Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

# Whose Truth?
## Sovereignty, Disinformation, and Winning the Battle of Trust

John T. Watts

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

SOVEREIGN CHALLENGE CONFERENCE PAPER

# Whose Truth? Sovereignty, Disinformation, and Winning the Battle of Trust

John T. Watts

ISBN-13: 978-1-61977-561-9

*Cover photo*: Japanese people protesting against the US Marine Corps base Futenma in Ginowan on 2009-11-08. (Nathan Keirn/Wikimedia Commons *https://www.flickr.com/photos/23093243@N03/4084803041/*)



September 2018

# CONTENTS

# INTRODUCTION

Disinformation, propaganda, and deception are concepts as old as conflict itself. But aided and amplified by the intersection of technological, cultural, and geopolitical changes, disinformation today creates risks to every aspect of society and undermines the institutions on which nations rely to function. In its most extreme form, disinformation threatens the sovereignty of nations and even poses risks to the rules-based international system. The scope and significance that disinformation has played in recent military conflicts, domestic politics, and international affairs has made the topic a particularly relevant focus for US Special Operations Command (USSOCOM) 2018 annual Sovereign Challenge conference. Established in 2005, the Sovereign Challenge program assists allied and partner nations in understanding and preparing for threats to their sovereignty by bringing together international Defense Attachés and other national security diplomats from across Washington with experts drawn from academia, business, media, and government.

Disinformation presents a particularly interesting challenge for governments to consider. Much of the impact of, and responses to, disinformation fall outside of the roles and responsibilities of government organizations. Yet the implications of disinformation campaigns create a multitude of risks and threats that governments must understand and be prepared for. The first-order effects of disinformation mostly impact individuals and communities in political and cultural ways. But collectively, the second- and third-order effects create a much greater risk to the entire system. Governments and military organizations must react, yet the ways and modes of that reaction must be carefully calibrated in order to avoid doing more harm than good. National governments must find a way to encourage and support wider, whole-of-society responses while resisting the urge to overreach. There is no single or easy solution, and each national context must be taken on its own merits. But through the wide-ranging discussions at this year's Sovereign Challenge conference, a number of key themes and considerations emerged from which the broad contours of an effective response begin to emerge.

Within this context, the conversations at the 2018 Sovereign Challenge conference were both provocative and enlightening. This paper will seek to summarize some of the key themes and insights from those discussions, weave them together into larger lessons, and build upon them to encourage further discourse. There are many ideas here drawn from others' excellent work and experience. Wherever possible, those ideas and further discussions will be linked through footnotes for readers to delve deeper and understand the original context from which these ideas were drawn. This paper owes much to all the speakers and participants of that conference, as without them the paper and the ideas it contains would not have come to be.

# SOVEREIGNTY AND TRUST IN A COMPLEX INFORMATION ENVIRONMENT

Sovereignty is a concept that lies at the heart of the Treaties of Westphalia, and therefore at the heart of the modern international system as we know it.[1] It is essential for the orderly conduct of international affairs and has been a key feature of the relative peace and security experienced by the world in modern times. However, it has been challenged repeatedly, and academics have prematurely declared an end to its modern relevance more than once. Today, those challenges are greater than ever. As rising powers seek to revise key tenets of the international rules-based system, as geographically dispersed religious and ideological extremist movements grow around the world, and as technology connects individuals in new and powerful ways, the concept of sovereignty faces greater challenges now than it ever has in the past.

Many of the challenges to sovereignty are not new. But the size, scope, and implications of those challenges today are sufficiently significant that they have developed new characteristics and now have the potential to be destabilizing. While the increasing multipolarity of the international system brings many positives, it likewise brings the return of great power competition. Large-scale, high-end conventional conflict is thankfully not a certainty from this increased competition, not least because it would result in such devastation that any advanced nation would seek to avoid it at almost any cost. However, the multipolarity in this new environment is volatile, and the need to achieve strategic aims without risking conventional conflict has fueled the development of hybrid capabilities that destabilize and undermine adversaries without breaching the threshold of open confrontation. This has reinvigorated the need for and utility of proxies and has coincided with the emergence of potent and disruptive technologies that empower actors in new and meaningful ways.

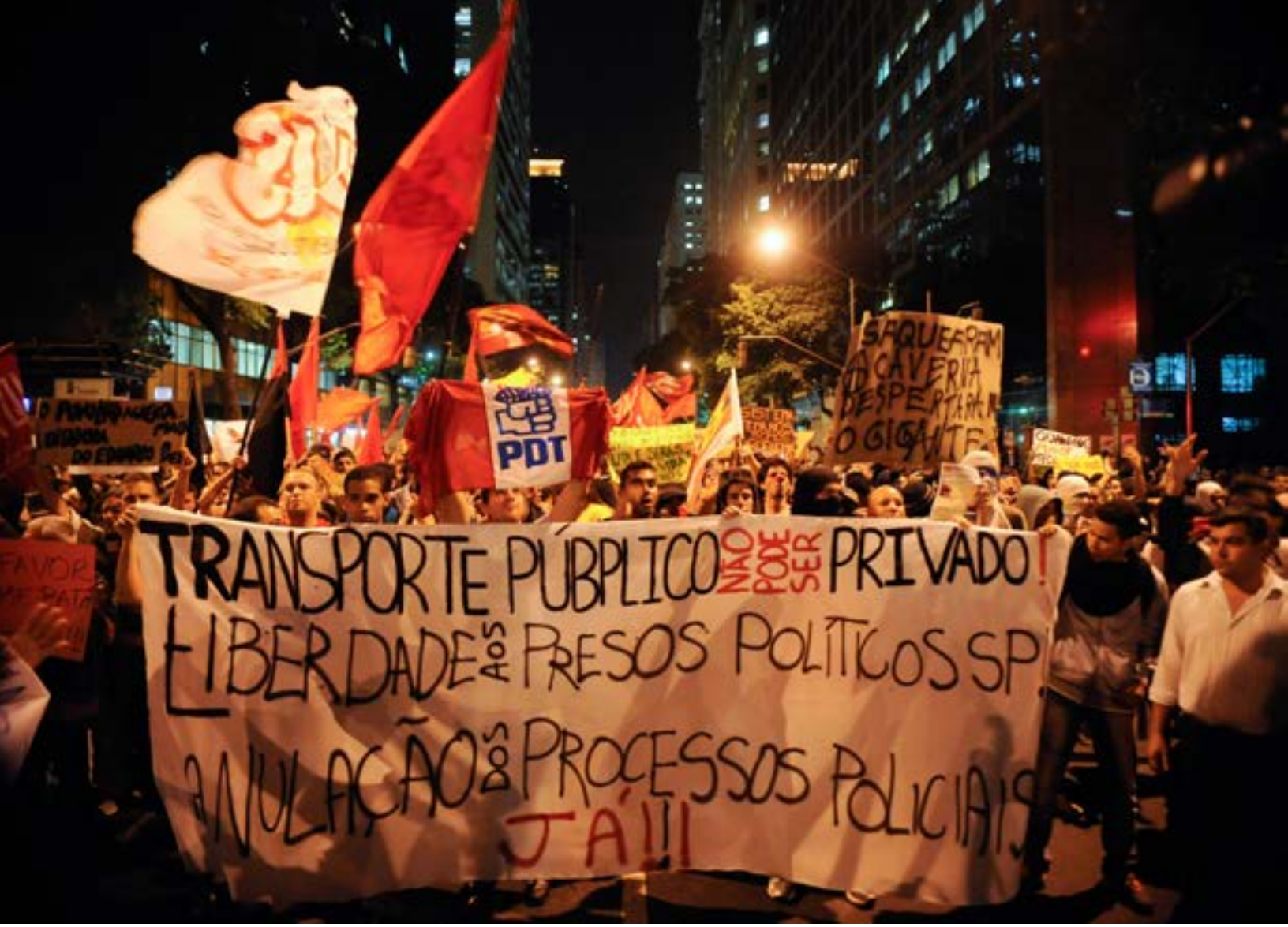
The technologies that define the modern era are not a threat in and of themselves. But the anonymity that new technologies provide, granting individuals and groups plausible deniability while amplifying their actions to an exponentially greater scale and scope, gives extant challenges a complexity and consequence beyond what we have experienced in the past. The democratization of technology has given individuals capabilities on par with corporations, and has given corporations capabilities previously within the purview of states. States, meanwhile, now have capabilities that we do not yet fully understand and which lack properly defined limitations, restraints, and international norms.

Sub-state, irregular, and lone actors have harnessed these capabilities to threaten the sovereignty of nation states in ways not seen in the modern era. After the industrial revolution, state control of powerful, expensive, and complex technologies gave them capabilities that few irregular groups could have hoped to possess. This limited the ability of sub-state groups to challenge national militaries, except in creative, resourceful, or specific ways. The continued advance of technology, however, is now reversing this trend. Pseudo-nations such as the Islamic State of Iraq and al-Sham (ISIS) have shown how organized, savvy, and disciplined sub-state groups can genuinely challenge a nation's sovereignty.

Sovereignty is inherently abstract. It is foundational to the concept of the modern state, yet it has no natural form. It relies on acceptance and recognition by individual citizens, organizations, and other nation states. It is made tangible and real by the national institutions that carry out actions on the state's behalf, fulfil the state's obligations to its people, and ensure the functioning of a rules-based society. For a rules-based order to function, there must be trust that each individual will be treated fairly and equally, and that those who fail to adhere to the community's standards will be punished. This is true for all forms of government as even the most oppressive must ultimately respond to the desires of its populace if it is to be sustainable. But it is particularly true in democratic ones and is true at every level: from a small financial transaction through to the peaceful transfer of political power from one government to another. Where this trust breaks down—through government corruption, persecution of minorities, or the failing of key institutions—societies cease to function effectively.

Trust is the foundation of a functioning society, and it relies on the perception and beliefs of the citizens who constitute it. It is the trust of a society in the institutions

1 Richard N. Haas, "World Order 2.0: The Case for Sovereign Obligation, "*Foreign Affairs*, January/ February 2017, https://www.foreignaffairs.com/articles/2016-12-12/world-order-20.




Brazilian Protestors, 2013 *Photo Credit:* Tânia Rêgo, Wikimedia Commons (*https://commons.wikimedia.org/wiki/File:2013_Brazilian_protests.jpg*)

of government that give sovereignty its legitimacy and power. It is also, therefore, a critical vulnerability that is underpinned by the information upon which people build their perceptions and beliefs. All societies rely on trust to function, but it is particularly critical in democracies. Disinformation erodes trust by shifting societies' perceptions and beliefs about government and its institutions. This can result from actions by external threats, but also occurs organically when disinformation about basic facts, scientific methods, and conspiracies are spread to sow confusion and advance specific agendas. When disinformation creates false perceptions and undermines beliefs, societal trust is eroded and thereby a nation's sovereignty threatened.

Unfortunately, trust in Western society is experiencing a crisis. The 2018 Edelman Trust Barometer has tracked this erosion, showing a 30 percent drop in trust in government over the last year in the United States. The Trust Index shows that average trust in institutions (including government, media, nongovernmental organizations, and business) among the general population dropped from 52 percent in 2017 to 43 percent in 2018—the steepest decline they have measured in a country. Among the "Informed Public," that same trust plummeted from 68 percent to 45 percent over the same period.[2] These findings, particularly around trust in media, are reinforced by studies done by Gallup[3] and Pew Research Center.[4] In the United States, part of this

2 Edelman, *2018 Edelman Trust Barometer: Global Report*, http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf.

3 Art Swift, "Americans Trust in Media Shrinks to a New Low," *Gallup News*, September 14, 2016, https://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx.

4 Amy Mitchell et al, "Trust and Accuracy" *The Modern News Consumer: News Attitudes and Practices in the Digital Era,* Pew Research Center, July 7, 2016, http://www.journalism.org/2016/07/07/trust-and-accuracy/.

can be explained by party affiliation, as there is a wide divergence in trust in institutions depending on voting preferences in the last election. As disinformation is often used to exaggerate beliefs and perceptions of different political groups, these data indicate a broader role played by local politics and culture in the erosion of trust and the disproportionate impact disinformation has at that level.

It should be noted that globally, the Trust Index barely changed at all, and in some places actually increased, including in China, South Korea, and Indonesia. Despite suffering a significant decline in its Trust Index, India, another of the world's most populous countries, still maintained a higher Trust Index than the United States and many Western nations. This would indicate that the challenges of trust are impacting countries to different degrees, without clear correlations between geographic regions or forms of government. This also highlights the importance of understanding the circumstances in each individual country, and particularly the significant cultural and local political elements of the challenge, which is further supported by a look at the number of markets with extreme changes over time. Moreover, there were significant losses in trust in 2014, 2015 and 2017, but gains in 2013 and 2016, indicating that it is not a steady erosion caused by technological changes, but rather a response to specific events.[5] This is also important as it demonstrates that trust can be regained over time with appropriate responses.

There appears to be a generational aspect in the changes to trust. Through the mid 2000s, the Edelman Trust Barometer notes a shift in trust from "authorities" to "peers" around 2005. By 2007, businesses are considered more trustworthy than government or the media, leading to a fall in the trust of government and a crisis of leadership around the start of this decade.[6] It is worth noting that this shift in trust from authorities happened at the dawn of the social media age but before it had become mainstream. Myspace and Friendster were used by younger generations, but mostly for sharing personal interests. Facebook launched in 2004, but was not available beyond the community of students at Ivy League schools for several years, and didn't surpass Myspace in popularity until around 2010. Meanwhile, Twitter launched in 2006. It is therefore hard to argue that the current loss of trust results solely from the emergence of social media, though there can be little doubt that it acted as a critical amplifier of broader trends.

## Information Overload

A thorough discussion of the growth of disinformation in the modern information eco-system raises larger and more difficult questions. In any examination of disinformation, it is inevitable to note that disinformation, censorship, and propaganda are nothing new. Control of information and truth have always been vital to the exercise of power, evidenced by the importance of seizing media and communications infrastructure for the successful execution of an attempted coup. But the scale and the scope of today's technology along with the connectivity and interdependence of the globalized world make the impacts exponentially more severe. Just as with the question of the role of technology, there is a question of causation and correlation in the relationship between disinformation and politics. Specifically, does disinformation create political polarization? is it a result of existing polarization? Or are they mutually reinforcing? After all, the disruption the international system is currently experiencing is a result of the convergence of multiple trends and is impacted by a variety of factors. It could be that the severity of the impact disinformation has had on some countries, and on the international system, is a result of these forces as much as culture and technology. Dr. Richard Haass, of the Council of Foreign Relations, has characterized this period as a "post-superpower" age, where power is more decentralized and decision makers have greater capability than they previously had creating an uncertain and increasingly unstable international system.[7] It may be that rather than disinformation, the power and influence of disinformation has appeared to be larger than it would otherwise be because of the vulnerability of the international system and subsequent fragility in its institutions.

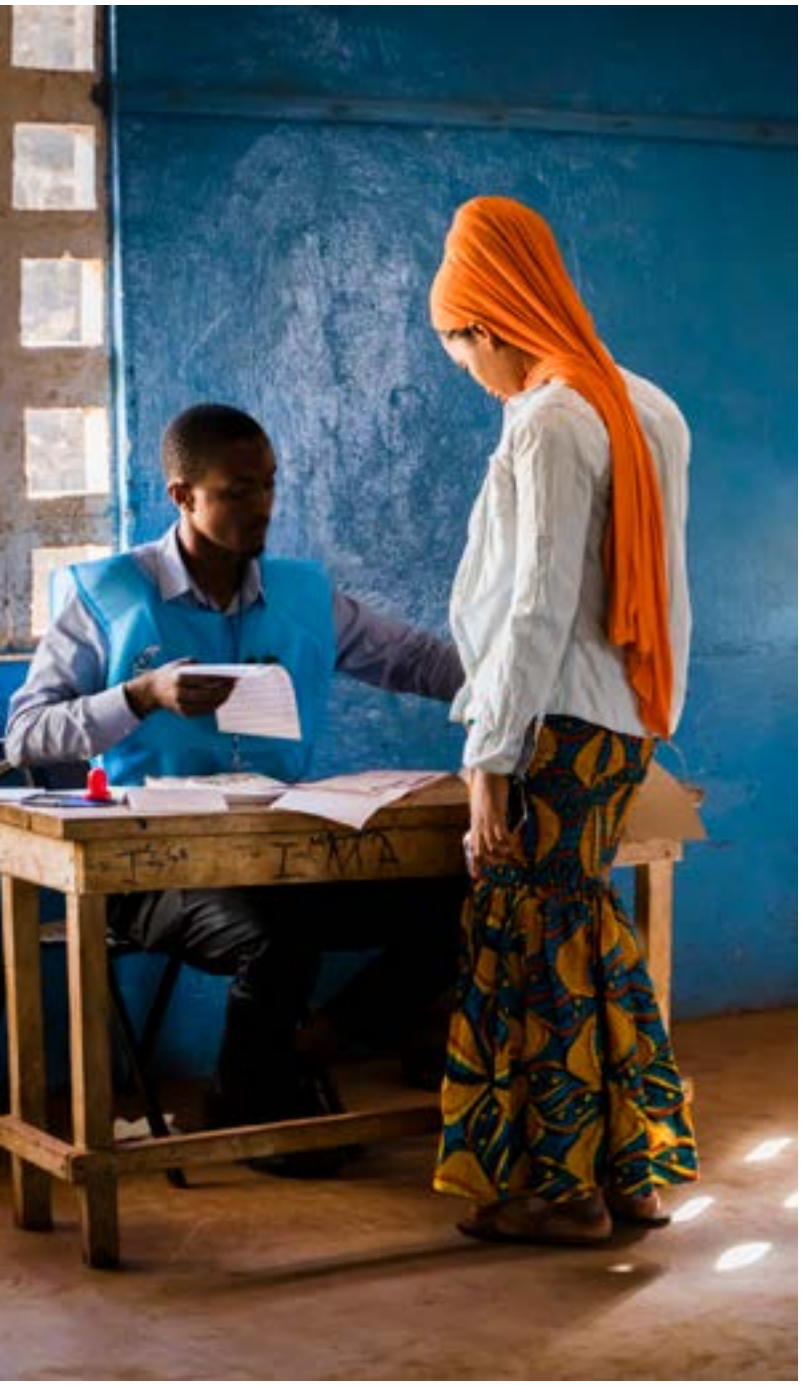
The ascendancy of disinformation and its political ramifications could also arise as a result of a paradigm shift we are experiencing but have simply not yet adapted to. In his book, *The Signal and the Noise*, Nate Silver argues that the disruption we are currently experiencing is no different from the "information overload" experienced after the creation of the printing press is 1440. Silver argues that the sudden accessibility of large quantities of information can overwhelm society. He argues that too much useless and poor-quality information results in increased isolation and polarization driving people to down select—that is, actively reducing the number of choices they consider—to limited sources of information and simplified narratives that fit our preconceived biases.[8] Just

5 Edelman, *2018 Edelman Trust Barometer*.

6 Edelman, *2018 Edelman Trust Barometer*.

7 Richard N. Haass, "World Order 2.0: The Case for Sovereign Obligation."

8 Nate Silver, *The Signal and the Noise,* Penguin Press, 2012, pp 1-12



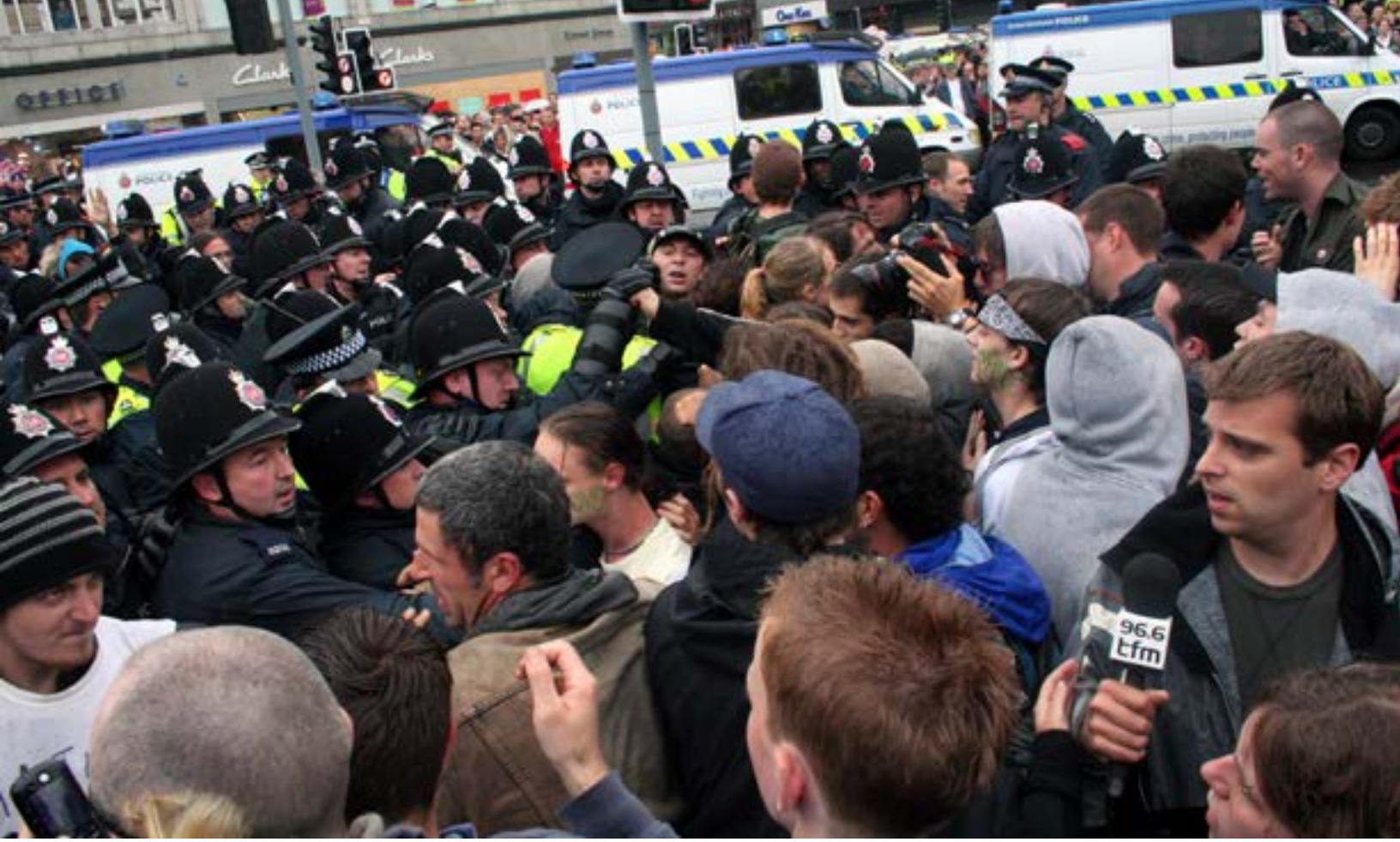
Voting in Sierra Leone, 2018 *Photo Credit:* Carol Sahley, USAID (*https://www.flickr.com/photos/usaidafrica/26824870737*)

as decades, and arguably centuries, of conflict and disruption followed the invention of the printing press, the invention of the internet is similarly creating conflict and disruption.

While the promise of unlimited information is seductive, it is also deceptive. Technology has democratized the ability for sub-state groups and individuals to broadcast a narrative with limited resources and virtually unlimited scope. Incidents can be broadcast around the world in real time from smart phones, while their appearance of being live and on-the-ground give them a veneer of authenticity. Yet they can be selective in what they show, lack context, and even be edited to mislead. This has resulted in the rise of battling videos where opposing groups seek to release additional "authentic" footage to provide greater context and counter the narrative. Meanwhile, those seeking to amplify a message carefully select the "facts" that suit their own agenda, and few seek further validation of authenticity. There are too many events, breaking news, and scoops for any individual to effectively process. As professional curators and gate-keepers dwindle and are replaced by self-appointed and unaccountable ones, individuals are forced to assess information in ways for which they are not trained.

This multitude of information sources, many of which cannot be trusted or relied upon, has several implications. The most important of these is the loss of shared facts. Without shared facts, society lacks the basis for a rational discourse. It is impossible to debate the nuances of policy when neither side can agree on foundational facts. And it is almost impossible to establish those facts when basic scientific methods are called into question and the lack of trust in the institutions that generate that data is dismissed by one side of the debate. This results not only from changes to the media industry, but from cultural trends borne of internet usage. The ability for individuals to find others with specific, niche, and in some cases fringe, interests and beliefs has allowed a multitude of internet enabled subcultures to develop. Most of these are benign. But technology works equally well for the benign and the malign, and those with radical and extremist views have been empowered as much as everyday hobbyists. These online subcultures create echo chambers where views are validated and reinforced, and individuals are incentivized within those subcultures to develop and amplify the core beliefs of the group. In many cases, these group have directly contributed to the erosion of established facts in pursuit of their beliefs, such as with the many "truthers," "chemtrailers," "anti-vaxxers" and other conspiracy theorists who believe that commonly held facts are inherent lies. These issues are often underpinned by pseudo-science and selective research as well as the misinterpretation of publicly available information, which has been taken out of context. Often, the concepts are given greater credibility and publicity through endorsement by high profile public figures.

It is no surprise that in this complex information environment, some raise questions about the very nature of



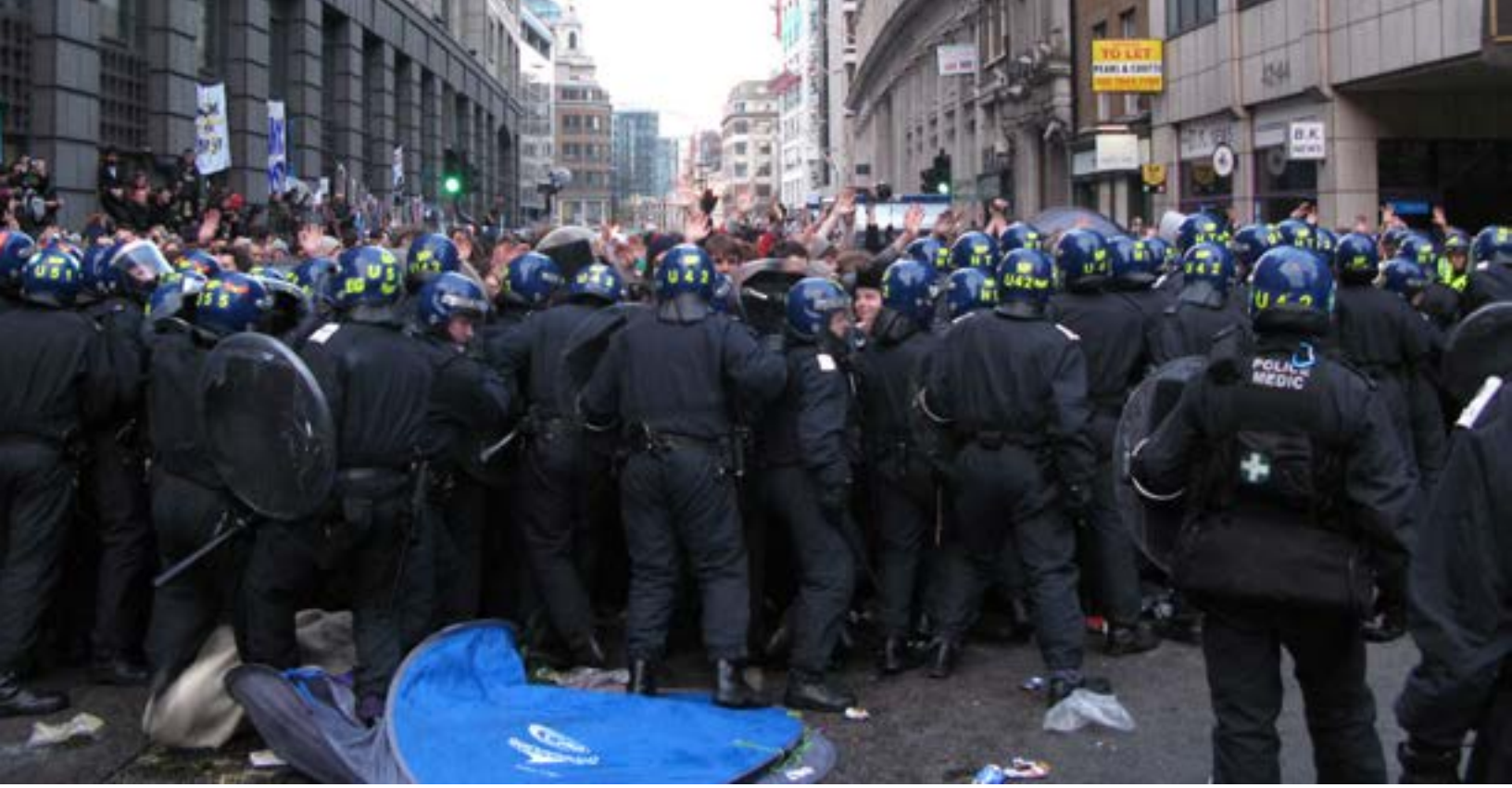

Police and protesters clash in Edinburgh ahead of the G8 protests, 2005 *Photo Credit:* Sam Fentress, Wikimedia Commons (*https://commons.wikimedia.org/wiki/File:EdinburghProtests1.jpg*)

truth. A discussion of what constitutes truth can quickly become deeply philosophical, abstract, and challenging. It echoes the writings of some of the world's greatest thinkers, from Plato to Descartes. These discussions arose during the Sovereign Challenge conference, and they illustrated how difficult it can be to agree on the definition of even the most foundational elements of the discussion. A thorough examination of these terms, their definitions, and the logic that underpins them belong in a longer and more academic piece. But for the purposes of this discussion, it is necessary to establish some simple working definitions. While "fact" and "truth" are often considered synonymous, they actually have very different meanings in this discussion. The commonly held definition of "facts" are that they objectively exist in reality, regardless of belief, culture, or other consideration. They cannot be logically disputed. "Truth" on the other hand is made up of facts, but can be tempered by beliefs and interpretation. As such, two people can draw two different "truths" from the same set of facts.

The lack of shared facts combined with down selected and fractured voices of trust and credibility has created information "bubbles." These are clusters of like-minded information sources that share similar views, promote similar interpretations of facts, and therefore present their own "truth." Often people are attracted to bubbles that reinforce their own biases and beliefs, eliminating objectivity around facts and truths. This questioning of underlying shared facts, the methods of establishing them, and the subsequent proliferation of contrasting disinformation has led to many questioning whether we now live in a "post-truth" era. While this is a legitimate question, it could equally be argued that in this era of information overload, the environment is better characterized as a moment of heightened competition between competing truths. If truth can be subjective, and even the individuals understanding of basic facts are no longer commonly shared, the question becomes whose truth is correct. As people react to the overload of information by down selecting the sources that they trust, they become vulnerable to the bias of those sources and to those who seek to manipulate them for their own ends.

## Media and the Information Marketplace

It is no coincidence that the erosion of trust in Western nations coincides with turbulence and disruption in the media industry. Around two thirds of the US population




Riot police officers "kettle" protesters at the Bishopsgate Climate Camp, London, 2009 *Photo Credit:* Charlotte Gilhooly, Wikimedia Commons (*https://commons.wikimedia.org/wiki/File:G20_climate_camp_police_kettling_protesters.jpg*)

worry about fake news, and believe that fabricated news causes confusion, particularly about basic facts.[9] This loss of truth and trust is neatly demonstrated by the Edelman Trust Barometer, In which 59 percent of respondents to the survey stated they are no longer sure what is true and what is not with 56 percent not sure which politicians to trust and 42 percent not sure which businesses.[10] A central challenge in the modern media environment is the explosion in potential sources of information or "content" with limited accountability resulting in a dilution of the quality. Importantly, the Edelman survey defined media as not only journalists and traditional publishers, but also "influencers," "brands," and broadly defined "content producers."

This explosion in the quantity and diversity of information and concurrent loss of shared facts has led to the challenging of commonly held truths. In the past, the general public had limited sources of information, which were managed by professional gatekeepers who were held accountable for the veracity and validity of the information they shared. Today's gatekeepers lack the accountability and consequences to deter the spread of false information. In many cases, the current structure of the media environment incentivizes bad behavior. If we compare the case of small, local news rooms to a large multinational "click bait" website, it is not hard to understand how we reached our present position. The market for local news is inherently limited and fractured. Local news requires a multitude of small organizations with high overhead costs and limited audiences. In the current media environment, where content producers are funded by advertisers that compensate based on website traffic, no one local site can compete with a national or international news source that has a potential audience of millions. This causes a rationalization of the market, producing a handful of winners amongst the large media organizations while the smaller ones are closed.[11] The ripple effect is the formation of a vacuum of and demand for locally relevant information, filled by bloggers and untrained content producers who do not follow journalistic convention and are not held liable, which keeps their overhead costs low enough to be viable. They are also incentivized to amplify attention grabbing but potentially misleading content to drive up their web page traffic and therefore their revenue.

9 Michael Barthel, Amy Mitchell and Jesse Holcomb, "Many Americans Believe Fake News is Sowing Confusion" *Pew Research Center*, December 15, 2016, http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/.

10 Edelman, op cit.

11 Paul Farhi, "Charting the years-long decline of local news reporting," *Washington Post*, March 26, 2014, https://www.washingtonpost.com/lifestyle/style/charting-the-years-long-decline-of-local-news-reporting/2014/03/26/977bf088-b457-11e3-b899-20667de76985_story.html?utm_term=.7a04cdebd0eb.

Because the market is structured to incentivize those who prioritize emotion, fear, and drama over truth, the saturated market forces content producers to continually push the boundaries of acceptability in search of greater attention and market differentiation. Those who can generate the most attention by playing to the audience's greatest fears, bias, and ignorance will generate more revenue. In this environment—where any individual can generate, modify, or subvert facts for material or political gain— there are multi-tiered incentives for individuals and groups around the world to generate misinformation and disinformation for little cost and significant reward. In contrast, truth telling and fact checking are expensive and of arguably less material value. Until the balance of this equation is shifted, either through incentivizing truth or increasing the costs of falsehoods, this trend will continue. Fortunately, shifts in the policies of social media platforms such as Facebook have had significant[12] impact on the type and quality of the content that is broadcast.

Another effect of the economic pressures on professional media providers is the tendency to cut costs by utilizing content generated by others with little modification or verification. As a result, companies and nongovernmental organizations (NGO) are evolving their press releases into complete articles developed by in-house storytellers—that is employees of a company who generate complete media for distribution through independent media channels. This in-sourced content generation allows them to tell their own story and develop their own narrative, knowing that they will reach the public intact but with the credibility of an independent news agency. This development presents an opportunity for organizations but is also a necessity for them to broadcast their message in an environment in which it is difficult to draw attention to the issues they care about. It can also be a power for good when the company or NGO has society's broader interests at heart. But it can also be used to further individual agendas and exacerbate the challenges of disinformation and erosion of trust. Once again, the need for independent and credible gatekeepers along with individuals committed to facts-based content generation will determine the ultimate effect.

The challenges created by the modern information marketplace may be addressed through natural maturation of the marketplace as it adapts to modern dynamics. For those wishing to transmit information, whether it be content producers or advertisers, there needs to be a recognition that "clicks" are a lazy and inaccurate measure of engagement with the information within. In many cases, readers will click on a sensationalist headline but only engage with the material long enough to establish bias, credibility, or answer a central question. Advertisers would get greater return on investment if their message was attached to better quality material that properly engages the reader. Their brand can also suffer harm if it is associated with poor quality or misleading material. By demanding that their advertising is proven to be associated with high quality material, they will eventually realign some of the market forces and shift the incentives of the producers.

In open and free media markets there will be other countervailing and self-correcting forces that will impact the prevalence of disinformation. In Western markets there remains a demand for "truth" among the general public that will incentivize content producers to focus on "truth" and invest in the expensive process of fact checking. Several high-profile media institutions have already made their commitment to fact checking and truth as a marketing tool and competitive advantage. CNN claims, for instance, that they are the "most trusted name in news" and Washington Post is using "Democracy Dies in Darkness" as its branding. Other journalists have described themselves variously as "truth-tellers" or "reality-based" news. However, bias can never be eliminated and the facts that a media organization chooses to present can shift perception of "truth" in and of itself. Some solutions to this challenge are already emerging. Social media platforms are experimenting with tagging news stories on where and how the content producer is funded. Other possible approaches could be to use a grading system akin to that used to rate the cleanliness of restaurants. But the more organizations invest in fact-checking, even if it is just for marketing purposes, the greater the likelihood the foundations for rational debate can be reestablished. Only time will tell how this rapidly changing information will eventually evolve, but the irony is that with the proliferation of disinformation that modern technology has created, traditional media institutions, which were undercut by that same technology, are becoming more important than they have ever been.

Technology is at the heart of the current challenge, and we cannot have an effective discussion about the possible solutions without addressing it directly.

12 Experiments run by Facebook that changed the way information was presented to users in Slovakia, Sri Lanka, Serbia, Bolivia, Guatemala and Cambodia saw a drop in organic interaction with some media entities by 60-75 percent: https://medium.com/@filip_struharik/biggest-drop-in-organic-reach-weve-ever-seen-b2239323413; Changes in the ways Facebook presents content has also been shown to significantly impact content producers business models: https://www.wired.com/story/how-bored-panda-survived-facebooks-clickbait-purge/.

Australia's Parliament House, Canberra, 2009 *Photo Credit:* JJ Harrison, Wikimedia Commons (*https://ml.m.wikipedia.org/wiki/%E0%B4%AA%E0%B5%8D%E0%B4%B0%E0%B4%AE%E0%B4%BE%E0%B4%A3%E0%B4%82:Parliament_House_Canberra_2.jpg*)

As noted above, it is not clear that the emergence of social media platforms and the ubiquity of electronic devices that enable it are the cause of the proliferation of disinformation. But they are indisputably both amplifiers and enablers of it. As such, there needs to be a recognition that mode matters. Social media communication platforms are far more capable and sophisticated than legacy platforms. They play an active role in determining what individuals see and which information is broadcast widely. In decades gone, a telecommunications company would not be held liable for a criminal or terrorist using a landline telephone to coordinate actions or harass individuals. Yet the bosses of social media companies are being called to testify before legislatures and being asked to justify the role their companies play.

It is appropriate that they are held accountable; after all, their platforms engage so many people across the globe and empower individuals to reach huge populations. But there are assumptions built into their algorithms that actively and automatically curate the information people are exposed to and therefore have a material effect on their perspective on facts and truth. Moreover, it is their approach to advertising and rewarding content producers that form much of the incentive structure that needs to be corrected. This is particularly consequential in developing countries where literacy and the critical analysis skills associated with tertiary education may not be as widespread. Internet penetration has exploded across developing countries, and where there is internet access there is often social media use. Facebook, for instance, is used by 90 percent of internet-connected Zimbabweans and 97 percent of Filipinos. For better or worse, they have become political spaces for discourse, and their manipulation has direct effect on political views. These platforms are powerful tools, and ones that are easily manipulated by threat actors seeking to impact the population's political views.

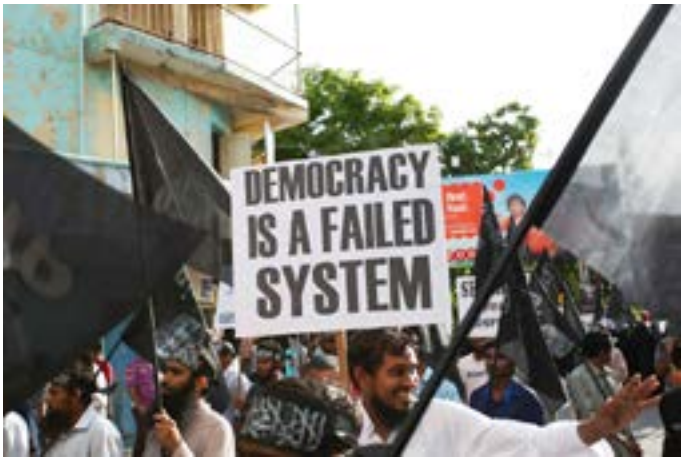
## Multifaceted Challenges and Diverse Threat Actors

In many cases, the trends that have supported the growth of disinformation are organic, grass roots, iterative, and have emerged over a significant time period. But when combined together, their effect is substantial and can impact the views and beliefs of the wider population. When harmful or incorrect ideas are broadcast over social media, they can even influence the views of people who would not otherwise be sympathetic to that perspective. People have a social need for acceptance that influences their higher-order rational thinking, pre-disposing them to accept ideas that are amplified by people they trust. When forwarded by a close friend or relation, false information carries additional legitimacy; once accepted by an individual, this false information can be difficult to correct. Additionally, when people are bombarded with a particular narrative or concept, it is likely that some of it will embed in their consciousness even if they are not inherently sympathetic to that view. There are also signs that once absorbed, incorrect information can be very difficult to dislodge entirely from people's consciousness. Moreover, when the very idea that facts are

wrong exists, or when the information environment is flooded by incorrect information, it devalues the credibility of all sources of information. All these trends create the perfect opportunity for exploitation by threat agents, who are both a symptom and amplifier of this phenomenon.

Extremists are fueled by increased political polarization, and thereby disinformation is both an effect of the extremists' views but also fosters new recruits. The rise in the number and prominence of domestic and international extremists has been enabled by technology that allows them to find ideas that resonate with them, validate personal or perceived grievances, and then connect and coordinate with others who share their views. Many extremists are heavily reliant on social media to self-radicalize, and often do so based on false information created and shared by other extremists. Once radicalized, the same individuals often become amplifiers of disinformation in aid of achieving their objectives and recruiting more adherents, further degrading the information environment. According to the speakers at the conference, self-radicalized extremists disproportionately rely on the internet throughout their radicalization and are more resistant to corrective behavioral re-training than those who have been radicalized by a community. They therefore pose a threat to the sovereignty of a nation in two ways: they contribute to the disinformation environment and the concurrent erosion of trust, and they may also pose a physical threat to the state and broader population.

Disinformation has also become a common political tool in many countries, with extremists in particular harnessing the medium to influence political views. In Indonesia,[13] India,[14] and many other developing countries, teams work full time to track narratives, smear opponents, and spread disinformation as part of normal political campaign activity. In doing so, they stoke sectarian and religious tensions and increase political polarization. In Kenya during the 2017 election, Islamist extremists and agitators of tribal divisions used similar techniques to actively engage anyone who may be sympathetic to their views. Digital penetration in Kenya is one of the highest in Sub-Saharan Africa at almost 90 percent, with around 72 percent of those users active on Facebook. Over twenty extremist groups took advantage of this platform to communicate with their




Street Protests in Maldives, 2014 *Photo Credit:* @DyingRegime, Wikimedia (*https://commons.wikimedia.org/wiki/File:Street_protest_calling_for_Sharia_in_Maldives,_Democracy_failed_system_poster.jpg*)

28,000 followers and aggressively recruit anyone who showed interest in their cause.[15] This trend highlights that the threat and impact of disinformation arises from and affects all levels of society, and responding to only one source of that disinformation will not be sufficient to eliminate the problems it causes.

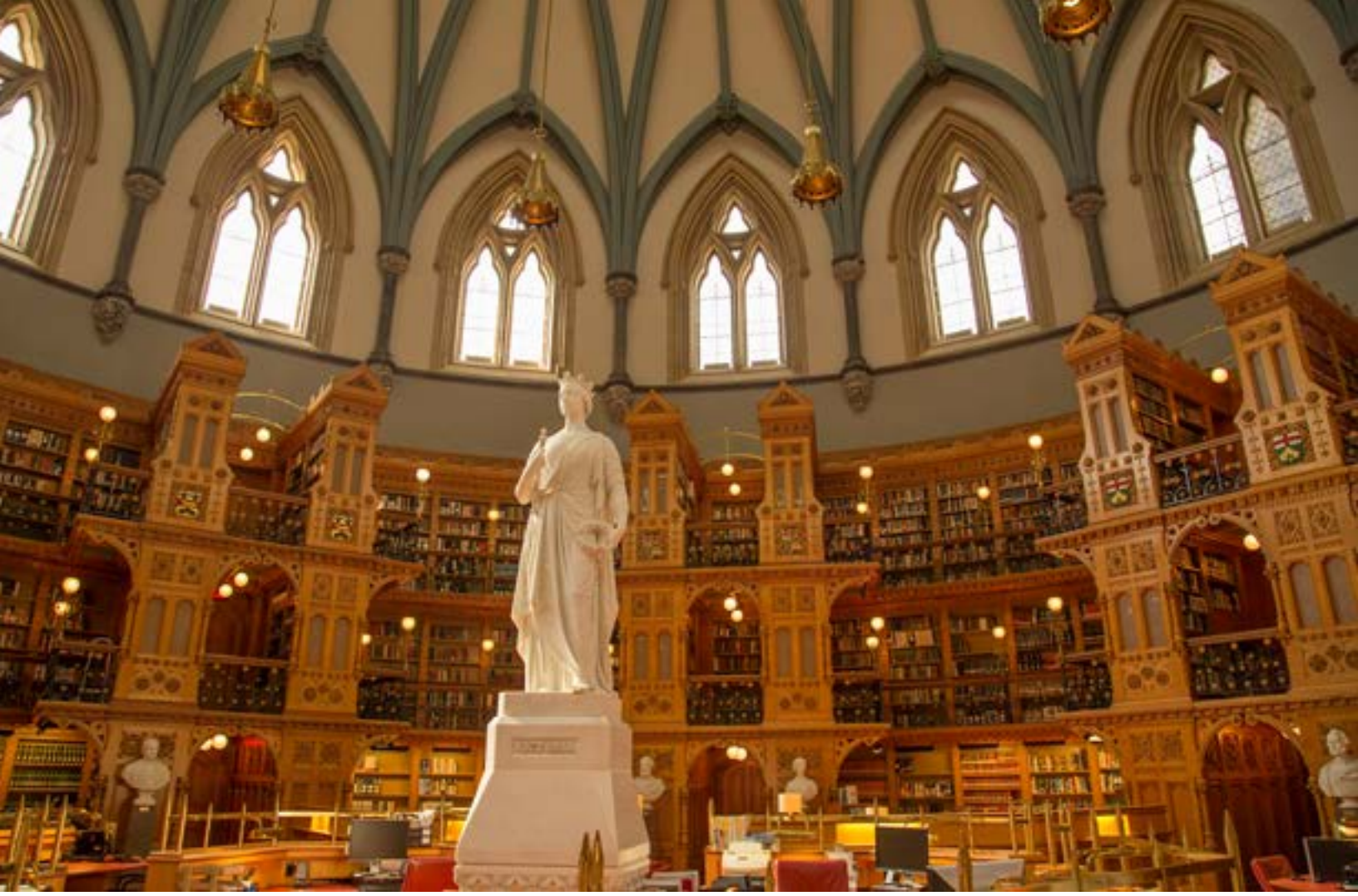
The spread of this disinformation can be dangerous, but a response by a national government risks interfering in political processes and further eroding institutions and norms. While there are many legitimate reasons for states to attempt to regulate and restrict the spread of disinformation, there is also the risk that the cure becomes more damaging than the ailment. In many developing nations, there are legitimate irregular and terrorist threats to national institutions and to the general public. But even in the most benign and justified circumstances, the justification of responding to disinformation spread by threat actors can be used to suppress minorities and political rivals, often validating the extremists' message and assisting them in recruiting new supporters.

In places such as Myanmar, United Nations (UN) human rights investigators have discovered clear links between hate speech spread through social media and atrocities undertaken against the Rohingya minority there. Yet the government of Myanmar has also sought to restrict

13 Yenni Kwok, "Where Memes Could Kill: Indonesia's Worsening Problem of Fake News," *Time*, January 6, 2017, http://time.com/4620419/indonesia-fake-news-ahok-chinese-christian-islam/.

14 "Whatsapp: Mark Zuckerberg's Other Headache," *Economist*, January 27, 2018, https://www.economist.com/news/business/21735623-popular-messaging-service-shows-facebooks-efforts-fight-fake-news-may-fail-whatsapp.

15 Zahed Amanullah and Anisa Harrasy, "Between Two Extremes: Responding to Islamist and Tribalist Messaging Online in Kenya During the 2017 Elections," *Institute for Strategic Dialogue*, 2017, http://www.isdglobal.org/wp-content/uploads/2018/02/Between-Two-Extremes-Feb-2018-ISD.pdf.



The Library of Parliament Ottawa Canada, 2014 *Photo Credit:* Tony Webster, Wikimedia Commons (*https://commons.wikimedia.org/wiki/File:The_Library_of_Parliament_Ottawa_Canada_6D2B5588.jpg*)

press access to those same atrocities to prevent accurate reporting of the truth, entrapping two journalists and arresting them on arcane charges. As countries such as Malaysia and Thailand seek to tighten rules around reporting and prosecute purveyors of "fake news," and independent news agencies in Cambodia and the Philippines are closed on regulatory grounds, there is a risk that the response to disinformation could be used as a tool for authoritarian regimes to eliminate dissent.

After all, nation states are not only the victims of disinformation and the accompanying drop in trust. Throughout history they have also been the perpetrators, using disinformation both against other nations and domestically. Freedom House has tracked government use of disinformation, distortion or manipulation online in thirty countries including trolls, bots, and false news outlets.[16] In the Philippines for instance, where, as previously mentioned, 97 percent of internet users have Facebook accounts, a "keyboard army" was employed to generate support for the government's brutal campaign against drug dealers and smother independent reporting of it. These irregular internet proxies drown the truth by flooding the information space with lies and falsehoods. They attack the credibility of any who speak out and harass them online. Using the network effect of social media, 26 Facebook accounts were tracked and discovered to be sending out identical incendiary narratives to over 12 million accounts.[17]

In countries such as Venezuela, the state itself has been the greatest threat to national institutions, deliberately dismantling and undermining them and politicizing what remains. Venezuela has systematically forced the closure of media outlets that criticize the government, using regulations, legal technicalities, and economic

16 "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy" *Freedom House*, https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy.

17 Lauren Etter, "When the Government Uses Facebook as a Weapon?," Bloomberg, December 7, 2017, accessible at https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook.

pressure. The government there has ousted independent leadership from national institutions including within the oil industry and military, then politicized the remaining staff. The government has also repressed the media by attacking journalists, rescinding permits, and having allies purchase media organizations to prevent opponents from utilizing them. When independent media companies such as RCTV moved to foreign jurisdictions, the cable channels they broadcast on were pressured into dropping their broadcasts and the advertising market was depressed to control content.

The erosion of trust in media and institutions, particularly in the West, is also the result of deliberate strategic action by adversarial nation states, which are yet another threat actor. Disinformation campaigns have become synonymous with the Kremlin and its informal network of proxies and with good reason. While disinformation occurs at every strata of society and across a continuum of actors, it is the form employed by nation states and their agents for geopolitical purposes that have been the most destructive. The loss of trust in the Western media and the rise of disinformation are no coincidence. While not a cause of the many outcomes already discussed, the Kremlin was able to harness developing cultural and technological trends to better achieve their objectives. Much of this effort stemmed from their experience in the late 1990s following the commencement of its second war in Chechnya. The Kremlin believed that its failure in the First Chechen War was caused by foreign and independent journalists. As with other authoritarian regimes, the Kremlin sought to suppress domestic media. But it was unable to control foreign media, so it sought to undermine their credibility. By harnessing online communities of "patriots" to harass foreign media entities and spread false news stories, the Kremlin discovered a powerful information weapon. They were agile, flexible, and bolder than bureaucratic state agencies and provided distance and deniability.[18]

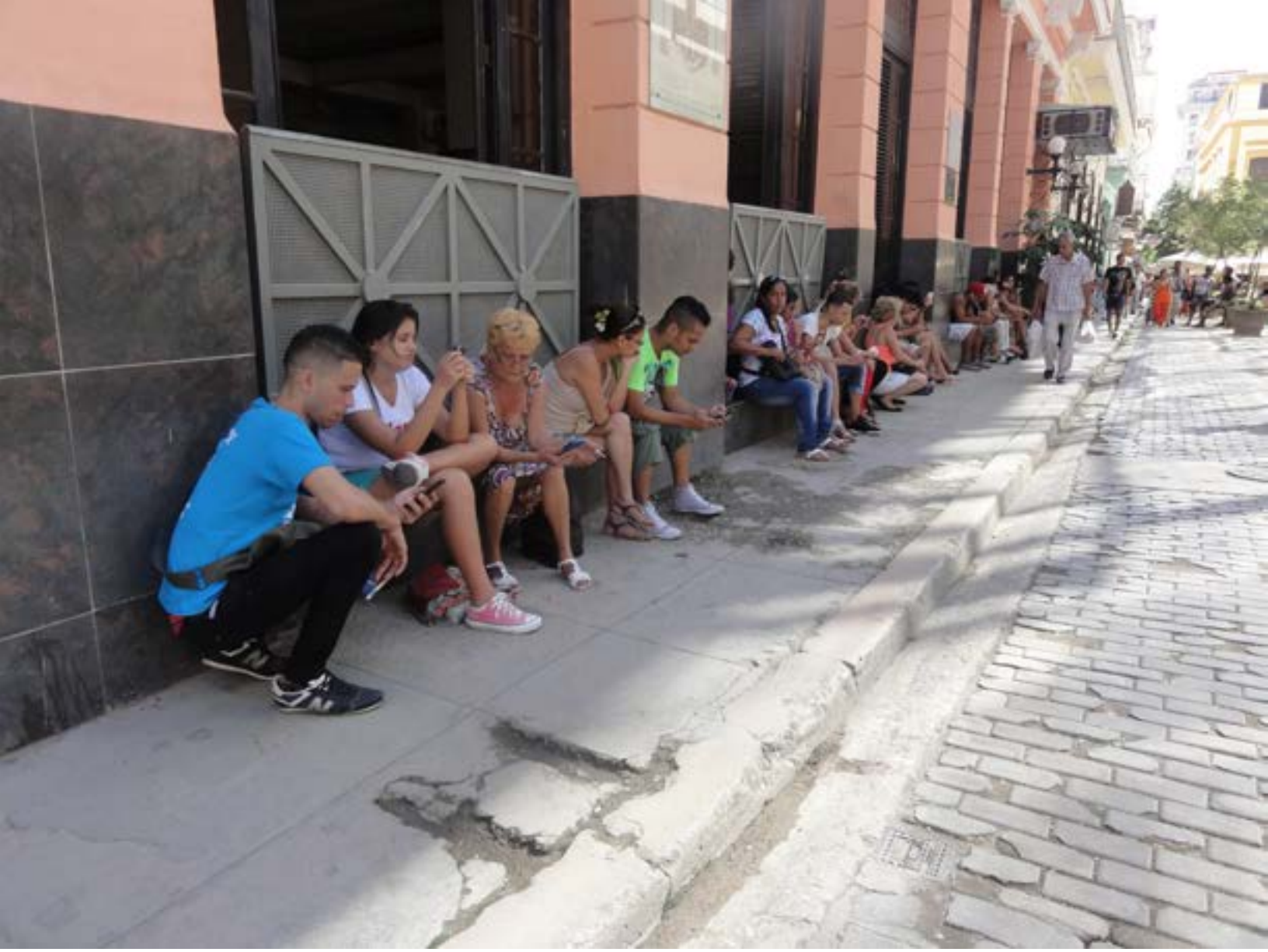
As the Kremlin has become bolder beyond its borders, these proxies have played a critical role in ensuring success for the Kremlin's objectives. The sophistication and capability of these tactics have developed over the past decade. Attempts to place false stories in the Ukrainian media in the early 2000s to shift the Ukrainian government's policy towards Turkmenistan did little. But in more recent actions in Georgia, Crimea, the Ukraine, and Syria, disinformation campaigns have been central to their success. However, it has wider implications than enabling covert military action and political subversion; the success of these proxies has not only undermined Russia's own institutions but also increasingly determined Russian foreign policy instead of the Russian Foreign Ministry. The proxies are easily provoked, unpredictable, and react to perceived threats that may have little or no explicit connection to Russian interests. These proxies also inherently lack accountability, meaning they are unconstrained by the norms and consequences of the international system that usually shape a nation's actions—truly blurring the line between state and sub-state action.

As such, even state-level disinformation campaigns cannot be viewed independently of grassroots activists and extant media, technological, and social trends. A key problem for states now that these groups are active, mature, and empowered is that they lack the controls and accountability of state instruments. They can act impulsively and without any forethought to wider implications. In Kremlin terms, they see the world through the lens of threats to political stability, so even unrelated events—such as Catalonian independence efforts or presidential elections in the Philippines—can be perceived as requiring a response. This was evident in Zimbabwe where trolls attacked opposition activists seeking the ouster of Robert Mugabe as they believed it may create a precedent and example to opponents of Putin. These online activists and networks of proxies, which blur the line between government and grassroots and represent a diverse spectrum of actors, have found a way to use technology to turn tactical actions into strategic effects. Just as increasing globalization and interconnectivity has made local issues global and vice versa, these actors blur the line between domestic and international activity. In this environment, these Russian-based trolls can be expected to move rapidly from involvement in the domestic politics in Zimbabwe to targeting elections in the United States, France, or Sweden, or from Catalan Independence to focusing exclusively on the Philippines.

## Responding to the Changed Environment

Beyond the incentive structures and opportunities that disinformation provides to those who use it, its very characteristics have an asymmetric advantage over truth and facts. Because it often relies on simplifying complex issues and emphasizing existing biases, it is more easily understood by the average person and often has more emotional resonance with its author. All good lies contain some element of truth, which makes them hard to dismiss out of hand and blurs the distinction between opinion and straight falsehood. Disinformation also has more resonance because it is often communicated in

18 Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: Public Affairs, 2015).



Cubans use a WiFi Internet HotSpot in Havana, 2015 *Photo Credit:* Othmar Kyas, Wikimedia Commons (*https://en.wikipedia.org/wiki/File:WiFi_Internet_Access_Havanna.JPG*)

more compelling ways. It creates a narrative that ties together meaning and identity and that communicates a larger message to the reader than the story itself, building on preconceived beliefs and assumptions while reinforcing bias. Familiarity is a key tool of an effective disinformation campaign, as people infer or assume messages that do not need to be explicitly stated. This can be communicated through apparently innocuous terms or imagery and is sometimes referred to as a "dog whistle"—a message that only select segments of a population understand or perceive. Once disinformation and the narratives it supports become truly embedded in a community's culture and gives meaning to people, it becomes mythologized and impervious to facts. Therefore, it cannot be easily resolved. The active leverage of disinformation campaigns in this way can be characterized as the "weaponization" of narratives.

For these reasons, facts themselves are not sufficient to combat disinformation. According to Ajit Maan, narrative warfare is a more powerful concept than information warfare alone, because it represents a battle over the meaning of information. In narrative warfare, our own ideas and narratives can be weaponized against us. An illustrative example is the way Islamic extremists have subverted the "war on terror" into a "war on Islam," which draws upon the fundamental identity of their target audience and resonates with an existing sense of oppression and aggression by Western forces.[19] When this occurs— when the concept

19 Ajit Maan, "Narrative Warfare," *Real Clear Defense,* February 27, 2018, https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html.

underpinning the disinformation becomes mythologized—our actions and words can automatically support and reinforce our competitors' narrative without them needing to take any action to distort them. As a result, the narratives can live on long after those behind their proliferation have stopped actively promoting it. This means that eliminating those individuals and organizations will not be sufficient to combat the narrative and may in fact help amplify it. On a lesser scale, this is also the case for censorship as those behind the narrative can use the attempt to repress the message as proof of its truth, importance, or authenticity.

Responses to weaponized narratives cannot rely on simple truth telling or countering lies. In addition to facts often being too complex, less interesting, and less meaningful to individuals, attempting to use them to counter disinformation is inherently reactive. In this information environment and under the asymmetric incentive structures of today's media environment, lies can be told too often and too easily for responders to "catch up," let alone counter. Even if the speed and volume of lies could be matched effectively, the responses would be less meaningful. Even then, the "truth teller" would be giving credibility to the source of the disinformation and would appear less authoritative. While an important tool, even counter-narratives are inherently reactive and cede ground to the false narrators.

The only answer to these weaponized narratives, therefore, is an embrace of the competition of ideas and confidence in the generation of our own narratives. The most powerful story is not necessarily the one that holds the most truth, but the one that holds the most meaning. There is no doubt that the most meaningful narratives are those that retain authenticity and credibility, so truth and facts must be central to our development of effective narratives. However, truth and facts are not sufficient to ensure effectiveness. Moreover, what is meaningful for one population may hold little meaning for another. Irregular groups such as ISIS have been effective in part because of their ability to micro-target specific demographics with tailored messages. States seeking to combat disinformation and harmful narratives must be equally attuned and agile if their narratives are to prevail.

This is something that the West used to be very good at. During the Cold War, the United States and its allies used their values as free, open, and prosperous nations to become an aspirational ideal to many countries under repressive rule. The soft power that the United States generated through engagement, culture, and values was extremely powerful. It still is today—so much so that even North Korea wants to establish a McDonalds in its capital Pyongyang. But we need to have confidence in our advantages and the truth of our own perspectives. Effectively combating disinformation campaigns and hostile narratives will not be easy. It will require a narrative strategy that understands the importance of meaning and identity to a wide spectrum of possible audiences. To connect with that audience effectively requires understanding them better than they understand themselves. But in this we may see the real challenge for countries seeking to combat hostile narratives.

As the world undergoes the disruption of technological change, as well as the subsequent inundation of information and polarization of political perspectives, the central challenge for many Western countries is that their societies have fractured. The subsequent loss in trust and vulnerability to hostile disinformation campaigns has already been explored. But it may also highlight the greatest challenge to winning the narrative competition: the manifestation of culture wars, evident in elections around the world, suggests that societies are struggling to understand themselves, let alone foreign audiences. If political entities that are organic to a society are unable to understand or message to itself, it is unlikely they will be able to do so effectively to others. Moreover, it reflects a broader lack of confidence in the identity and values of that society. It is hard to forge an authentic narrative that reflects the best aspects of a society or community when those within it have incompatible understandings of what that narrative is and whether it is correct.

The environment has changed and is unlikely to shift back, and hand-wringing does nothing to remedy the situation. If the current environment is indeed the result of societal shifts to which we have not yet adapted, then it is likely that over time natural responses and adaptions will form. Resilient societies contain self-correcting forces, and many anthropological and historical studies can illustrate how new cultures adapt and new norms form. But this process can be accelerated and shaped through a range of responses at all levels. Markets will, and have already begun, to adjust the incentive structures for how content producers are rewarded. This will impact the decision on the investment that content producers make in the quality of their information. But that should not stop the wider population from continuing to pressure content producers to do so quickly by being more judicious in what each individual engages with and how they support media organizations. Many of the responses and adaptions mentioned below are already underway, whether they be elected officials holding social media companies to account or individuals buying subscriptions to respectable media companies.

However, by being clear about what responses are available, and the importance they have within the broader context, society can more quickly contain and correct the damage from disinformation.

An effective response requires a holistic strategy that can be broadly separated into four facets: the *message*, the *messenger*, the *market*, and the *mode*. This strategy requires responding to active threats, but also to cultural and technological shifts. In some cases, a particular response does not need to be lengthy, complicated, or sophisticated. Ridiculing a false narrative or piece of disinformation may resonate with audiences and be sufficient to counter it so long as that response aligns with a broader narrative that holds meaning for the audience. An effective response will come from the cumulative actions—both big and small – by a variety of actors across the full spectrum of society. Disinformation has society wide impacts, and no single actor can—or should—be solely responsible for countering it.

The *message* must be centered on a carefully crafted narrative. Some of this must come organically through society rediscovering its identity and confidence—something that can be encouraged but not forced. Societies are at their most appealing when they have a clear understanding of who they are and what they stand for, as well as when they exude a confidence in the strength of that identity. This confidence is at the heart of soft power and is unmistakable among those countries with strong cultural appeal. For countries riven by cultural rifts, generating a strong message will require leadership across all levels of society.

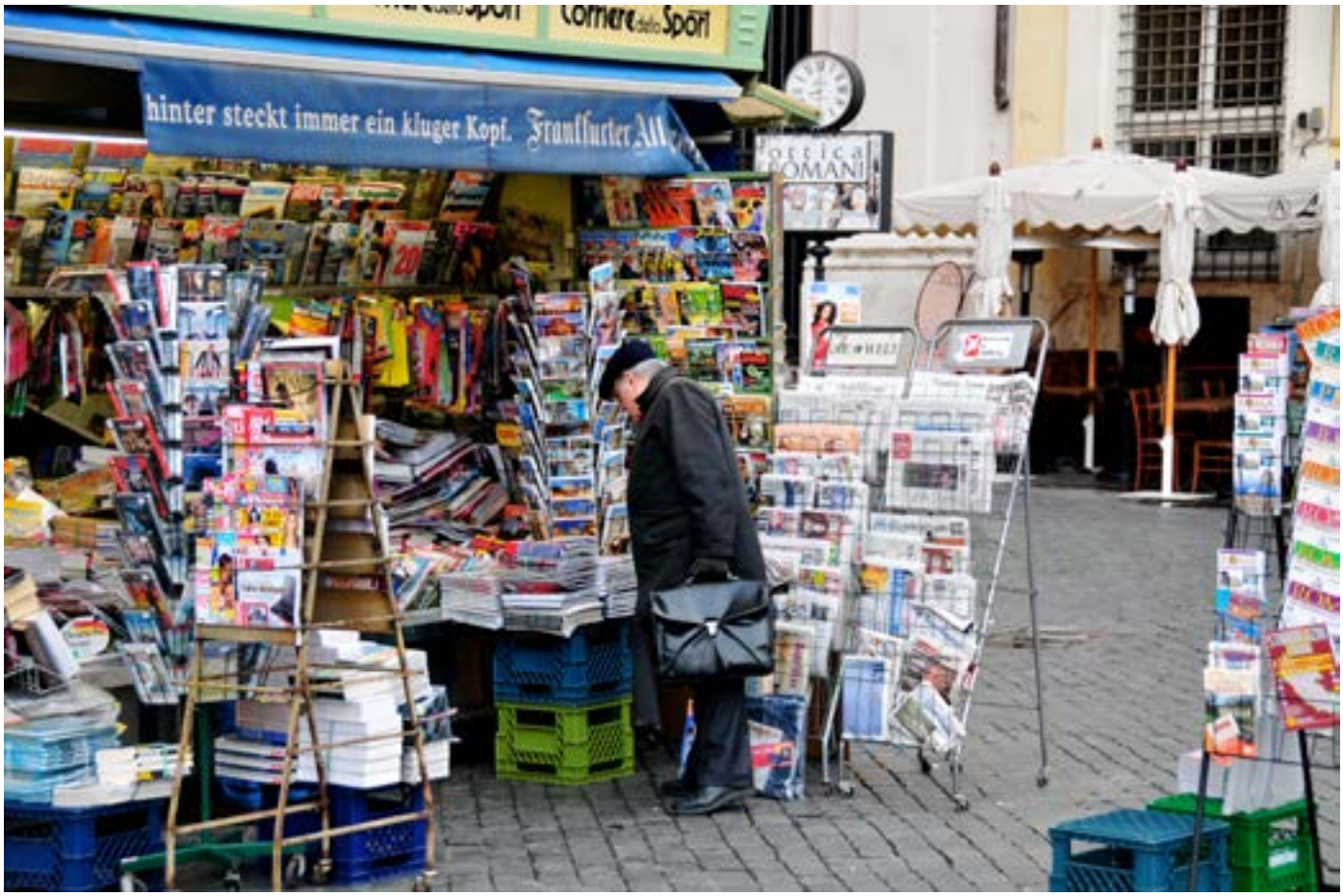
The message itself must be consistent across society, but there must also be tailored measures which target specific local circumstances and communities. Thought must also be given to the longer-term implications and potential consequences. It is important to understand how each community will receive a particular message—what seems ridiculous to one group may appear logically self-evident to another. The same idea or narrative may need to be repackaged for different audiences in order to have the same effect or communicate the same meaning.

Most importantly, the message must model the values we seek to reinvigorate. This includes being fact-based, honest in the inherent bias of any particular piece of content, and aware that there are alternate perspectives. Studies such as the Edelman Trust Barometer referenced earlier show an awareness and concern over the authenticity of information amongst the general population and a latent appetite for truth. This means that the challenges we currently face are not intractable and that developing ways to counteract disinformation will be welcome by the majority of the population.

The *messenger* is also critical, as the credibility of the narrator is essential to the success of the narrative. It must come from all levels and be both authentic and credible. The same psychological biases that empower the spread of disinformation should be leveraged to make the corrective message more likely to resonate. For instance, since people are more likely to believe information shared by an acquaintance, a correction of disinformation must be shared by the communities targeted by disinformation. Similarly, just as individuals can inadvertently absorb disinformation when inundated by it, so too their perspective can be balanced by constant exposure to corrective, fact-based information. Therefore, at-risk communities must be empowered and supported in responding to falsehoods. Outside commentators will never have the same meaning or authenticity as those native to a community, particularly when the outside commentators are from a different social, cultural, political, or religious group. In Singapore, for instance, communities at risk of Islamic radicalization were empowered to lead the response to those who subverted religious teaching to meet their own extremist agenda. The importance of the messenger applies on multiple levels, from government through institutions to the community and the individual, and must represent collective action by a community seeking a better quality of information.

The *market* in this context is meant broadly, referring to the structural and systemic aspects of the marketplace of ideas that limit the asymmetric advantages of disinformation. In some ways this is literal: the economic incentives of how the new media and information environment operates need to mature, with regulators, advertisers, and audience putting pressure on the content producers and broadcasters to better filter the quality and character of the information they provide. Gatekeepers need to again become professionalized and held to account, even if that is in a different form than what they were previously. This does not need to be government driven—indeed it is better if it is not. That is not to say that regulation of this environment should not continue to evolve, just that the market can drive most of these changes and incentivize the investment in quality controls. For that to happen, however, there needs to be a collective demand for it. This requires awareness and intent by the broader community and a demand for action at all levels.

In another sense, this market is conceptual: the market place of ideas has become more competitive and we




Newspaper stand in Rome, 2008 *Photo Credit:* Ed Yourdon (*https://www.flickr.com/photos/yourdon/3076622657*)

need to understand that reality and adapt accordingly. Society is slowly waking up to the scale and scope of the threat that disinformation poses and all the ways it can be applied. This awakening should be supported and facilitated by journalists, academia, and national governments by illuminating the actions and connections between threat actors and how they seek to achieve their goals. Organizations such as the Atlantic Council's Digital Forensics Research Laboratory pursue this goal through educating the public on current disinformation activities and methods used. Governments have in the past tipped off journalists to attempts by foreign actors to inject fabricated news stories into the media environment. Meanwhile, investigative journalists are uncovering the linkages and networks of actors, such as Wikileaks founder Julian Assange's link to the Kremlin. The global community—both national governments and their societies—need to mature the cultural norms and international norms surrounding disinformation. Individuals need to push back against acquaintances who spread disinformation on social networks, while governments need to create consequences for such activities that limits and mitigates their ill effects, as has happened with other sovereignty breaching actions such as state espionage. Most critically of all, nations and communities need to hone their narrative responses and compete aggressively within the marketplace of ideas to ensure they provide a more compelling narrative founded on fact and truth.

Beyond the narrative battle and credibility of the narrator, the *mode* is equally important because of the unique properties of the technological platforms involved. Social media sites are uniquely different from previous commercial communication platforms because the architecture on which social media platforms are built is incentivized, and in turn incentivizes other actors, to act in certain ways. Social media algorithms determine what people see and do not see, and have now been directly linked to ethnic violence in several regions around the world. Social media has acted in its own best interests with little regard for the implications to the broader public. The platforms must recognize this and reform themselves. Indeed, this is already underway, with most major social media and information focused technology giants, including Facebook,

Google, YouTube, and Twitter, launching campaigns to purge fake accounts, verify information sources and limit the spread of misleading content.

Governments must grasp the importance of these issues and the risks to the general public. They must act to protect their people by reshaping the incentives and consequences for how messengers act. And the general public needs to hold both to account, thinking more critically about the role these platforms play in society. More generally, there may need to be a conceptual rethink around personal data and privacy where the business model of social media companies is reversed to provide individuals with both more control and financial compensation for the way the companies utilize their information. Individuals auctioning their data to social media platforms, for instance, would radically change the business models and incentives of those companies, and therefore the way they operate.[20] Perhaps this represents an inevitable maturation of a new and disruptive cultural and technological development, but regardless it is a discussion that needs to occur quickly and subsequently lead to direct action. These platforms are now a permanent reality and society will need to evolve its norms, etiquette, and laws to ensure such platforms are beneficial to society rather than harmful.

## Whose Responsibility?

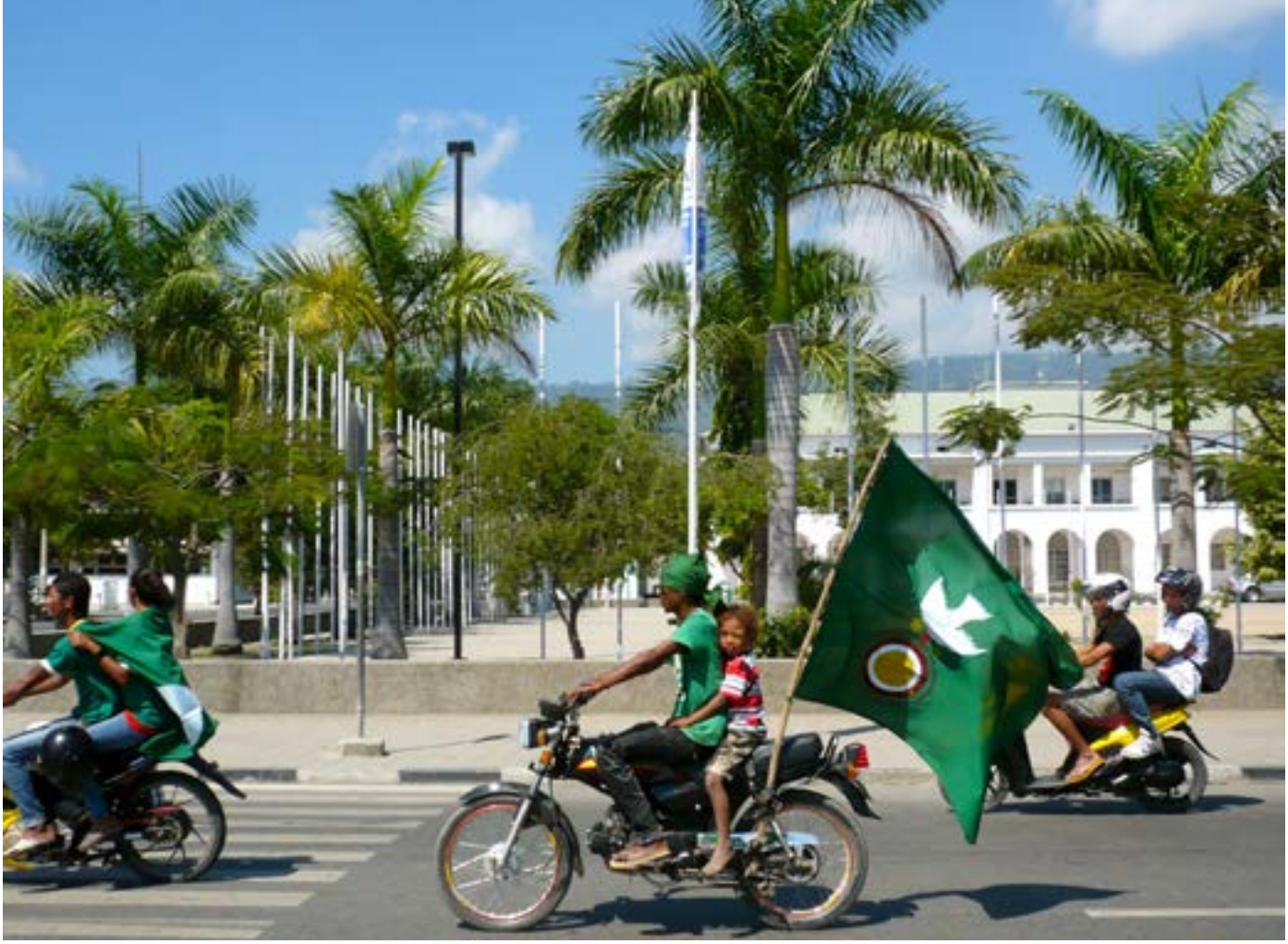
The complexity, ubiquity, and nuance of the challenge posed by disinformation requires collective action by actors at all levels. No one group can effectively resolve the challenge, and the response will be gradual and iterative. Many of the elements of an effective response to disinformation have been covered above, and the green shoots of this response are already evident. But there are limits to the role each group can play, and it is important for all levels of society to understand how their actions contribute to the renewal of a fact-based information environment, as well as the societal trust that underpins national sovereignty. Moreover, no one actor can be expected to act in a completely unbiased and incorruptible manner. One group gaining too much leverage over the response could prove counter-productive, or even exacerbate the problem.

The difficulty of the task should not be underestimated. Many of the speakers at the Sovereign Challenge conference pointed to a latent desire within the general population for fact and truth in the information environment, while also asserting that "trust is gained in drips and lost in buckets." Adapting to the current disruption, maturing of cultural norms, and modernizing the governance of the new environment will be a long and- slow process, which will undoubtedly suffer numerous setbacks. Nonetheless, a maintenance of the long-term objectives and smart responses by those who appreciate the significance of the issues will accelerate society's rebound from the current disruption. As each facet of society has a specific role and responsibility in responding to disinformation, it is worth considering each in turn.

Government plays a critical but limited role in an effective response. For all the reasons above, government responses must be restrained and judicious lest they undermine the nongovernmental elements that are more important to a healthy, free, and open exchange of ideas in democratic societies. This exchange, and its nongovernmental components, are necessary to properly counter disinformation. New and emerging technologies and businesses must be regulated and held accountable by elected officials, particularly where they impact public interests. This is no different from the regulation of pollution, fair business practices, or safety regulations for personal transport. But this regulation should take the form of guidelines, best practice, and informing the public rather than direct control. A longer debate is necessary regarding privacy and the corporate use of personal information, and laws will need to be updated to reflect the challenges of our time. Governments can also play a proactive role in supporting the other elements of society by being transparent and open when they detect disinformation-linked activity, particularly that driven by adversary-states looking to sow discord or extremist groups acting to cause harm to society. They also have an active role to play in countering extremist narratives and information operations overseas. But even in both these cases, they are imperfect messengers who would be better supporting other actors' efforts. Their most important role is in regulating and holding accountable the markets and modes of the information environment.

Business and the private sector may not naturally understand the role they play in combating disinformation, but theirs is one of the most important. They are not only the driver of the markets and the modes, but also key messengers and message generators. In the West at least, they have been thrust into a central role due to the general public's increased trust in them as institutions. This may be temporary, but they should take this responsibility seriously. After all, they rely on the

20 "Should internet firms pay for the data users currently give away?," *Economist*, January 11, 2018 https://www.economist.com/news/finance-and-economics/21734390-and-new-paper-proposes-should-data-providers-unionise-should-internet.



Supporters of KHUNTO Party campaigning on motorcycles during the 2012 parliamentary elections in Dili, Timor Leste, 2012 *Photo Credit:* Janina M Pawelz, Wikimedia Commons (*https://commons.wikimedia.org/wiki/File:KHUNTO_Campaign_Dili_2012.jpg*)

rule of law and effectiveness of governance that underpin national sovereignty as much as any other societal actor. In a less abstract and directly relevant way, ethical business is a best practice that is important to modern consumers. Just as "sustainable," "eco-friendly," "ethically sourced," or "American made" are key marketing messages, "fact-based" content generation and broadcast should be a central business practice. Several large tech companies are already moving to align with these principles and experimenting with ways to highlight the source of information. A useful first step is to affix information to online content about who owns or funds the creator of that information, in a similar way that food products carry nutritional information. Additional nutritional information on food items does not prevent someone buying an unhealthy food option, but they can at least understand what it is they are purchasing. In the same way, people would be free to read any content they like, but would have a better understanding of its inherent bias and overall reliability.

The technology industry, and particularly those who control prominent social media platforms, needs to reform itself in a number of ways. As society shifts its expectations about these platforms and companies, the platforms should seek to get ahead of the trend by exploring alternate ways to generate income and modifying their business models, thereby shifting the way they treat personal data before government regulators and consumers demand it of them. They have a critical and immediate role to play not only in preventing the dissemination of disinformation and labelling of the content already being broadcast across their platforms, but in actively countering extremist groups that use their platforms to harass targets, recruit like-minded agitators, and stir up ethnic and religious divisions that have been used to instigate violence around the globe. In such cases, they need to actively cooperate with governments to identify threat actors that pose tangible risks to the safety and security of segments of the population. But while social media platforms hold significant risks to societies, they also provide significant opportunities for civic engagement as well. Some parts of the developing world have extremely high internet penetration, and even where there is significant media repression, civil society can flourish in an online environment.

Nongovernmental organizations and civil society have perhaps the most important role to play. As the manifestation of the collective interests and values of a

community, they can simultaneously be the message generator, the messenger, and the marketplace in and of themselves. At the top of this spectrum, think tanks, research institutions, and academia have a critical role in understanding the nature of the challenges, developing specific responses, and educating the general public. At the other end of the spectrum, grass roots organizations can pressure governments and businesses to act, thereby mobilizing the public to lobby for change. As was discussed in relation to the rise of extremist groups, NGOs also represent a first and most appropriate response to threat actors seeking to subvert communities toward misguided causes. As with all levels, they can equally be the cause of disinformation as much as a remedy or bulwark against it. There are numerous "civil society" groups, which are the source and advocates of the disinformation campaigns and attempts to undermine trust in institutions that this paper seeks to combat. For example, fact checking of media reporting was repeatedly discussed as an important check and balance on misinformation, one that would be inappropriate for government or business to undertake. When run by objective and well-intentioned gatekeepers, fact checking services can play a vital role. But such activities undertaken by a biased and unaccountable civil actor could be more harmful than not having one at all. Wikileaks, for instance, operates with the perceived credibility of being an objective agent of global transparency, and yet Wikileaks also has been highly selective in the way it uses information for its own agendas while also maintaining links to the Kremlin.

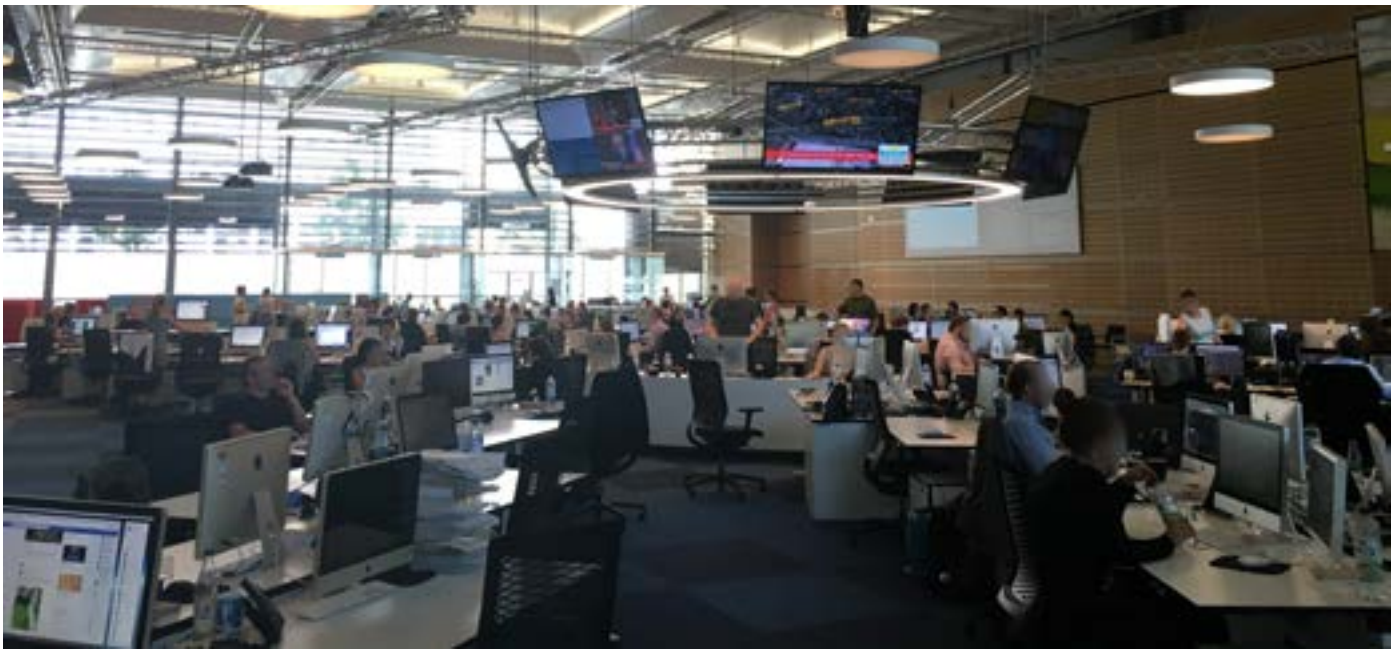
As the key generators of both the message and as the primary messengers, media organizations are still central actors in the response to disinformation. In this sense we must distinguish between the dwindling number of professional media actors (e.g., journalists and editors) and the informal and unaccountable "content generators" who are often conflated with them. While they are facing a deeply disrupted, fractured, and challenging industry, media professionals arguably play a more important role than they ever have before. As the number of professional "gate-keepers" has been eroded, those who remain are more vital than ever. This is not to suggest that all journalists, editors, or media executives are innocent in the dissemination of disinformation or the murkiness or the current information environment. Rather, the industry needs continued reform and improvement. Greater guidelines and best practice are needed to increase transparency about bias. Distinguishing between objective reporting, opinion, and paid-for content would go a long way toward restoring trust in the media as an institution.

But there is an inherent accountability in the diversity of opinion, and the importance of a free and independent press was a recurring and emphatic theme throughout the conference. It should also be noted that amongst the general public, in the United States at least, the majority (58 percent) favors information freedoms over government attempts to limit disinformation. In the same vein, a majority (56 percent) currently favors a tech company-led response to disinformation. Since government will necessarily still have a role to play, this reinforces the importance of collective action across sectors and industries.[21] Just as attempts to limit media spreading disinformation is likely to do more harm than good, as is the case with the attempt to co-opt well-intentioned journalists. Their value stems from truly independent and objective reporting. Any attempt to influence them will undermine their credibility, further erode trust, and reinforce the narrative of disinformation campaigners that no one can be trusted. While governments can alert the media to issues of which they may not otherwise be aware, journalists and other media professionals must remain objective messengers of truth, not of the counter-narrative itself.

On the other hand, media producers need to recognize that adversaries are out there and actively seeking to cause harm through their medium. They have a responsibility to respond to threats and raise awareness of the incidents occurring, both because it is their business to do so and because of a larger duty of care. In doing so, they need to be careful not to "carry the virus," as one speaker put it. This means they should consider disabling commentary systems—the function of allowing the general public to leave comments beneath a particular media item—and be careful to refer to the spreading of false information and providing a fact-based correction without explicitly repeating the false message itself.

Finally, there are responsibilities that each individual must accept and act on. This starts with a critical curiosity and an awareness of the changed information environment. Each individual needs to educate himself/herself on how the environment has changed, as well as understanding how to apply critical analysis to the information he/she consumes in order to better filter the quality. Biases will remain, and individuals have a

21 Amy Mitchell, Elizabeth Grieco, and Nami Sumida, "Americans Favor Protecting Information Freedoms Over Government Steps to Restrict False News Online," Pew Research Center, April 19, 2018, http://www.journalism.org/2018/04/19/americans-favor-protecting-information-freedoms-over-government-steps-to-restrict-false-news-online/.



WELT Newsroom at the Axel Springer house in Berlin, 2016 *Photo Credit:* ASUKomm, Wikimedia (*https://commons.wikimedia.org/wiki/File:WELT_Newsroom.jpg*)

right to their opinion. But if they desire a better quality of politics and society, then they need to have an awareness of the information bubble in which they live. They must also seek to balance their perspective by exposing themselves to views that they may not fully understand or agree with. Improved education in schools and colleges will help in the long-run—and again there are already experiments underway in this field—but an immediate response is for individual citizens to collectively demand more from the content generators and broadcast platforms and to work toward building a society resilient to disinformation through increased education. Individuals also need to understand that they are now their own media entity: what stories and information they project over social media, either from personal experience or sharing news they have read, have a tangible impact that contributes to the broader information environment. It is a responsibility all need to understand and embrace. If this can lead to the reestablishment of some degree of shared facts, then serious policy debate can resume, and trust will slowly be rebuilt.

## CONCLUSION

The information environment has changed, and the realities of the new environment will persist for the foreseeable future. The convergence of cultural, geopolitical, and technological trends has created new threats and risks to all levels of society. Disinformation is an unfortunate and ubiquitous facet of the new information environment, and one that has been leveraged by extremists, ideologues, and geopolitical rivals to achieve their strategic goals. Left unchecked, disinformation has the potential to corrupt societies perspectives and beliefs, eroding trust and thereby the institutions that underpin a nation's sovereignty. But that battle is not over. The same trends that have created the current disruption also contain self-corrective forces, and natural adaption and evolution will occur to temper some of the negative effects of the new information environment.

The first elements of this process are already evident as individuals, societies, and markets begin to understand the magnitude of the risks and respond to them. But we should not be complacent or apathetic about our response. There are a range of actions that can be taken by actors at all levels to respond to disinformation. The task now is to understand the roles and responsibilities of institutional and societal group, and incubate an effective response. Trust is hard to gain and easily lost. The information environment has been polluted and mutated, both by organic cultural and technological trends and by threat actors seeking to exploit them for their own ends. Both must be addressed in respective and appropriate ways. It will take time and dedicated collective action to respond to the risks and threats posed by disinformation. It will take a coordinated response to repair the message, messenger, market, and mode of information by all levels of a society. But if successful, the threats of disinformation can be mitigated and the foundations of a rebuilding of trust can begin to safeguard the sovereignty of all nations.

# ABOUT THE AUTHOR

**John T. Watts** is a Nonresident Senior Fellow at the Atlantic Council's Scowcroft Center for Strategy and Security.

Watts has spent more than a decade and a half working across military, government, and industry, focused predominantly on the nature of future warfare and implications of complex emerging security risks. At the Atlantic Council, he has created the Emergent Futures Lab to develop new insights into future threats by combining experimental approaches and non-traditional perspectives with established expertise. He also focuses on Indo-Pacific security issues.

Previously, as a senior consultant with a Washington-based consulting company, he advised international, military, federal, and local government agencies. Through this work, he improved strategic planning and technology evaluation approaches, exercised emergency management teams, facilitated non-traditional interagency initiatives, developed new operating concepts, and analyzed the impact and opportunities of emerging, disruptive technologies and threats.

Prior to moving to the United States, he was a staff officer at the Australian Department of Defence, working in a variety of strategic planning, implementation, evaluation, and management roles. His primary focus was organizational capacity building as well as the development and implementation of strategic guidance and military preparedness. Watts also spent more than a dozen years in the Australian Army Reserves, where he held command, training, officer development, and emergency management positions. His most recent position was as a liaison officer with the Virginia National Guard.

Watts holds an Honours of Arts (International Studies) from the University of Adelaide, Australia, and a Masters of International Law from the Australian National University.

# Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org