'RICOCHETS & REPEATERS'

WHY THE PUBLIC RELEASE OF INTELLIGENCE WORKS AS A MEANS OF STRATEGIC COMMUNICATION IN THE 21ST CENTURY AND WHY IT IS INSIDIOUSLY DANGEROUS

AUTHOR

Maj Luke Turrell

The author gained a Masters degree in Strategic Communication as a Chief of the General Staff scholar and is now the Executive Officer of CHACR

'A real stroke of genius': US leads efforts to publicise Ukraine intelligence – ***Financial Times*** **headline, 6th April 2022**

THE release of intelligence by the USA and UK prior to the invasion of Ukraine was quite rightly deemed to be a masterly use of strategic communication. At a stroke it not only neutralised dangerous Russian false flag disinformation in Europe but also planted the seeds of a coherent and largely unified NATO response; a response Russian strategic and military planners may not have anticipated from a 'brain dead' organisation.

But why does public release of intelligence work as a means of strategic communication in the 21st century? The answer includes understanding the development of globalisation, long standing democratic calls for transparency in government and the implications of mass and social media. It also incorporates something called 'inoculation theory'. This widely accepted theory works like a vaccine; it 'pre-bunks' dis- and misinformation in advance rather than trying to disprove a message after it has landed. In a world of cognitive overload and fake news, our prehistoric brains are seeking something we can trust.

The danger is the use of intelligence for strategic communication creates insatiable demand from politicians and expectation from the public for a product. A product that is by its nature incomplete, out of context and intended to highlight a certain truth rather than tell the whole story. In a Western world characterised by performative social power, repeated use to promote rather than inform policies is fraught with danger. It's not only unsustainable but, as the Iraq War in 2003 proved, risks damaging the very integrity which gives it its strategic communication power. And yet the *2021 Integrated Review* indicated defence intelligence would "become more agile in exploiting its knowledge for impact and effect"[1] so there are real cultural dangers for intelligence and strategic communications professionals.

For readers of this CHACR *In-Depth Briefing*, there are two messages. Strategic communication that uses the public release of intelligence is effective in ways and for reasons you probably hadn't considered. And dangerous in ways you might not have anticipated.

CONTEXT

The context is important. Globalisation has democratised information in the Western world. This coupled with the growth of mass and social media produced an explosion of information, far too much for people to fully comprehend. E O Wilson said we've stumbled into the 21st century with "palaeolithic emotions, medieval institutions and god like technology".[2] This god like technology, especially when employed by social media, is especially challenging to our

[1] *CP 411, Defence in a Competitive Age, (March 2021): 65.*

[2] *Susan Ratcliffe, Oxford Essential quotations, 4th edition, (2016): 538 Susan Ratcliffe, Oxford Essential quotations, 4th edition, (2016): 538.*

Stone Age emotions. When algorithms feed us the same information several times, our primitive brains can't help giving it credence. If in a 1st century village you heard the same information several times from multiple sources, it was probably true. Fundamentally, our brains haven't had time to evolve sufficiently. So, when we are faced with multiple plausible but contradictory truths, we crave something we can trust.

As a result, there have been increased demands for transparent government.[3] From the 1970s democratic countries recognised the importance of 'open government' and introduced reforms. In the UK, the gradual public unveiling of the security and intelligence services in the 1990s is testament. However, this was rarely borne from altruistic openness. More cynical observers point to a perception of openness rather than any greater public oversight. In 2009 the MI5 Director General noted openness and transparency "supported public confidence in us". This focus on promoting public trust and confidence came not only after the 2003 Iraq 'dodgy dossier' but also the Snowden and WikiLeaks revelations. In the wake of these revelations polls indicated people recognised their privacy was in some cases secondary to their security. However, security and intelligence agencies quickly recognised the fundamental risks in losing public trust and sought to minimise the damage with a PR campaign of 'openness'.

"WIKILEAKS USED TRADITIONAL MEDIA TO REPEAT THEIR REVELATIONS AND SOCIAL MEDIA TO RICOCHET THEM BACK INTO THE MAINSTREAM. THEY GAINED RESPECTABILITY AND TRUST BY BEING CARRIED BY MAINSTREAM MEDIA, COUPLED WITH REACH FROM SOCIAL MEDIA."

The Snowden revelations whilst initially seen as a threat, also offered significant opportunity. They drove cultural change within intelligence organisations and paradoxically led to an increase in the release of intelligence.

LESSONS FROM SNOWDEN

Snowden and WikiLeaks taught intelligence agencies the value of 'repeaters and ricochets'. WikiLeaks used traditional media to repeat their revelations and social media to ricochet them back into the mainstream.[4] They gained respectability and trust by being carried by mainstream media, coupled with reach from social media. The strategic communicators within intelligence agencies were watching and taking note. They also noted how WikiLeaks cut through the noise of the cluttered information environment.

Strategic communications professionals had long recognised that communication message control was over and making your voice heard was increasingly difficult.

And yet WikiLeaks engineered strat com gold by delivering trustworthy access to secrets, a topic Sir John Scarlett, former chair of the Joint Intelligence Committee considered to be 'like sex' as both encourage fantasy.[5] And sell papers.

"[News] cycles are very short, and to break through you have to bring something innovative and sparkling[...]"[6]

And so strategic communicators recognised three inherent principles. You need to demonstrate openness within democratic society to enjoy public confidence. Public secrets gain credibility and reach by being released into mainstream and social media to be repeated and ricocheted around. And secrets sell papers. Culturally intelligence agencies also recognised, much like the 1930s aphorism that the 'bomber always gets through', that secrets will eventually get out. This drove a culture of 'use it or lose it' and led to a greater use of intelligence for strategic communication purposes.

UNPRECEDENTED?

The release of intelligence isn't, as many media outlets have suggested, unprecedented. Examples from the Cuban Missile Crisis, the 1917 Zimmerman telegram, and the public disclosure by Prime Minister Stanley Baldwin in 1927 that the Government was intercepting Soviet telegrams[7] suggest it's unfamiliar, rather than unprecedented. Moreover, it's being used at a speed and scale commensurate with 21st century technology. However, as Stephanie Carvin of the Centre for International Governance and Innovation points out "it's vital that intelligence agencies understand the conditions that created success before generalizing this approach to

---

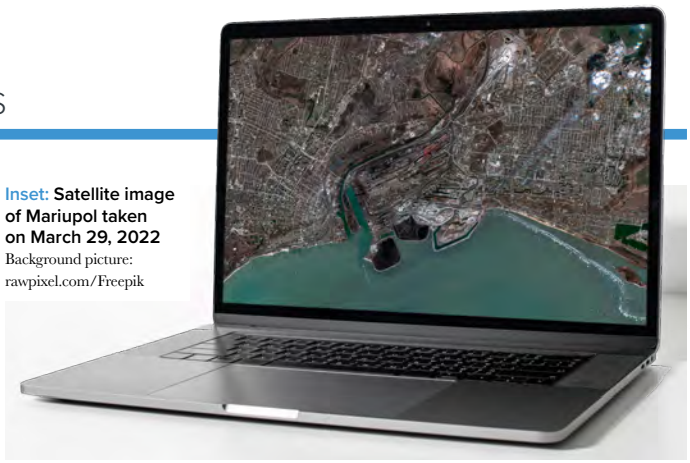
[3] *See Ann Florini, "The End of Secrecy", IN Power and Conflict in the Age of Transparency, edited by Bernard I. Finel, and Kristin M. Lord, Palgrave Macmillan, 2002.*

[4] *Neville Bolt, "The Leak Before The Storm", The RUSI Journal, 155:4, (2010): 46-51*

[5] *David Omand, Securing the state, (2010): 250.*

[6] *Ofek Riemer, "Politics is not everything: New perspectives on the public disclosure of intelligence by states" Contemporary Security Policy, 42:4, (2020): 588.*

[7] *Richard Norton-Taylor, In Defence of the realm? The case for accountable Security Services, (1990): 18.*



Inset: **Satellite image of Mariupol taken on March 29, 2022**
Background picture: rawpixel.com/Freepik

future conflicts and heralding a new era of intelligence primacy". If, as Professor Rory Cormac thinks, UK use of intelligence to support strategic communication is a "huge cultural shift"[8] then analysis is both important and timely.

RUSSIAN DISINFORMATION PRE-BUNKED

Prior to the invasion of Ukraine in February 2022, Russia sought to justify their invasion by manufacturing Ukrainian provocations. Long established in the Russian playbook, it actually echoed Nazi Germany's actions prior to the invasion of Poland.[9] In this case, the US release of intelligence 'pre-bunked' their disinformation.

Traditionally lies were countered by evidence and argument. However, studies reveal it's difficult to correct people once they're exposed to falsehood.[10] Not only does belief linger (the 'continued influence effect'[11]) but people are reticent to admit they've been deceived.[12] And repeated exposure to misinformation can actually increase people's belief even though they know it to be false, an effect known as the "illusory truth effect".[13] As a result, Inoculation Theory pre-emptively introduces psychological resistance.[14] Let's take the opening three paragraphs of a *New York Times* article quoting a senior US Government official on the prospect of a Russian false flag operation.[15]

Washington – The United States has acquired intelligence about a Russian plan to fabricate a pretext for an invasion of Ukraine using a faked video that would build on recent disinformation campaigns, according to senior administration officials and others briefed on the material.

This was the forewarning or threat of a persuasive attitudinal attack that functioned like a medical inoculation. It highlighted a vulnerability in the audience's thinking and triggered a protective response and resistance.

The plan – which the United States hopes to spoil by making public – involves staging and filming a fabricated attack by the Ukrainian military either on Russian territory or against Russian-speaking people in eastern Ukraine.

The threat was made more explicit to increase the effect.[16]

Russia, the officials said, intended to use the video to accuse Ukraine of genocide against Russian-speaking people. It would then use the outrage over the video to justify an attack or have separatist leaders in the Donbas region of eastern Ukraine invite a Russian intervention.

And refutational pre-emption provided ready-made arguments and enabled the audience to practise defending the truth, a process known as counterarguing.[17]

In this way the release of intelligence prior to the invasion of Ukraine marked a watershed. Intelligence agencies and politicians harnessed all the lessons from globalisation, mass and social media and inoculation theory to ensure the effect of Russian false flag disinformation was successfully neutralised.

NATO UNITY – A STRATEGIC COMMUNICATION IMPERATIVE

In addition to learning the contextual lessons, the careful rebuilding of US and UK intelligence agency credibility was important to encourage acceptance of the released intelligence. Russia's track record of lies and disinformation did nothing for the credibility of their messages. However, not everyone was convinced by NATO's message, and many were surprised when the invasion of Ukraine actually happened in February 2022.

"SOPHISTICATED, COMMERCIALLY-AVAILABLE SATELLITE IMAGERY ENABLES TRUE SOURCES TO BE EASILY OBFUSCATED."

What was instrumental was intelligence as a means of internal strategic communication to reinforce NATO alliance unity. NATO has long identified the unity of its member states as its centre of gravity. Therefore, by sharing intelligence the US and UK ensured NATO members were 'on the same page' when the invasion happened. And the response in the form of sanctions and support to the Ukrainian government could begin immediately. It may be that the sacking of the French military intelligence chief had more to do with French political intransigence than his professional failings.

SO, WHAT'S THE PROBLEM?

The danger isn't that the release of intelligence risks compromising human or technical sources; the protocols and processes are too conservative for that. And rapidly increased open-source imagery intelligence and human intelligence and sophisticated, commercially-available satellite imagery enables the true sources to be easily obfuscated.

"The price of admission to the spy satellite business used to be a billion dollars... Now, anybody with a credit card can buy high-resolution satellite photos."[18]

The problem is intelligence, especially intelligence that has

---

[8] *Karla Adam, "How U.K. intelligence came to tweet the lowdown on the war in Ukraine", The Washington Post, 22 April 2022, washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine*

[9] *Martin Gilbert, The second world war: a complete history, (2014): 1.*

[10] *U. K. H. Ecker, S. Lewandowsky, M. Chadwick, "Can corrections spread misinformation to new audiences? Testing for the elusive familiarity backfire effect". Cogn. Res. Princ. Implic, (2020): 5, 41.*

[11] *Ibid.*

[12] *Jon Roozenbeek, Sander Van der Linden, Thomas Nygren, "Pre-bunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures", Harvard Kennedy School Misinformation Review, 3 February 2022.*

[13] *L. Fazio, N. M. Brashier, B. K. Payne, E. J. Marsh, "Knowledge does not protect against illusory truth", J. Exp. Psychol. Gen 144 (2015): 993–1002.*

[14] *Josh Compton, "Inoculation theory." The SAGE handbook of persuasion: Developments in theory and practice 2 (2013): 220-237.*

[15] *Julian E. Barnes, "U.S. exposes what it says is Russian effort to fabricate pretext for invasion", New York Times 3 Feb 2022.*

[16] *Joshua Compton, Bobi Ivanov, and Erin Hester, "Inoculation Theory and Affect." International Journal of Communication 16 (2022): 14.*

[17] *Joshua Compton and Michael Pfau, "Inoculation theory of resistance to influence at maturity: Recent progress in theory development and application and suggestions for future research." Annals of the International Communication Association 29, no. 1 (2005): 97-146.*

[18] *Vernon Loeb, "Spy Satellite Will Take Photos for Public Sale," Washington Post, 25 September 1999.*

been declassified, is incomplete. It's out of context and intended to highlight a certain aspect of a policy, rather than tell the whole story.[19] The truth, wrote George Kennan, "is sometimes a poor competitor in the market place of ideas – complicated, unsatisfying".[20] As a result, a simplified and therefore manipulated 'story' is more effective. The Butler report after the invasion of Iraq made clear if intelligence is to be used more widely by governments those doing it must be careful to explain its uses and limitations with clearer and more effective dividing lines between assessment and advocacy.[21]

The challenge is, as we have seen above, intelligence is effective as a tool of strategic communication. In part because of the respect intelligence agencies have cultured through careful releases of foiled terrorist attempts or state plots and the inherent sexiness of their product. However, this perception is based on a seemingly oracle-like quality to intelligence that no intelligence professional would recognise.

And as a result, the public, politicians, and senior military officers will demand more of it. Lots more. And the demand for repeated and consistent intelligence will be perpetuated because "they expect you to know," since "you created an impression that you know everything".[22]

DANGERS OF INTELLIGENCE AS A TOOL OF STRATEGIC COMMUNICATION

The use of intelligence has therefore created a multitude of issues. The first is best exemplified by the run up to the Iraq war. Policy drove the requirement for intelligence, rather than intelligence driving the policy. Where the intersection of intelligence and strategic communication has worked well historically it was invariably based on synergy between intelligence and the political objectives.

The second is when the release of intelligence becomes routine, mistakes can be made. When US officials leaked intelligence to *The New York Times* that the US had enabled the targeting of 12 Russian generals and the sinking of Russia's Black Sea flagship, the Moskva, it heralded a stinging response from the CIA Director. Not least because if true, it would have indicated actions that made the USA a belligerent in the conflict. "It's dangerous when people talk too much, whether it's leaking in private or talking in public about intelligence issues".[23] *The Financial Times* suggested a bragging culture was creeping in.

Thirdly, intelligence is likely to be misused for strategic communication effect when it could be better used. After the poisoning of Sergei Skripal, the decision to publish information critical to criminal proceedings reflected the political reality that victory in the court of public opinion was worth more than any more formal proceedings.[24]

Fourthly, insatiable demand for intelligence will water down its effect. Tom Fletcher laments in his book *The Naked Diplomat* that the UK government shift to digital communications has resulted in mundane and repetitive content. The danger, as Jonah Peretti founder of *BuzzFeed* points out, is that brands are damaged when they give audiences content they don't value. And Defence Intelligence's Ukraine updates have been widely criticised for repeating bland information already available in quality journalism.

So finally, when the intelligence behind the strategic communication proves to be inaccurate, as it inevitably will at some point, it will damage the very credibility that made it powerful as a means of strategic communication. However, not because the power and credibility stem from the intelligence. From a strategic communication perspective, the power sits with the organisations and institutions that produce the intelligence. And damage to the credibility of the organisations may take generations to repair and reduce overall UK defence capability as a result.

SO WHAT FOR STRATEGIC COMMUNICATIONS?

The use of intelligence to serve strategic communication goals is a new paradigm for intelligence.[25] Using intelligence to counter disinformation and reinforce your narrative enables intelligence to support policy rather than just inform it.[26] Harnessing academic theory and societal and technological developments will make UK strategic communication more compelling, productive, and effective. And yet there are clear risks. Hopefully, greater awareness and management of the risks should prevent them being realised.

This article was selected as a winning entry in the KCL-ARRC initiative 2022 and is reproduced here with the kind permission of the ARRC Journal.

---

[19] *Glenn Hastedt, "Public intelligence: Leaks as policy instruments – the case of the Iraq war", Intelligence and National Security, 20:3 (2005): 419-439.*

[20] *Michael P Colaresi, Democracy Declassified: oversight and the secrecy dilemma in liberal states, (2014): 9.*

[21] *Rt Hon The Lord Butler, "Review of Intelligence on Weapons of Mass Destruction" (2004): para 468.*

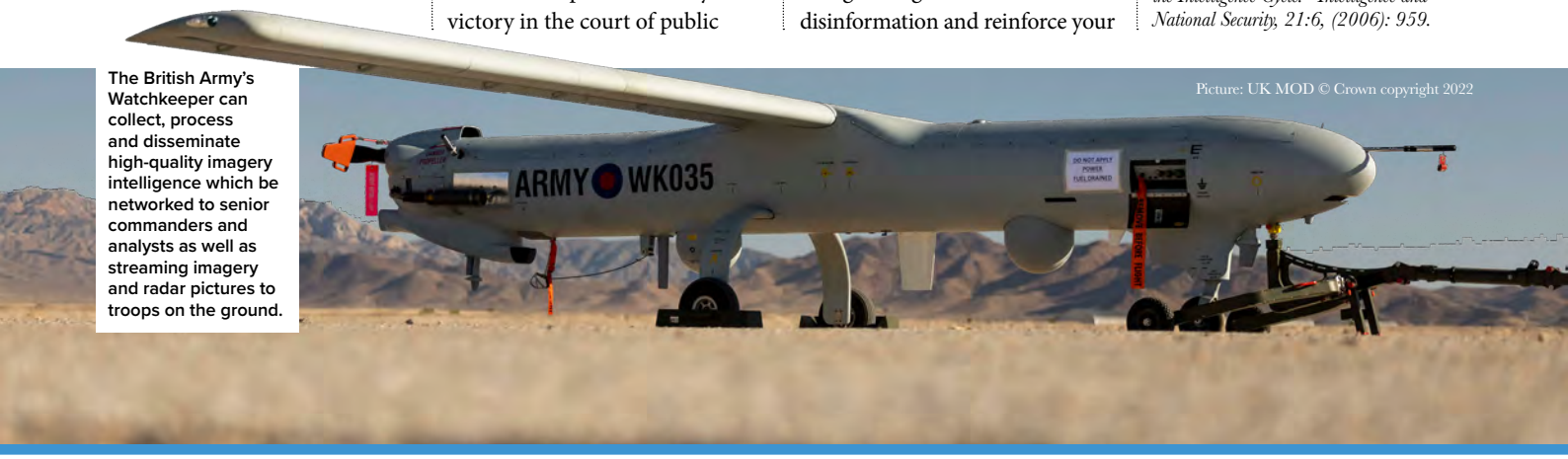
[22] *Ofek Riemer, "Politics is not everything: New perspectives on the public disclosure of intelligence by states" Contemporary Security Policy, 42:4, (2020): 583.*

[23] *Edward Luce, "What the CIA thinks: William Burns on the new world disorder", Financial Times, 13 May 2022, ft.com/content/03860857-e160-4920-9e81-28527dda5560*

[24] *Mark Urban, The Skripal Files; Putin, Poison and the new Spy War, (2019): 306.*

[25] *Felicia Schwartz and Demetri Sevastopulo "A real stroke of genius': US leads efforts to publicise Ukraine intelligence", Financial Times, 6 April 2022. ft.com/content/9b3bc8c0-d511-4eec-9cbd-5a4f432f6909*

[26] *Arthur S, Hulnick, "What's wrong with the Intelligence Cycle." Intelligence and National Security, 21:6, (2006): 959.*



The British Army's Watchkeeper can collect, process and disseminate high-quality imagery intelligence which be networked to senior commanders and analysts as well as streaming imagery and radar pictures to troops on the ground.

Picture: UK MOD © Crown copyright 2022