CRISIS RESPONSE

VOL:17 | ISSUE:3 | SEPTEMBER 2022 WWW.CRISIS-RESPONSE.COM JOURNAL

Protection Prevention Preparedness Response Resilience Recovery

SPACE EXPLORATION

HEALTH | ANTAGONISM | JUNK

Emergency Management | PsyOps | Leadership | Public Safety & Security | Violence & Trafficking | Climate Tech

Editor in Chief
Emily Hough
emily@crisis-response.com

Editorial Assistant
Sue Chamberlain
sue@crisis-response.com

Design & Production
Chris Pettican

News and Blog research
Lina Kolesnikova

Subscriptions
Crisis Response Journal is published quarterly; it is available by subscription in hard copy or digital.
hello@crisis-response.com

Published by Crisis Management Limited, Sondes Place Farm, Westcott Road, Dorking RH4 3EB, UK
© Crisis Management Limited 2022.
Articles published may not be reproduced in any form without prior written permission.
Printed in England by The Manson Group, UK
ISSN 1745-8633

www.crisis-response.com
follow our *CRJ* company page on LinkedIn
follow us on twitter @editorialcrj

contents

News & Comment

News 4

We need a new social contract 8
Public policies should be based on the facts of the human lifecycle, suggests Albert Weale

Emergency management

The moral compass 12
Beverley Griffiths maps out an ethical emergency management framework

Hubris, hierarchy & humanity 14
Emily Hough speaks to Lucy Easthope about emergency and disaster management

Talking preparedness 18
After Covid are people risk fatigued or more risk aware? Amanda Coleman investigates

Legal facets 20
Legal frameworks, tools and expertise in disaster risk management are underestimated and underutilised, says Olga Shashkina

Towards national resilience 22
Raditya Jati describes the journey towards implementing Indonesia's concept of 'risk to resilience'

Climate technology 24
Emily Hough speaks to Wake Smith about possible climate change solutions, however unpalatable they might be

Leadership

Leadership: What it takes 28
Competencies are shifting from what to do to who you are, according to Eric McNulty

Human factors 30
Andy Blackwell explains how empowering and motivating frontline responders benefits organisational performance, innovation and culture

The lost art of oration 32
There's great power in being an outstanding orator, says Brad Borkan; and it's a vital communication skill for leaders

A university experience 34
Anthropologist Melissa Schrift examines one university's leadership response to the Covid-19 pandemic

The importance of creativity 37
A creative element is helping the EPS as it reviews and revises its competence framework, writes Jeannie Barr

Public safety & security

The new battlefield of the brain 38
Information warfare is an integral component of military strategy, explains Ekaterina Kostioukhina

Catapulting cows 42
Chris Needham-Bennett presents an overview of psychological operations and commercial disinformation

From hope to reality 46
Chris Singer examines the CBRN threat landscape and preparedness

The perils of 2G and 3G switch-off 48
European roamers might not be able to call 911 on their cellphones in the USA, warn Freddie McBride and Rudolf van der Berg

Urban security 50
Lina Kolesnikova examines the blame game after Liverpool fans were tear gassed, crushed in bottlenecks at turnstiles and assaulted at a football match in Paris

Crowded venues 52
Christopher Kemp says a crisis can create the opportunity to rethink safety and security

Societal effects of disaster 56
Cristina Pogorevici looks at far reaching ramifications of a nightclub fire in Bucharest on Romania's emergency response and the country's political atmosphere

Escalation of mass shootings 60
Violence in the US and elsewhere is at an all-time high, writes Jennifer Hesterman. What can we learn to prevent or mitigate it?

Conflict zones & crime 62
Conflict offers opportunities for criminal networks, says Lina Kolesnikova, from smuggling to human trafficking

Violence, trafficking & abuse

Domestic violence in Ukraine 64
The war in Ukraine could set us back 20 years, undoing progress made in tackling domestic violence, and exacerbating the issue even further, writes Valeriia Troshchylo

A deep and enduring disinterest 67
Disasters give a rare opportunity to theorise about causes of increased violence against women. Debra Parkinson elaborates

Covid-19 and trafficking 70
Manika Kamthan examines how the pandemic and lockdown in India combined to create an environment ripe for exploitation, including trafficking and abuse

Climate & modern slavery 72
The climate change and slavery connection has yet to make itself overtly obvious in Pakistan. But that doesn't make it any less lethal. Luavut Zahid investigates.

Breaking the silence 76
Emily Hough speaks to Purna Sen about a call to address sexual aggression at – or in the name of – the United Nations

Space matters

Do look up 80
Gianluca Pescaroli provides an introduction to why we should all be aware of future hazards in outer space

The new iron curtain 84
Johan Eriksson and Giampiero Giacomello examine natural risks and antagonistic threats in space

Health risks 86
What do crisis planners and responders need to know about health risks in outer space, and why? Ilan Kelman and Myles Harris elucidate

Space capabilities 88
No feature on space would be complete without the issue of space debris – and the consequences of not managing it responsibly. Henry Heren starts the discussions

Space is hard 90
Growing environmental and geopolitical complexities are arising from ever greater expansion into space, explains Ewan Haggarty

A tragedy of the commons 92
Dead satellites in earth orbit accumulate as junk, increasing the risk of catastrophic collisions with active spacecraft or other debris. Kristen Lagadec looks at what we need to do

The risk to first responders 94
The pace at which technology has advanced and the appetite for consumption mismatch industry progress to ensure the services are robust, writes Chloe Van Dop

Regulars

Events & diary dates 96

Frontline 98

Climate change p24

Malte Mueller | Adobe Stock

Battle for our minds p38

Ajay | Adobe Stock

Cover story: Outer Space
Cover image: Gracie H Broom

Breaking the silence p76

Nubefy | Adobe Stock

Space feature p80

Dotteyeti | Adobe Stock

comment

On p76 of this edition I talk to Purna Sen, who appeared in a BBC documentary featuring whistle-blowers. She discusses the sexual harassment of people working at the United Nations, and examples of sexual exploitation and other abuse of those who its agencies are tasked to help. At the core of such abuses lie strict hierarchies and power that cannot be challenged, as well as the malignant construct that the mistreated person is often somehow at fault.

On page 14, I speak to Lucy Easthope; one of the areas she talks about is the very real risk of responders causing further distress to those affected by a disaster, often through poorly thought out policies that fail to centre humans at the heart of planning. Easthope also highlights hierarchies and the difficulty of challenging power.

One example of unintended consequences in technology arises on p48, where our authors warn that the 2G/3G switch off could leave Europeans travelling to the USA unable to call 911 emergency services through their cell roaming provider.

On p24 I speak to Wake Smith about the range of possible, and rather concerning, technologies that could help mitigate the effects of climate warming on our planet. Smith is calling urgently for more research to avoid any unintended consequences of deploying potentially life-changing technology on a global scale – the 'least bad' options – without understanding what could go wrong.

Elsewhere (p80), authors outline our vulnerabilities to what is happening in outer space, warning of the consequences that space debris and shifting political alliances could have down here on Earth. Here, at least, governance consensus might be forming.

It is impossible to sum up the burning indignation that the CRJ team felt when reading some articles for the first time. Among those outlining violence against women in conflict or after disasters, abuse of power and exploitation, or the self interest and slow action surrounding global climate governance, there are many articles that offer hope. But they are in danger of being overwhelmed by those that highlight human malice, ineptitude or plain indifference.

Catapulting cows and trojan herrings

What was the preserve of the military and intelligence services has seeped into the commercial world. Here, **Chris Needham-Bennett** presents a broad overview of psychological operations (PsyOps) and commercial disinformation

While the first psychological operations campaign may be lost in time, one PsyOp involving a cow being fired at the enemy provides a good reference point. In the 12th Century, the defenders of Hochosterwitz Castle in Austria risked being starved out by attacking forces. They slaughtered a healthy cow, stuffed it with grain and fired it out of the castle. The attackers concluded that their enemies under siege could never be starved out if they had so much food that they could afford to waste it in this fashion and moved to a secondary target.

PsyOps have always accompanied warfare and, in an increasingly digital world, their potential reach is growing; what was the preserve of the military intelligence is seeping into the commercial world in the form of disinformation. Many nations are reforming their PsyOps units in the light of antagonistic state campaigns, but few of their populations have a good understanding of its definition and aims. Curiously, only two decades ago, even some military commanders frowned on PsyOps as being somehow unsporting.

Over the last 20 years, there has been a growing recognition of the power and reach of PsyOps, so much so that even neutral Sweden has formed an agency for psychological defence. Writing in the *Financial Times*, Braw astutely highlights the key issue that public trust in government is the Achilles' heel of democracies, which can be targeted by antagonistic PsyOps. Braw also notes that it is not only state actors who are using PsyOps, saying: "Private sector organisations are using a commercial offering known as 'disinformation as a service' to conduct malign influence operations against their competitors."

PsyOps are being rehabilitated very rapidly, their moral position is being considered and their wider commercial deployment increasingly recognised.

We all practise some form of PsyOps when we attempt to influence others and hyperbolic but regulated advertising campaigns – a mild form of PsyOps – are familiar to us all. Almost axiomatically, it is difficult to assess the exact impact of PsyOps, but there are two reasons to assume they have some efficacy. With their aim to influence perceptions, attitudes and behaviour, they can be compared with advertising. It has been reported that one brand of beer spends almost £8m a year on advertising in the UK alone. The thus extrapolated global advertising expenditure itself does not mean it works, but the likelihood of commercial organisations wasting money on such a scale is unlikely and, unsurprisingly, advertising commentators are quite adamant that adverts work.

Perhaps paradoxically, the single biggest endorsement of the efficacy of PsyOps lies in attempts to block, ban or suspend enemy PsyOps outreach to one's own populace. This is understandable, given the alleged work rate of foreign actors. Christopher Till, writing in *New Media and Society Journal*, cited Singer and Brooking, who recounted the required work rate of Russian Internet Research Agency PsyOps agency employees, who were: "Expected as a daily minimum to post comments on news articles 50 times, manage six Facebook accounts with at least three posts, hold two discussions in news groups and manage ten Twitter accounts with 50 tweets per day."

Propaganda did not always have the negative connotations it has today. Its origin was simply that of propagating one's view, but western/NATO PsyOps were placed in a taxonomy of 'white, grey and black' by the NATO Allied Joint Doctrine for Psychological Operations of 2014.

Adverse effect on credibility

White PsyOps involve products disseminated and acknowledged by the sponsor or accredited agency. Grey PsyOps involve products that do not specifically reveal their source, while black PsyOps involve products that appear to emanate from a source other than the true one. UK PsyOps are predominantly, but not exclusively, white. History indicates that black campaigns are generally less successful than white and they may have an adverse effect on credibility of other sources.

It is fascinating that 'attribution' as opposed to effectiveness, or some other measure, is perhaps key to the analysis or discernment of PsyOps.

The BBC World Service is a form of white PsyOps and while the BBC is not a state broadcaster, one might detect a slightly pro-British slant. Even the former Russian President Mikhail Gorbachev praised the BBC News Russia for its thorough and detailed reporting to which he had access during his arrest in an abortive military coup in 1991, saying it had been his main source of information during his incarceration.

However, attribution alone is a crude measure of how much PsyOps content is contained in any broadcast, and it neatly sidesteps the issue of intent and morality. Let's consider the work of Leni Riefenstahl, a brilliant propagandist whose seminal film, *Triumph of the Will* (commissioned by Hitler in 1934), is still viewed as perhaps the best example of a white PsyOps film. The imagery, the cinematography, the innovative long-shots and novel aerial photography were far ahead of their time. The target audience was the German 'Volk' and it was thought that the film influenced many into admiration for the achievements of the Nazi party. However, the intent of the film to promote a vision of Hitler as the saviour of Germany is, at least in retrospect, morally dubious. This begs the question as to the moral dimension of white PsyOps and the possible misnomer or misinterpretation that white PsyOps are somehow morally distinguishable from grey and black. Film-maker Frank Capra condemned the movie's ultimate effects, saying it: "Fired no gun, dropped no bombs. But as a psychological weapon aimed at destroying the will to resist, it was just as lethal."

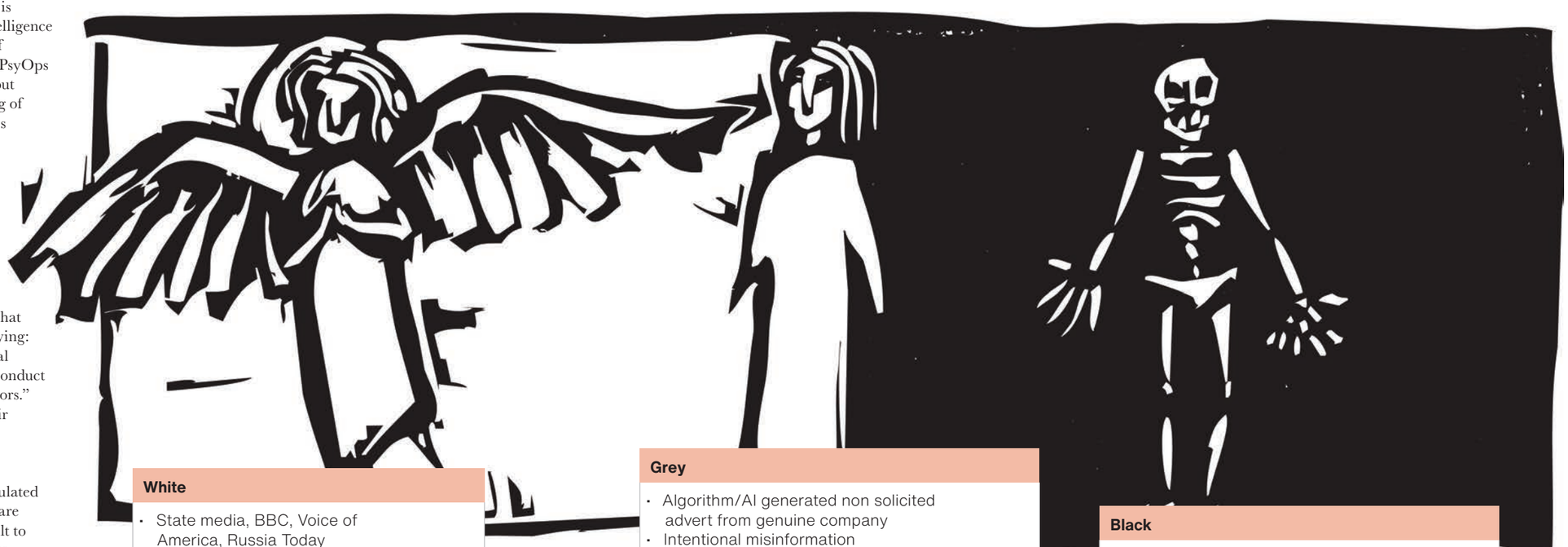


Figure1: *PsyOps have been described as 'white, grey and black', but we must be careful not to disappear into a warren of different types of information*

Xochicalco | 123rf

White

- State media, BBC, Voice of America, Russia Today
- Normal regulated advertising
- Accidental misinformation
- Normal attributable reviews, eg *Michelin Guide*

Grey

- Algorithm/AI generated non solicited advert from genuine company
- Intentional misinformation
- False anonymous reviews or paid reviews with bias
- Purposeful malinformation
- Any non attributable advocacy

Black

- Fake news
- Disinformation – commercial/state
- Some forms of cyberattack
- False flag operation

Thus, simply because the PsyOp is attributable it does not bestow moral rectitude on the operation; the connotation of its being white is perhaps misleading as it implicitly conveys a sense of innocence. Indeed, even the NATO 2014 taxonomy, with UK authored comments, is a piece of PsyOps in its own right as it implies a UK preference for the white end of the spectrum, thereby reinforcing the idea that its messages are to be trusted as they are seldom grey and almost never black.

Grey PsyOps are non-attributable to a source, best illustrated by the well known QAnon movement. That it has been used for PsyOps purposes by non-US actors seems broadly accepted, as noted by James Suber: "…if QAnon does disappear, it will still have highlighted a path for both nefarious extremists and state-actor rivals to polarise and divide American society, often with violent consequences."

What is remarkable, or suspicious, is how few contributors dominate the content of QAnon campaigns, with one UCL researcher noting that: "Just a handful of content creators," were responsible for more than 72.8 per cent of the total submissions in the community.

The grey PsyOps of QAnon are essentially based on the adage of 'seeing is believing'. Just like big data, QAnon is organised according to the principle that enough information will reveal patterns and the connections between everything.

This anonymous virtual world described by Hannah in a paper published in *Social Media and Society*, is a PsyOps bonanza. If one turns to cognitive biases and some heuristics, (mental short cuts), the QAnon platform 'scores' spectacularly well and is, to the PsyOps operative, very fertile ground. One can identify the following possible confirmation biases in the nature of QAnon and its target audiences:

- **Anchoring bias:** The person seizes on one piece of information to make the decision;
- **Effort justification:** The person values the information more if they have struggled to research it;
- **Apophenia:** (Illusory correlation) the inclination to make linkages between unrelated data;
- **Confirmation bias:** One actively seeks information that confirms a belief;
- **Egocentricity:** One overvalues one's own perspective;
- **Agent detection:** One presumes an intelligent agent at work;
- **Plan continuation bias:** An ability to adapt a plan when the situation changes; and
- **The Dunning Kruger effect:** People overestimate their own ability, especially if unskilled in that area.

Arguably the key bias is apophenia; this was commented upon by van Prooijen and Douglas in *Applied Cognitive Psychology*, when they noted that people who detect order in randomness are more prone to be credulous of conspiracy theories that potentially offer the person: "A clear but wrong casual explanation." In another paper, van Prooijen also suggested that higher levels of education were inversely correlated with adherence to conspiracy theory or theories, the assumption being that the faculty of critical thinking, enhanced by education, could offer a level of discernment that others lacked. This highlights the possible need for the education of the potential recipients of PsyOps to be 'vaccinated' against their effects.

Turning to black PsyOps, the deepfake surrender broadcast purporting to feature President Zelenskyy of Ukraine on March 17, 2022, was ostensibly an excellent example of black Russian PsyOps. A Ukrainian news channel, TV 24, appeared to have been hacked and the message was broadcast live on its site; it was widely downloaded and promulgated. The veracity of the broadcast was very quickly discredited and there were several very apparent flaws that any viewer can spot immediately.

QAnon is organised according to the principle that enough information will reveal patterns and the connections between everything

However, if one takes a cynical view of black PsyOps, one could entertain the thought that it was actually a Ukrainian operation, because its result on the Ukrainian population could be summarised as follows:

- The enemy's PsyOps are clumsy and blunt;
- Zelenskyy would never say this now or in the future. Any subsequent attempt to repeat the attack would be futile; and
- The Ukrainians are now sensitised to such attempts and will scrutinise any similar broadcasts with mistrust.

This latter explanation might indeed be the case as the Ukrainian Centre for Strategic Communications and Information Security apparently, very prudently, had previously issued a dire warning as to the possibility of deepfakes being distributed. Sky News reported that it said: "Imagine seeing Vladimir Zelenskyy on TV making a surrender statement. You see it, you hear it – so it's true. But this is not the truth. This is deepfake technology… this will not be a real video, but created through machine learning algorithms." Then, lo and behold, such a video appeared some weeks later, almost exactly as it had previously been described. Just whose black PsyOps this was remains a question but, as a PsyOps vaccine to the Ukrainian people, it would be difficult to improve upon.

The author's considered suggestion is that it was what could be termed a 'Trojan herring'. It looks for all the world like the original Trojan horse style of attack by the enemy, but is actually a red herring laid out for all to see by the defenders themselves. It was perhaps an attempt to vaccinate the Ukrainian public and to enhance its discernment.

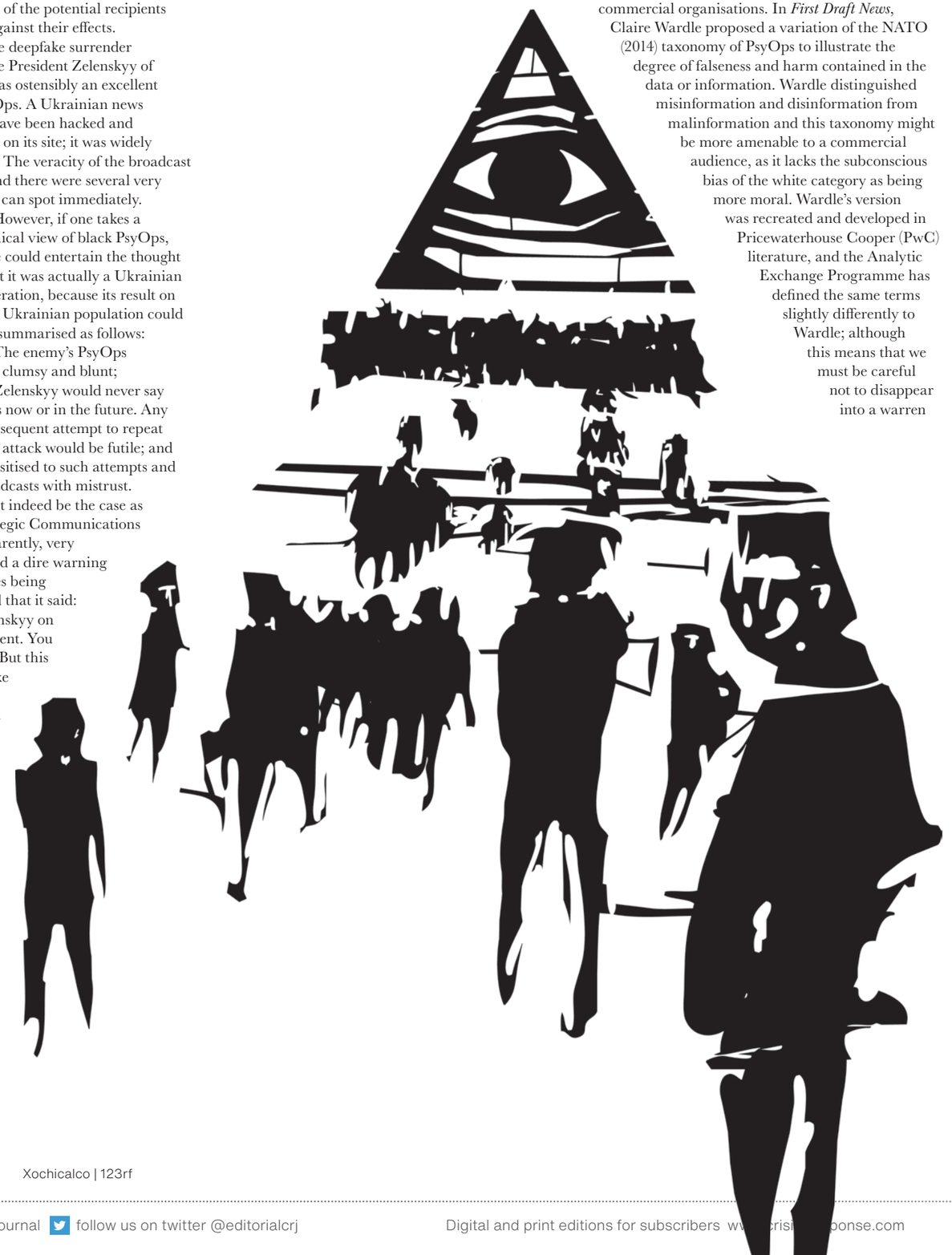
Commercial PsyOps now focus not just on target populations, but specific commercial organisations. In *First Draft News*, Claire Wardle proposed a variation of the NATO (2014) taxonomy of PsyOps to illustrate the degree of falseness and harm contained in the data or information. Wardle distinguished misinformation and disinformation from malinformation and this taxonomy might be more amenable to a commercial audience, as it lacks the subconscious bias of the white category as being more moral. Wardle's version was recreated and developed in Pricewaterhouse Cooper (PwC) literature, and the Analytic Exchange Programme has defined the same terms slightly differently to Wardle; although this means that we must be careful not to disappear into a warren of different types of information:

- **Misinformation:** Could be shared false information but the person sharing believes it to be true;
- **Disinformation:** Information purposefully constructed to do harm; and
- **Malinformation:** Genuine information that could cause reputational damage and is used for this purpose.

So, theoretically, if one shared disinformation believing it to be true, it becomes misinformation. But malinformation, if shared, cannot become disinformation because it was true information in the first place. Frankly the NATO categories seem clearer.

Nevertheless, PwC highlights the development of disinformation as a service and provides an example of costs as follows: "$15-$45 to create a 1,000-character article; $65 to contact a media source directly to spread material; $100 for ten comments to post on a given article or news story; and $350-$550 per month for social media marketing."

PwC quotes other examples, including a major soft drinks manufacturer's plant being closed following a fake news item on parasites in the plant and footage of a popular self-drive electric car crashing into a robot that was revealed to be a Russian fake.



Xochicalco | 123rf

Intuitive appeal

Commercial disinformation might be no great surprise, but what is astonishing is that disinformation seems to have an intuitive appeal. A study published in *Science* in 2018 demonstrated that the more novel content of fake news or disinformation made people more inclined to share it than a mundane – but true – news story.

To summarise, white, grey and black PsyOps, despite being defined by attribution, remain the clearest taxonomy into which dis-, mis- and malinformation can be accommodated, as outlined in Figure 1 (p42).

While the notion of educating populations to be discerning sounds laudable, one presumes that the government conducting such education is not without self-interest and the education risks being a PsyOp in its own right. The idea that persuasive cognitive biases, such as those as used in the QAnon model, can be vaccinated against is at least open to question and is unlikely to be resolved soon.

The innocent hyperbole of advertising is a far cry from the manipulation of a populace by a rival state or paid criminal. The background problem now seems to be a possibly justified lack of public confidence in public agencies and politicians who hitherto would have been convincing in discrediting such attacks. This brings us back to the key issue of public trust in government, which can so easily be eroded by such attacks.

Previously the preserve of the military and intelligence services disinformation has seeped into the commercial world. It is increasingly available and apparently more appealing than real news stories. It remains to be seen how corporate organisations respond to this critical question of public trust when they are attacked. CRJ

Author

DR CHRIS NEEDHAM-BENNETT *is the Managing Director of Needhams1834 Ltd and a Visiting Professor at University College London, UK*

- *A full list of citations and references is available on request, email hello@crisis-response.com*

CRISIS RESPONSE

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY

SUBSCRIBE NOW

visit **www.crisis-response.com** for rates and special offers

Authoritative global coverage of all aspects of security, risk, crisis management, humanitarian response, business continuity planning, resilience, management, leadership, technology and emerging trends

PRINT | DIGITAL

CRISIS RESPONSE

JOURNAL | WEBSITE | EVENTS | SOCIAL MEDIA | NETWORKING | BUSINESS DEVELOPMENT

MULTIPLY

the force of your business

Open doors to the people you really want to meet. **Influence your market** and **build your brand awareness**, across the global crisis and emergency response fields.

Key Network Partnership:

We call them Key Network Partnerships. Because you're not just becoming a partner of ours - but leveraging access to our entire global network. It's about connecting you with the right decision-makers. We open doors and introduce you to the right people, with the power to transform the next phase of your business development. And it's about intelligently marketing your business, to your target audience, across our global platforms. Extending your reach, increasing your exposure and driving your brand awareness.

Call CRJ today about becoming a Key Network Partner on **+44 (0)203 488 2654**

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY

www.crisis-response.com