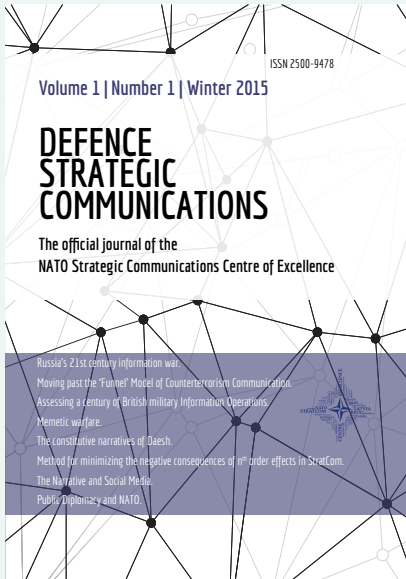
- Burke, Brian L., Andy Martens, and Erik H. Faucher, 'Two Decades of Terror Management Theory: A Meta-analysis of Mortality Salience Research', *Personality and Social Psychology Review* 14 N° 2 (2010): 155–95.
- Carr, Madeline, 'Public–Private Partnerships in National Cyber-Security Strategies', *International Affairs* 92 N° 1 (2016): 43–62.
- Carrapico, Helena, and Benjamin Farrand, 'Discursive Continuity and Change in the Time of Covid-19: the Case of EU Cybersecurity Policy', *Journal of European Integration* 42 N° 8 (2020): 1111–26.
- Chen, Ming, Raymond R. Burke, Sam K. Hui, and Alex Leykin, 'Understanding Lateral and Vertical Biases in Consumer Attention: An In-store Ambulatory Eye-Tracking Study', *Journal of Marketing Research* 58 N° 6 (2021): 1120–41.
- Cheung-Blunden, Violet, and Jiarun Ju, 'Anxiety as a Barrier to Information Processing in the Event of a Cyberattack', *Political Psychology* 37 N° 3 (2016): 387–400.
- Chiappetta, Andrea, 'Digital Geopolitics: The New Global Challenge', in *The Palgrave Handbook of Global Social Change*, R. Baikady et al. (eds), (Cham: Springer International, 2022), pp. 1–18.
- Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen, 'Public–Private Partnerships on Cyber Security: A Practice of Loyalty', *International Affairs* 93 N° 6 (2017): 1435–52.
- Christou, George, 'The Collective Securitisation of Cyberspace in the European Union', *West European Politics* 42 N° 2 (2019): 278–301.
- Conduit, Dara, 'Digital Authoritarianism and the Devolution of Authoritarian Rule: Examining Syria's Patriotic Hackers', *Democratization* (2023): 1–19.
- Crandall, Matthew, and Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy* 36 N° 2 (2015): 346–68.
- Cunningham, Fiona S., 'Strategic Substitution: China's Search for Coercive Leverage in the Information Age', *International Security* 47 N° 1 (2022): 46–92.
- Czerny, Milàn, 'Selective Law Enforcement on the RuNet as a Tool of Strategic Communications', *Defence Strategic Communications* 9 N° 9 (2020): 53–85.
- Dunn Cavelti, Myriam, and Andreas Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science', *Contemporary Security Policy* 41 N° 1 (2020): 5–32.
- Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, 'Strategic Aspects of Cyberattack, Attribution, and Blame', *Proceedings of the National Academy of Sciences* 114 N° 11 (2017): 2825–30.
- Egloff, Florian J., 'Contested Public Attributions of Cyber Incidents and the Role of Academia', *Contemporary Security Policy* 41 N° 1 (2020): 55–81.
- Egloff, Florian J., and James Shires, 'Offensive Cyber Capabilities and State Violence: Three Logics of Integration', *Journal of Global Security Studies* 7 N° 1 (2022), ogab028.
- Egloff, Florian J., and Max Smeets, 'Publicly Attributing Cyber Attacks: A Framework', *Journal of Strategic Studies* 46 N° 3 (2023): 502–33.
- Eisenberg, A.E., J. Baron, and M.E. Seligman, 'Individual Differences in Risk Aversion and Anxiety', *Psychological Bulletin* 87 N° 1 (1998): 245–51.
- Fiske, Susan T., Amy J.C. Cuddy, and Peter Glick, 'Universal Dimensions of Social Cognition: Warmth and Competence', *Trends in Cognitive Sciences* 11 N° 2 (2007): 77–83.
- Fouad, Noran Shafik, 'The Non-anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity', *Review of International Studies* 48 N° 4 (2022): 766–85.
- Franchi, Tássio, and Leonardo Vichi, 'The Beginning of Warfare on the Internet: Zapatista Strategic Communications', *Defence Strategic Communications* 6 (2019): 123–54.
- Georgieva, Iliana, 'The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace', *Contemporary Security Policy* 41 N° 1 (2020): 33–54.
- Gerschenkron, Alexander, *Economic Backwardness in Historical Perspective* (Cambridge: Belknap Press of Harvard University Press, 1962).

- Gilli, Andrea, and Mauro Gilli, 'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security* 43 N° 3 (2018): 141–89.
- Glaser, Barney G., and Anselm L. Strauss, *Discovery of Grounded Theory: Strategies for Qualitative Research* (Routledge, 2017).
- Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen, 'State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation', *International Affairs* 94 N° 5 (2018): 975–94.
- Guenther, Lindsey, and Paul Musgrave, 'New Questions for an Old Alliance: NATO in Cyberspace and American Public Opinion', *Journal of Global Security Studies* 7 N° 4 (2022), ogac024.
- Hacıyakopoglu, Gulizar, 'The "Fake News" Label and Politicisation of Malaysia's Elections', *Defence Strategic Communications* 5 N° 5 (2018): 87–128.
- Hansen, Lene, and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53 N° 4 (2009): 1155–75.
- Hare, Forrest B., 'Precision Cyber Weapon Systems: An Important Component of a Responsible National Security Strategy?', *Contemporary Security Policy* 40 N° 2 (2019): 193–213.
- Hogg, Michael A., and Deborah I. Terry, 'Social Identity and Self-Categorization Processes in Organizational Contexts', *Academy of Management Review* 25 N° 1 (2000): 121–40.
- Holmstrom, Miranda, 'The Narrative and Social Media', *Defence Strategic Communications* 1 N° 1 (2015): 118–32.
- Hornsey, Matthew J., 'Social Identity Theory and Self-Categorization Theory: A Historical Review', *Social and Personality Psychology Compass* 2 N° 1 (2008): 204–22.
- Hughes, Rex, 'A Treaty for Cyberspace', *International Affairs* 86 N° 2 (2010): 523–41.
- Ifeanyi-Ajufo, Nnenna, 'Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation', *Policy Design and Practice* 6 N° 2 (2023): 146–59.
- Jensen, Benjamin, Brandon Valeriano, and Ryan Maness, 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist', *Journal of Strategic Studies* 42 N° 2 (2019): 212–34.
- Kallender, Paul, and Christopher W. Hughes, 'Japan's Emerging Trajectory as a "Cyber Power": From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies* 40 N° 1–2 (2017): 118–45.
- Kari, Martti J., and Katri Pynnöniemi, 'Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception', *Journal of Strategic Studies* 46 N° 1 (2023): 56–84.
- Kello, Lucas, 'The Meaning of the Cyber Revolution: Perils of Theory and Statecraft', *International Security* 38 N° 2 (2013): 7–40.
- Kostyuk, Nadiya, and Carly Wayne, 'The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public', *Journal of Global Security Studies* 6 N° 2 (2021), ogz077.
- Kurowska, Xymena, and Anatoly Reshetnikov, 'Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization', *Security Dialogue* 49 N° 5 (2018): 345–63.
- Leal, Marcelo M., and Paul Musgrave, 'Backwards from Zero: How the US Public Evaluates the Use of Zero-Day Vulnerabilities in Cybersecurity', *Contemporary Security Policy* 44 N° 3 (2023): 437–61.
- Leal, Marcelo, and Paul Musgrave, 'Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks', *Foreign Policy Analysis* 18 N° 2 (2022), orac003.
- Leal, Marcelo M., and Paul Musgrave, 'Hitting Back or Holding Back in Cyberspace: Experimental Evidence regarding Americans' Responses to Cyberattacks', *Conflict Management and Peace Science* 40 N° 1 (2023): 42–64.
- Lee, Heajune, 'Public Attribution in the US Government: Implications for Diplomacy and Norms in Cyberspace', *Policy Design and Practice* 6 N° 2 (2023): 198–216.
- Lesk, Michael, 'The New Front Line: Estonia under Cyberassault', *IEEE Security & Privacy* 5 N° 4 (2007): 76–79.
- Liebetrau, Tobias, 'Organizing Cyber Capability across Military and Intelligence Entities: Collaboration, Separation, or Centralization', *Policy Design and Practice* 6 N° 2 (2023): 131–45.

- Lilli, Eugenio, 'Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence', *Contemporary Security Policy* 42 N° 2 (2021): 163–88.
- Lindsay, Jon R., 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39 N° 3 (2014): 7–47.
- Lutscher, Philipp M., Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti, 'At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Nondemocratic Regimes', *Journal of Conflict Resolution* 64 N° 2–3 (2020): 373–401.
- MacWilliam, Ian, 'Islamic State and Jihadist Media Strategies in the Post-Soviet Region', *Defence Strategic Communications* 9 (2021): 15–52.
- Martin, Guy, Saira Ghafur, James Kinross, Chris Hankin, and Ara Darzi, 'WannaCry—A Year On', *BMJ* 361 (2018).
- Maschmeyer, Lennart, 'Subversion, Cyber Operations, and Reverse Structural Power in World Politics', *European Journal of International Relations* 29 N° 1 (2023): 79–103.
- McGraw, Gary, 'Cyber War Is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36 N° 1 (2013): 109–19.
- Mott, Gareth, Jason R.C. Nurse, and Christopher Baker-Beall, 'Preparing for Future Cyber Crises: Lessons from Governance of the Coronavirus Pandemic', *Policy Design and Practice* 6 N° 2 (2023): 160–81.
- Mueller, Milton L., 'Against Sovereignty in Cyberspace', *International Studies Review* 22 N° 4 (2020): 779–801.
- Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis, 'Internet Security and Networked Governance in International Relations', *International Studies Review* 15 N° 1 (2013): 86–104.
- NATO, 'Deterrence and Defence', 10 October 2023.
- NATO, 'Multi-Domain Operations in NATO—Explained', 5 October 2023.
- NATO Strategic Communications Centre of Excellence, 'About Strategic Communications', 11 November 2023.
- Oorsprong, Ferry, Paul Ducheine, and Peter Pijpers, 'Cyber-Attacks and the Right of Self-Defense: a Case Study of the Netherlands', *Policy Design and Practice* 6 N° 2 (2023): 217–39.
- Petty, Richard E., Pablo Brinol, and Joseph R. Priester, 'Mass Media Attitude Change: Implications of the Elaboration Likelihood Model of Persuasion', in *Media Effects*, Jennings Bryant and Mary Beth Oliver (eds), (Routledge, 2009), pp. 141–80.
- Poznansky, Michael, and Evan Perkoski, 'Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution', *Journal of Global Security Studies* 3 N° 4 (2018): 402–16.
- Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35 N° 1 (2012): 5–32.
- Rid, Thomas, and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38 N° 1–2 (2015): 4–37.
- S&P Global, 'Top Geopolitical Risks of 2023', S&P Global, 2023.
- Scaife, Nolen, Patrick Traynor, and Kevin Butler, 'Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)', *IEEE Potentials* 36 N° 6 (2017): 28–31.
- Schulzke, Marcus, 'The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty', *Perspectives on Politics* 16 N° 4 (2018): 954–68.
- Shandler, Ryan, Michael L. Gross, and Daphna Canetti, 'Can You Engage in Political Activity without Internet Access? The Social Effects of Internet Deprivation', *Political Studies Review* 18 N° 4 (2020): 620–29.
- Shandler, Ryan, Michael L. Gross, and Daphna Canetti, 'A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel', *Contemporary Security Policy* 42 N° 2 (2021): 135–62.
- Shandler, Ryan, Michael L. Gross, Sophia Backhaus, and Daphna Canetti, 'Cyber Terrorism and Public Support for Retaliation—A Multi-country Survey Experiment', *British Journal of Political Science* 52 N° 2 (2022): 850–68.
- Shen, Yi, 'Cyber Sovereignty and the Governance of Global Cyberspace', *Chinese Political Science Review* 1 (2016): 81–93.
- Shires, James, 'Cyber-Noir: Cybersecurity and Popular Culture', *Contemporary Security Policy* 41 N° 1 (2020): 82–107.

- Smeets, Max, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 41 N° 1–2 (2018): 6–32.
- Speckhard, Anne, Ardian Shajkovi, and Mohamed Ahmed, 'Intervening in and Preventing Somali-American Radicalization with Counter Narratives', *Journal of Strategic Security* 11 N° 4 (2018): 32–71.
- Stevens, Clare, 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet', *Contemporary Security Policy* 41 N° 1 (2020): 129–52.
- Stoddart, Kristan, 'UK Cyber Security and Critical National Infrastructure Protection', *International Affairs* 92 N° 5 (2016): 1079–1105.
- Tadesse, Michael M., Hongfei Lin, Bo Xu, and Liang Yang, 'Personality Predictions Based on User Behavior on the Facebook Social Media Platform', *IEEE Access* 6 (2018): 61959–69.
- Tanczer, Leonie Maria, '50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers', *Contemporary Security Policy* 41 N° 1 (2020): 108–28.
- Teece, David J., 'Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance', *Strategic Management Journal* 28 N° 13 (2007): 1319–50.
- Telpaz, Ariel, Ryan Webb, and Dino J. Levy, 'Using EEG to Predict Consumers' Future Choices', *Journal of Marketing Research* 52 N° 4 (2015): 511–29.
- Tor, U., "'Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* 40 N° 1–2 (2017): 92–117.
- Tuncdogan, Aybars, Oguz Ali Acar, and Daan Stam, 'Individual Differences as Antecedents of Leader Behavior: Towards an Understanding of Multi-level Outcomes', *Leadership Quarterly* 28 N° 1 (2017): 40–64.
- Tuncdogan, Aybars, A.D. Boon, Tom Mom, Frans Van Den Bosch, and Henk Volberda, 'Management Teams' Regulatory Foci and Organizational Units' Exploratory Innovation: The Mediating Role of Coordination Mechanisms', *Long Range Planning* 50 N° 5 (2017): 621–35.
- Tuncdogan, Aybars, and Aidan Hughes, 'Guiding Word-Of-Mouth (WOM) through Organic Social Media for Effective Strategic Communications: A Literature Review', *Defence Strategic Communications* 11 (2022): 115–50.
- Tuncdogan, Aybars, Adam Lindgreen, Henk Volberda, and Frans van den Bosch, 'A Brief Look at the Strategic Renewal Literature', in *Strategic Renewal*, Aybars Tuncdogan et al. (eds), (Routledge, 2019), pp. 3–18.
- Tuncdogan, Aybars, and William Shiue, 'Dynamic Capabilities', in *Encyclopedia of Tourism Management and Marketing*, D. Buhalis (ed.), (Edward Elgar, 2020).
- Tuncdogan, Aybars, and Henk W. Volberda, 'The Effects of Perceived Corporate Brand Personality on Individuals' Exploration and Exploitation Orientations: The Moderating Role of Self-Brand Connection', *R&D Management* 50 N° 2 (2020): 188–97.
- Valeriano, Brandon, and Ryan C. Maness, 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11', *Journal of Peace Research* 01 N° 3 (2014): 347–60.
- World Economic Forum, *The Global Risks Report 2023*, 18th edn (WEF, 2023).
- Wu, Ji, Liqiang Huang, and J. Leon Zhao, 'Operationalizing Regulatory Focus in the Digital Age: Evidence from an E-Commerce Context', *MIS Quarterly* 43 N° 3 (2019): 745–64.

Read all back copies
stratcomcoe.org/publications




Read all back copies
stratcomcoe.org/publications

Volume 5 | Autumn 2018

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence



The Acoustic World of Influence: How Musicology Illuminates Strategic Communications
Hostile Gatekeeping: the Strategy of Engaging With Journalists in Extremism Reporting
The 'Fake News' Label and Politicisation of Malaysia's Elections
Brand Putin: an Analysis of Vladimir Putin's Projected Images
What Does it Mean for a Communication to be Truified?
Strategic Communications at the Pyeongchang Winter Olympics: a Groundwork Study

ISSN: 2500-8486
DOI: 10.1096/2018.RSCA.5

Volume 6 | Spring 2019

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence




How the global war on terror killed the prospect of justice for Kenyan victims of violence
Analysing Strategic Communications through early modern theatre
Strategic Communications as a tool for great power politics in Venezuela
The beginning of warfare on the internet: Zapulista Strategic Communications
Measuring the effect of Russian Internet Research Agency information operations in online conversations
Reverse engineering Russian Internet Research Agency tactics through network analysis
From swarms to ping-pongs: time for a CVE step-change?
On finding the ethical in the age of digital battle spaces

ISSN: 2500-8486
DOI: 10.1096/2019.RSCA.6

Volume 7 | Autumn 2019

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence




Cyril Ramaphosa's Strategic Presidency
Sanctions—Strategic Miscommunications? The Case of Iran
Blue Amazon: Brazil's Maritime Vocation
Global Rorschach Test: Responding to China's Belt & Road Initiative
War and Truth
The Elephant in The Room: Measurement of Effect

ISSN: 2500-8486
DOI: 10.1096/2019.RSCA.7

Volume 8 | Spring 2020

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence



A Rise By Any Other Name?—Strategic Communications in Israel
Shaping an Antarctic Identity in Argentina and Chile
Disinformation's Societal Impact: Britain, Covid, And Beyond
Understanding Fake News: A Bibliographic Perspective
Under The Security Umbrella: Japan's Weak Stayingpower to the World
AI Ethics: A Strategic Communications Challenge
Communicating Threat in An Era of Speed and Fetishised Technology


ISSN: 2500-8486
DOI: 10.1096/2020.RSCA.8

Read all back copies
stratcomcoe.org/publications

Volume 9 | Autumn 2020

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
 NATO Strategic Communications Centre of Excellence




Islamic State and Jihadist Media Strategies in the Post-Soviet Region
 Selective Law Enforcement on the Internet as a Tool of Strategic Communications
 Capitalism, Communications, and the Corps: Iran's Revolutionary Guard and the Communications Economy
 'Climate Emergency': How Emergency Framing Affects The United Kingdom's Climate Governance
 The Long Decade of Disinformation
 The Rise of Anxiety Propaganda: Reflections on a Changing World

ISSN: 2500-0486
 DOI: 10.3999/0318-RSCA.9

Volume 10 | Spring - Autumn 2021

DEFENCE STRATEGIC COMMUNICATIONS

The official Journal of the
 NATO Strategic Communications Centre of Excellence



The Birth and Coming of Age of NATO Stratcom: A Personal History
 How US Government Fell in and Out of Love with Strategic Communications
 Insights into PRC External Propaganda
 The Role of the 1990s in the Kremlin's Strategic Communications
 Strategic Communications in History: The Emperor Augustus
 Pipeline of Influence: Nord Stream 2 and Informationsmatters Vienna
 Emotion and Empathy in Germany's 2015 Refugee Crisis
 Analysis of Kremlin Disinformation Campaigns after the Poisoning of Alexei Navalny
 Rhetorical Agency: Considerations from Africa
 National Identity Construction and History Textbooks in Post-Yugoslav Montenegro
 Billionaire Royal Advances, Trading Bats
 Saying Goodbye to the (Post-) Soviet Union?

SPECIAL EDITION

Volume 11 | Autumn 2022

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
 NATO Strategic Communications Centre of Excellence

Shot by Both Sides: The War in Ukraine, Italy, and NATO's Strategic Communications Challenges
 Skimming the Narrative Floor: The Legal and Psychological Grounding for the European Union's Ban on Russian State-Sponsored Media
 Measuring the Effectiveness of Celebrity Activism: Celebrity Advocate v Celebrity Endorser
 Guiding Word-of-Mouth (WOM) Through Organic Social Media for Effective Strategic Communications: A Literature Review

Disinformation and Scholarly Communications
 Persuasion Not Propaganda: Overcoming Controversies of Domestic Influence in NATO Military Strategic Communications
 Democracy, Power, and Our Falling Imaginations
 The Ugly Mirror Avots
 Russia v The World: Was That Inevitable?
 Home before Dark: China's Approach to The Russian War in Ukraine

Volume 12 | Spring 2023

DEFENCE STRATEGIC COMMUNICATIONS

The official Journal of the
 NATO Strategic Communications Centre of Excellence

Special Issue: Strategic Ambiguity

Why Strategic Ambiguity Is So Ambiguous
 The Clarity Trap
 Unmapping the Indo-Pacific: A Strategic Communications Perspective
 Strategic Communications, Ambiguity, and Taiwan
 Sanctions, Communication, and Ambiguity

Geopolitics by Metaphor: The Sweet Spot between Specificity and Ambiguity
 Talking about War Crimes: War Crimes Discourse and Strategy
 Hybrid after All: The 'Grey Zone', the 'Hybrid Warfare' Debate, and the PLA's Science of Military Strategy
 Inherent Strategic Ambiguity between Objectives and Actions: Russia's 'Information War'
 Weathering the Storm: The European Union's Strategic Ambiguity on Twitter during the COVID-19 Pandemic

