Volume 6 | Spring 2019

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the
NATO Strategic Communications Centre of Excellence

ISSN: 2500-9486
DOI: 10.30966/2018.RIGA.6

ON FINDING THE ETHICAL IN THE AGE OF DIGITAL BATTLE SPACES

A Review Essay by M.R. Dahlan

Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life
Jennifer Kavanagh and Michael D. Rich. RAND Corporation, 2018

Exploding Data: Reclaiming Our Cyber Security in the Digital Age
Michael Chertoff. Atlantic Monthly Press, 2018

LikeWar: The Weaponization of Social Media
P.W. Singer and Emerson T. Brooking. Houghton Mifflin Harcourt, 2018

Keywords—*Ethics, ethical, positive space, negative space, The Hijaz, digital, social media, digital battle spaces, weaponization data, AI, sharp power, truth, facts, disinformation, fake news, warfare, narrative, discourse, strategic communications, Truth Decay, RAND, Rich Kavanagh, Exploding Data, Chertoff, LikeWar, Singer, information*

About the Author

Prof. Dr. Malik R. Dahlan is Senior Mediation Fellow at the Harvard University Davis Center Negotiation Task Force. He is Professor of International Law and Public Policy at Queen Mary University of London.

The familiar distinction between hard and soft power, which seemed a useful way to simplify the multidimensional dynamics of interstate influence in the century gone by, seems hopelessly insufficient to describe what is happening in the one we are in now. The reason is, of course, the comprehensive breakdown of the post-war order and the apparent return to Bismarckian competition between nation states. Future historians looking for the cause of this return to Realism will not be short of suspects, but perhaps in retrospect it was unfortunate that globalisation was carried forward under the banner of neoliberalism, given the role of deregulated financial markets in the crash of 2008.

Alongside this return to more anarchic relationships among nation states, we also have an increasing breakdown in the economic, cultural, and political order within them. The old alternation between centre left and centre right parties within political systems, bounded and ballasted by mixed economies and relatively generous welfare states, is eroding and European elections are able to produce results that would have been unthinkable a generation ago. That political motility reflects a dissolving of the old sources of authority within the media: the digitisation and socialisation of mass communication has created many competing sources of fact and opinion, with the result that societies are losing their common ground, both in terms of the mutually agreed facts, and in the way those facts can reasonably be interpreted. We are living in a period where technological progress is creating an 'age of anger'. In the words of one recent book that attempted to summarize the zeitgeist, our current era is characterised by 'a loss of cohesion and confidence and a greater willingness to accept the remedies put forward by populist politicians'.[1]

So, if the idea of soft power no longer seems to explain how one state affects another using its forces of attraction and engagement, what will replace it? One suggestion is 'sharp power'—a term coined in November 2017 by the National Endowment for Democracy and published in an article in *Foreign Affairs* magazine. Sharp power refers to the ability of state and non-state actors to combine the time-honoured methods of the public relations industry with micro-marketing made possible by data mining techniques, using social media as the individualised delivery platform. The story that tends to be told after the 2016 US elections is of the vulnerability of democratic states to the aggressive and subversive policies employed by authoritarian governments as a projection

1 Pankaj Mishra, *Age of Anger: A History of the Present* (Macmillan, 2017).

of state power. The attraction of sharp power is clear, and the list of states that have been accused of employing it on the global scale includes China and Russia, of course, but there is no shortage of actors in the regional arenas. In the Middle East, for example, Turkey, Saudi Arabia, Iran, Qatar, and the UAE have all been accused of sharp practices.

As an illuminating aside, this issue of interstate influence has been one of the hallmarks of Islam's relationship with the Judeo-Christian West. I recently concluded a study of the relationship, in which one of the most profound conclusions was that particular spaces—in this case sacred spaces—have become a source of contention and wilful misinterpretation and are transformed from positive into negative spaces. Historically, Jerusalem, Mecca, and Medina were the home of God—shared sacred spaces where peace was institutionalised. The Hajj pilgrimages were a kind of Islamic internet, where the tide of humanity washing in and out of holy places created a vast market for the exchange and elaboration of ideas.[2] Now we have the *neo-medievalists* of Daesh and the post-modernists of al-Qaida who, like the Wahhabists before them, are intent on filling an ethical positive space with negative darkness.

Before the advent of the sharp power narrative, another concept that shed even more light on erosion of the public realm was put forward in a report by the RAND Corporation—the idea of 'truth decay'. This notion is intended to convey 'the diminishing role of facts and analysis in American public life'. The extent to which this decay makes Western liberal democracies vulnerable to being sold a bill of goods has already been apparent in the UK's decision to leave the EU after a campaign that illustrated, to most people's complete satisfaction, the effectiveness of sharp power and truth decay; we also have the various intrusions into the 2016 US elections. RAND's study, the first book I discuss in this essay, is a work of self-examination intended to set out what a think tank can do to maintain quality research and analysis. I will also consider two other recent books, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*, written by Michael Chertoff, a former US Secretary of Homeland Security, and *LikeWar: The Weaponization of Social Media* written by P.W. Singer and Emerson T. Brooking. Each of these books represents a significant attempt to survey the field of strategic communications in the disinformation age. Lawyers such as myself can find themselves left out of the conversation. Partly, I think, because

2 Malik R. Dahlan, *The Hijaz: The First Islamic State* (Oxford University Press, 2018).

DOI 10.30966/2018.RIGA.6.8.

laws and constitutional norms no longer seem to safeguard the validity of political processes such as elections and referendums in the way that they once did. National security now seems more vulnerable than it ever did in the era of mutually assured destruction, and the ethical horizon that lends perspective to that security has never seemed more occluded.

Before I begin my commentary on the three books, I would like to note that artificial intelligence (AI) was a fourth contending theme for discussion because of the importance of AI and machine learning to the way states can interact with their citizens. However, such books have been reviewed extensively elsewhere and it is somewhat to the side of the questions of security and the strategic communications world.[3]

Truth Decay

Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life, by Jennifer Kavanagh and Michael D. Rich, is a 300-page RAND Corporation report that alerts us to the way our ability to rely on facts is diminishing as our reliance on that ability is growing. The book refers to this phenomenon as the 'truth decay paradox'.

As defined, truth decay turns out to be the interrelation of four trends: an increasing disagreement about facts and their analytical interpretations; a blurring of the line between opinion and fact; an increase in the relative volume and resulting influence of opinion and personal experience over fact; and lowered trust in formerly respected sources of facts. This theory offers a more sophisticated taxonomy than the fake news narrative. And, as the book notes, many American sectors—military, technology industry, and organised sports, among others—increasingly rely on facts and data as essential to survival or necessary for success. One point we can surely all still agree on is that it is bad practice to make decisions without first searching for and establishing the facts necessary to calculate the consequences of those decisions, whether one is in the army, in business, or voting in an election.

It comes as no surprise that political discourse has been hospitable to this multiform blurring of facts. If one is in the persuasion business, success comes to those who deal in partial truths or outright falsehoods that appeal to

3 An example is this recent book by the head of Google China: Kai-Fu Lee, *AI Super-Powers: China, Silicon Valley and the New World Order* (Houghton Mifflin Harcourt, 2018).

the prejudices and biases of your target audience. The RAND report is truly worrying in that it casts doubt on the availability of an objective discourse, which might serve as a corrective to these half-truths and outright fabrications. In the past a reservoir of commonly accepted facts and well-supported analyses was provided by government, academia, and accredited experts, which meant that there was general acceptance of, say, the benefits of vaccinating children. Now such authorised knowers are increasingly treated with scepticism. These developments drive a wedge between policymakers and the public, as well as between the groups that make up the public.

This report also describes RAND's findings about the causes of truth decay, which turn out to be due partly to the fallibility of human information processing and partly to the inability of that processing to cope with the sheer volume of information available to us, much of which is opinion posing as fact. Then there is the inability of cash-strapped schools to arm their pupils with the tools needed for critical thinking and the wider polarisation in politics, society, and the economy—a staple concern of op-ed pages around the world.

It comes as no surprise that cultures subject to this deterioration are more vulnerable to groups that wish to amplify the effects of truth decay drivers for their own political or economic ends. RAND's list of possible bad actors includes foreign states and domestic groups lobbying for particular policies. The most spectacular example, of course, was the controversy over who exactly was bankrolling and finagling the pro-leave campaign in the 2016 Brexit referendum. Now we have to deal with the possibility that democratic processes can be decisively influenced by shadowy groups pursuing hidden agendas and financed by dark money.

To what extent is all of this new, and to what extent have campaigns of influence been part of the political environment in earlier eras? Kavanagh and Rich comment that whenever new forms and styles of communication arise, especially when coupled with social, political, and economic unrest, one tends to see a blurring of the distinction between facts and opinions, as well as the increased relative volume of opinion over fact. RAND researchers also found some evidence of declining trust in institutions as sources of factual information in two of these historical periods. That said, the contemporary era stands alone in possessing the full spectrum of causes: the result of the concatenation of new technologies, social media, 24-hour news coverage, and the removal of the possibility of debate and compromise as a result of political polarisation.

Kavanagh and Rich maintain that the consequences of truth decay are direct and severe, both to American democracy and to the concept of liberal democracy in general. More specifically, they damage America's civic and political institutions and its societal and democratic foundations through the erosion of civil discourse, political paralysis at the federal and state levels, the disengagement of citizens from political and civic life, and uncertainty in the formation and implementation of national policy.

An absence of a common store of fact and opinion causes a vicious circle of mistrust among citizens. It can lead them to narrow their sources of information, to cluster with people who agree with them, to avoid meaningful discussions about core issues, and to feel alienated from local and national policy debates. Politics drifts into dysfunction when debate lacks a shared factual basis. In governance, that can lead to delayed decisions, deferred economic investment, and reduced diplomatic credibility.

Part of the issue is that liberal democracies rely on systems of checks and balances that are often prone to gridlock if politicians lose interest in cooperating with each other, at least enough to ensure that the system functions. Meaningful and lasting reform is usually the result of some level of bipartisan collaboration between the two major parties. That applies to reforming a major entitlement programme, modernising US military forces, or completing a major trade deal. This is only possible when both parties agree on the facts. When they don't, the result can be policy oscillation—a sequence of repeal-and-replace zigzags.

As US policy-makers argue over basic facts, legislative processes have become increasingly dysfunctional, and this has prevented decisions on consequential issues such as immigration and health care, leaving millions in limbo. One example of this political dysfunction and stalemate—the October 2013 US Federal government shutdown—produced serious consequences for military veterans awaiting medical care and job retraining, limited the creation of private-sector jobs, and undermined action to ensure food and transportation safety.[4]

This policy whiplash creates uncertainty about the long-term direction and consistency of American policy and has serious consequences for individuals and corporations. Uncertainty about the future of the Affordable Care Act, for instance, has contributed to rapidly rising insurance premiums. Facts matter.

4 US White House Office of Management and Budget report 'Impacts and Costs of the October 2013 Federal Government Shutdown', 7 November 2013.

RAND's researchers reviewed more than 250 articles and books in an attempt to show how sources of fact-based analysis, such as the RAND corporation itself, can make a contribution to the struggle against truth decay. Four streams of inquiry were identified:

First, how has truth decay manifested itself in the past, and how was it overcome?

Second, what are the vectors that spread truth decay? This line of inquiry includes questions regarding how media content has changed over time, how the speed and nature of information flows have evolved, what the latest developments in the education system and curriculums are, how polarisation and political gridlock have (or have not) worsened, whether or not civil discourse and engagement are eroding, and how the level of uncertainty about US policy has changed.

Third, we must investigate how information is disseminated, processed, and consumed, as well as the roles played by interested institutions, authorities, and intermediaries, and the benefits and challenges of technological advancement. The scale of the challenge is apparent.

The final item on the agenda is, of course, the need to develop and evaluate solutions. Priority areas include educational interventions, improving the information market, developing and rebuilding institutions, bridging social divides, and harnessing new technologies, behavioural economics, psychology, cognitive science, and organizational self-assessment. The scale of the solutions is equally impressive and will require quite an effort from those responsible at a time when such efforts are becoming increasingly difficult to mobilise.

Moving forward, the RAND Corporation itself plans to continue investigating three areas: the changing mix of opinion and objective reporting in journalism, the decline in public trust in major institutions, and initiatives to improve media literacy in light of 'fake news'. Media literacy will be its first area of focus—that is, the ability to apply critical thinking to evaluate the reliability of what we are being told or sold.

One potential quick win for which there is already a vocal constituency is action to increase transparency in social media. Platforms could provide clarity on where their advertising money comes from. They could open their application programming interfaces and work to identify and monitor the existence of bots on their systems. Kavanagh and Rich also argue that social media users need to

be part of the answer. 'We can implement all the regulations that we want, but if people aren't willing to look for facts and take the time to identify what is a fact, then I don't think it makes a difference', the authors note. 'There has to be an understanding of why facts matter—and why it's important to be an informed participant in democracy—if democracy is what you want.'[5]

Exploding Data

Exploding Data explores the profound changes wrought by the digitisation of more and more elements of modern life. Chertoff's central argument is that current legal and policy notions about privacy, freedom, and security must be reformulated in light of this technological revolution.

The book begins with an explanation of how the data revolution that grew out of the internet came to involve much more than just digital infrastructure. The growth of the internet spurred the explosive growth of data storage capacity, and of the computer processing power necessary to understand and make use of this vast store of data. The development of wireless technology radically increased the number of endpoints that could connect to a network, culminating in an internet of things that allows almost any device to be configured to connect to a network and supply it with data. An outgrowth of this has been the increasing number of physical control systems that are managed and regulated through internet connections. This inevitably raises the risk of network-based attacks against critical infrastructure such as energy, transportation, and health care. The disruption to the electric grid in Ukraine and the damage done by ransomware are examples used to illustrate these impacts.

Among the consequences of this revolution is the need to consider whether rules striking a balance between government surveillance and individual rights need to be recalibrated. Similarly, there is the question of whether the US should follow Europe in conferring on individuals the right to control their data by requiring clear notice and affirmative consent before it can be harvested. Also critical is the need to resolve how national laws interact with a technology in which data is global.

The book argues that the ability of adversaries to use data maliciously to conduct

5 Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life* (RAND Corporation, 2018) and a short article by Laura Hazard Owen, 'The era of "truth decay": 12 things we still don't know about our weird time', *Nieman Lab*, 26 January 2018.

'information operations', as Chertoff calls it, and even to carry out cyber-attacks with destructive consequences, means that cyber conflict is on the horizon. The novel policy problems now facing us include exactly what status to accord a cyber-attack carried out by a hostile state: where does such an attack stand as a *casus belli*, for example?

Chertoff's view is that NATO should adopt a multilateral approach to setting policy focus. NATO must develop an understanding of the doctrines, tactics, and techniques used by adversaries in their attempts to undermine the West's social cohesion and the trust citizens of Western countries place in their governing institutions. This includes the realisation that 'information operations' are designed to promote disunity within the Western alliance, to encourage mistrust of government, and to generate confusion that interferes with responding to aggression.

Naturally, an open society is at something of a disadvantage when it comes to tackling these threats, since responding with Chinese-style internet censorship would be like throwing the baby out with the bathwater. As discussed in the book, ethical issues raised by influence operations stem from the complex interplay between the need to defend against malicious propaganda and to uphold the principle of free speech. However, some level of action is certainly justified: for example, he says:

> It should be permissible to expose and/or block orchestrated campaigns to manipulate search engines through botnets or troll farms. Similarly, media platforms should bar agents who impersonate others or conceal their identities as foreign agents. On the other hand, I think we must resist the temptation to censor content with which we disagree, even if we believe it to be incorrect. To do the latter would run the risk of undermining the free speech which is fundamental to western democracies.[6]

LikeWar

P.W. Singer and Emerson T. Brooking, two national security experts, have titled their analysis in homage to nineteenth-century Prussian military theorist Carl von Clausewitz, author of the ten-volume series *On War*. The aim is to bring

6 From a private interview with Michael Chertoff, author of *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (Atlantic Monthly Press, 2018) on 20 October 2018.

a similar level of analysis to the new battle space presented by social media. If cyberwar is about hacking networks, *LikeWar* is about hacking the people who make up the nodes of the networks. This is a space where military units influence elections using the techniques of information warfare and where teenage digital marketers change the course of military battles wielding selfie-taking smartphones.

Singer and Brooking were moved to begin their study after seeing how the Arab Spring revealed the power of social media to drive major political change. In societies where the public realm was almost entirely closed to dissenting opinion, Twitter and Facebook made it possible for democratically minded protesters to share information, to organise protests, and, ultimately, to topple institutionally entrenched dictatorships. This is a Western position that arguably puts too much emphasis on the technology at the expense of social forces. After the democratic gains across the Arab world proved unsustainable, or curdled into violence, another facet of the technology emerged. Within a few years, Daesh was using the internet with great sophistication to mobilise recruits, spread propaganda, and encourage attacks in the US and elsewhere. Then came an actual attack on Western democracy conducted via social media itself—the spread of Russian disinformation as part of efforts to sway the UK Brexit vote and the 2016 American presidential election.

LikeWar argues that in the space of a decade, the internet has been transformed from a positive space into a battlefield where information itself is weaponised. The online world is now just as indispensable to governments, militaries, activists, and spies as it is to advertisers, shoppers and those looking to find love. And whether the goal is to win an election or a battle, or just to sell a music album, the same tactics are used. Whether what is shown is battlefield footage of a tank being destroyed or a Nazi-sympathising cartoon frog, the aim is to grab attention. Once that has been done, ideologues are able to make contact with a few dozen sympathisers out of a population of millions and then groom them to attack their fellow citizens. Voices from around the globe can stir the pot of hatred and resentment between rival ethnic groups. Foreign actors can influence a country's politics from afar, realising the political objective of a war without arms. *LikeWar* explains how these scenarios are no longer hypothetical. Each has already happened and will happen many more times in the years to come.

The book describes an abrupt and momentous development in war and international politics that has transformed how quickly information spreads,

how far it travels, and how easy it is to access. It explains how information has reshaped everything from military operations to the news business to political campaigns. Singer and Brooking suggest that no country has better mastered the possibilities of this new form of warfare than Russia, a state that has become a master of *maskirovka*. Russia has currently taken the lead in weaponising social media, using its online strength to substitute for its relative decline in military power. This is, perhaps, an essential element of its sharp power strategy. But Russia is leading a crowded field: Singer and Brookings argue that states across the globe have similar programmes under way, from crackdowns in Turkey to China's bold new social credit system that is priming an entire society for digital management of everyone's online activity and turning it into a single 'trustworthiness score'.

The internet has given governments not just new ways of controlling their own people but also a new kind of global reach through the power of disinformation. In many ways, Russia's far-reaching strategy to influence other countries' domestic politics through social media is not limited to sending targeted messages to people in particular micro-marketing categories. It also aims to jam the entire democratic political process by flooding the digital and political space with division, dissension, and distrust, pushing conspiracy theories and lies and supporting the most extreme voices in any debate using its army of trolls and bots.

One explanation for the potency of this new battle zone and the way it has been revolutionising warfare is its congruence with newly evolving forms of information capitalism. We are most familiar with this from Facebook, but in reality, information is the common currency of the influence industries. As Singer and Brooking point out, social media now form a human-made environment run by for-profit companies. Its platforms are designed to reward not ethics or veracity but 'virality'. Online battles may be about politics and war, but they are propelled by the financial and psychological needs that underly the algorithms of the attention economy, as calibrated by clicks, interactions, engagement, and immersion time. This changes what it takes to win, whether the fight is a marketing war, a real one, or a strange hybrid of the two. Figure out how to make something go viral and you can overwhelm the truth itself.

There is also a consensus as to what works in this battle space: Singer and Brooking examined the tactics of a top Daesh recruiter, Taylor Swift's marketing team, Donald Trump's campaign managers, and neo-Nazi trolls, and they found consistent patterns. For all the seeming complexity, there are certain dynamics

DOI 10.30966/2018.RIGA.6.8.

that govern virality: narrative, emotion, authenticity, community, inundation, and experimentation. Those who prevail are those able to shape the story lines that frame public understanding, provoke the responses that impel people to action, connect with followers at a personal level, build a sense of fellowship, and do it all on a global scale, repeatedly, using individual reaction to each tweet or post as feedback data for future refinements.

A powerful claim by the authors is that the laws of this new space have been re-set by a small number of people who can instantly shift an information war in one direction or another. *LikeWar* uses Mark Zuckerberg and Twitter CEO Jack Dorsey as examples of how concentrated digital power has become. Unfortunately, it seems to be the case that these social media giants have failed to think through the political, legal, and ethical dimensions of the once-positive information space they were among the first to colonise. Nor have they planned contingencies for how bad actors might abuse, and good actors misuse, this space. They turn to technology as the answer, above all the burgeoning fields of artificial intelligence, machine learning, and automation. They believe this might solve the crises of the negative space problems of censorship and content moderation. But, as Singer and Brookings explain, it is not difficult to foresee that AI systems will also be weaponised.

It should be added that there is an opportunity cost to this abuse and misuse of social media. The extent to which social media has led to the force-draft enrolment of every digitised individual into a new kind of continuous online battle space means we have lost sight of the possibilities of social media to accomplish positive change. Access to social media can allow people to form new kinds of networks, expose crimes, save lives, and prompt far-reaching reforms. When it is used to foment violence, spread lies, spark wars, and even erode democracy itself, all those benefits are eroded.

As with Kavanagh and Rich's work, the authors of *LikeWar* see public policy playing a major role in helping to improve the quality of citizens' online environment. Indeed, corporate and state action is essential: there are important things individuals can do, but they won't matter unless actions can be taken by companies and by governments. Digital literacy is one part of the puzzle, as are regulation and the employment of AI to police digital social space.

LikeWar is a book about how the internet changed war and politics. It is also a story about how war and politics changed the internet. Because the internet is always evolving, our response must evolve with it. In the words of P.W. Singer:

'Social media may have started out as a space for fun, but it has also now become a new kind of battlespace. And it is one that has threatened NATO like the alliance has never been before.'[7]

7 From a private interview with P.W. Singer, co-author of *LikeWar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, 2018) on 30 January 2019.