



WORLD LEADERSHIP ALLIANCE  
CLUB DE MADRID

# Protecting Information Integrity

## National and International Policy Options

Report of the Roundtable on Global Governance  
for Information Integrity held in Riga (Latvia) on  
27 September 2018

November 2018

Co-organized with



Ministry of  
Foreign Affairs  
Republic of Latvia

Latvia 100

# CONTENTS

INTRODUCTION	3
INFORMATION INTEGRITY: A DEFINITION	4
POLICY APPROACHES FOR INFORMATION INTEGRITY PROTECTION	5
1.Develop a Bill of Digital Rights	6
2.Legislate the Digital Environment - Not Content	6
3.Encourage Voluntary Action	8
4.Support the Publication of Reliable Information	8
5.Educate Citizens	9
LOCUS OF POLICY-MAKING FOR INFORMATION INTEGRITY PROTECTION	11
Limits of the Nation State	11
International Cooperation for Societal Resilience	12
International Cooperation for Information Integrity Protection	12
WAY FORWARD	13
ABOUT THIS REPORT	14

# INTRODUCTION

Citizen access to information is a fundamental pillar of democratic societies. The exercise of political rights – from electing leaders to expressing policy views – requires citizens to have access to reliable, balanced and complete information on current affairs, government action and political actors. The World Leadership Alliance – Club de Madrid’s (WLA-CdM) [\*Next Generation Democracy project \(2014-2018\)\*](#) identified the flow of information through new technologies and social media as one of the main drivers of democracy around the world in the next decade. Spurred by controversies surrounding the allegedly malevolent circulation of fake news on social media in sensitive political moments in the US, the UK and Spain, among others, leading global institutions, both public and private, are rushing to set up new structures to understand and respond to the complex relationship between information integrity, online communication platforms and political processes. The UN High-Level Panel on Digital Cooperation, the EU’s High-Level Expert Group on Fake News and Online Disinformation, and the Kofi Annan Commission on Elections and Democracy in the Digital Age, are just a few examples of the wave of attention the topic is receiving on the global stage.

New information and communication technologies, particularly social media, open new channels of citizen participation and engagement in elections and governance. They allow for direct interaction between political leaders and citizens, create a space for the expression of political ideas that might otherwise not find their way in the political debate, and make it easy for citizens to engage in nation-wide political conversations. In countries where traditional media cannot veer free from government restraint, social media provide an alternative outlet for free speech and



– as the Arab revolutions of 2010-2012 taught us – become a powerful tool for democratic reform. They can facilitate citizen access to information from State institutions, increasing government transparency and making it easier for citizens to keep political leaders accountable. They also offer new online solutions for the provision of public services, allowing the State to better serve citizens.

But new information and communication technologies, and social media in particular, also bring about new challenges. Online anonymousness, zero-cost publishing and zero-cost retransmission favor the propagation of political messages, including fake news, hate speech, extremist and polarizing ideas, that would meet more hurdles and receive less attention in the non-digital world. Content algorithms, whereby search engines and newsfeeds prioritize content related to the user’s browsing history, have created echo chambers that push online citizens away from multi-faceted analysis into ideological one-sidedness. The use of personal data and browsing history to target advertising has further encouraged polarizing trends by allowing the promoters of disruptive political ideas to easily identify the audience most likely to take action on their behalf – including, in some cases, by using personal data shared by online platforms unbeknownst to their users.

---

**“Truth decay is the  
derivative function of  
information integrity”**

*Stijn Hoorens, Associate Director,  
RAND Europe, 27 September 2018*

# INFORMATION INTEGRITY A DEFINITION

The academic community, akin to the policy-making community, has redoubled the attention it pays to the relationship between digital technologies and political processes. Research in the fields of communications, political science, sociology and even neuroscience has started providing insight into how political information circulates online, how citizens respond to it, and how it affects political and social dynamics.

Yet, the terminology surrounding these phenomena remains blurry. The term *fake news* is widely used in reference to the online circulation of false or manipulated statements presented as information, but many experts prefer to use other terms – such as *disinformation*, *misinformation* and *information manipulation* – to distinguish between intentional and non-intentional actions, malevolent and non-malevolent purposes, complete falsehoods and manipulated statements. While efforts are being made to formalize the terminology surrounding fake news, much less attention is being paid to coining a general term to refer to the broader array of phenomena that affect the information that reaches citizens through online platforms and social media. There is no consensual term to refer to fake news, content algorithms, echo chambers and micro-targeted advertizing all at once.

Drawing on the terminology employed in Stanford University's [Project on Democracy and the Internet](#) and the Institute for

Statecraft's [Integrity Initiative](#), the WLA-CdM has settled for using the term *threats to information integrity*, where we define information integrity as the trustworthiness, balance and completeness of information to which citizens have access on current affairs, government actions, political actors and other elements relevant to their political perceptions and decision-making. Threats to information integrity include all processes that skew the relationship between the whole factual truth and the information that citizens receive through social media and online platforms. The term, therefore, goes beyond intentional actions to also include the deterioration of information integrity that come as a collateral effect of business practices, social dynamics and the transformation of journalism in the digital environment.

Threats to information integrity are not new. Propaganda has existed for decades and influenced political perceptions in many sensitive moments of history. What is new is the scope and reach of the threats to information integrity in the digital environment. Big data opens the possibility to leverage more user information than ever before to influence political perceptions through highly targeted messaging; preference-based content algorithms are reducing interactions across ideological groups beyond the natural segregation that affects social interactions outside the digital environment; and, for the first time in history, the circulation of factually incorrect information is accompanied by widespread disagreement over basic facts.

---

**Information integrity refers to the trustworthiness, balance and completeness of information**

# POLICY APPROACHES FOR INFORMATION INTEGRITY PROTECTION

Protecting the integrity of the political information that reaches citizens through social media and online platforms seems like a desirable objective for any democracy. According to the Reuters Institute's [Digital News Report 2018](#), public demand for government intervention to protect information integrity is high, particularly in Europe and Asia.

Nevertheless, the practical implications of information integrity protection make the choice of a policy approach delicate. Can freedom of speech – a fundamental right enshrined in international law – be curtailed in the interest of information integrity? If information integrity protection aims to give citizens access to truth, who is to be the arbiter of truth? And who should be liable to change their behavior in the interest of information integrity: online platforms or individuals?

These questions were the focus of the **Roundtable on Global Governance for Information Integrity** organized in Riga (Latvia) on 27 September 2018 by the WLA-CdM and the Ministry of Foreign Affairs of the Republic of Latvia, bringing together Latvian

and international experts, policy-makers and civil society representatives in policy discussions informed by the interventions of five democratic former Heads of State and Government from Austria, Latvia, Mongolia and Tunisia.

The number of countries who have developed or are developing legislation to protect information integrity – including France, Germany, the UK and up to ten others, according to a [March 2018 report](#) by the S. Rajaratnam School of International Studies – brought particular attention to the role of legislation, versus other approaches, as a tool for information integrity protection. While there was a diversity of views among participants, a broad consensus emerged around the complementarity of different policy approaches and the imperative to combine them wisely to ensure that information integrity protection enhances, rather than restricts, democratic rights.

The following sections present five policy options that were identified throughout the Roundtable as particularly recommendable for policy makers.

*Roundtable on Global Governance for Information Integrity,  
Riga (Latvia), 27 September 2018*





# 1. DEVELOP A BILL OF DIGITAL RIGHTS

The impetus to protect information integrity in democratic societies responds to the threat that its deterioration is posing to essential elements of the democratic system, such as electoral processes, informed political debate and vibrant professional journalism. While different actors have different views on the policy measures needed to protect information integrity, all start from a common desire to protect democratic rights. How do democratic rights, such as those enshrined in the *International Covenant on Civil and Political Rights*, apply to the digital environment? Agreement on this fundamental question, participants at the Roundtable suggested, is a necessary step to ensure that policy measures taken to protect information integrity further democratic rights, rather than restrict them.

While there is general agreement that civic and political rights do apply to the digital environment, the concrete, practical implications of these rights remain unclear. Does the right to “seek, receive and impart information and ideas of all kinds” (Article 19) translate into an obligation for content algorithms to show users content that reflects ideas of all kinds? Is the right for protection against “unlawful attacks on honour and reputation” (Article 17) incompatible with the viral circulation of false information about individuals? What conditions must fake news meet to be considered an unlawful attack? Other rights enshrined in international law also raise questions in relation to the digital environment. Does the right to education (Article 26 of the *Universal Declaration of Human Rights*) include a right to digital literacy? If threats to information integrity are

becoming an instrument for hybrid warfare, is there a need for a Geneva Convention for cyberspace?

While these are complex questions, participants to the Roundtable underscored that reaching an agreement on these principles would be both easier than and a precondition to building consensus on policy measures for information integrity protection.

## 2. LEGISLATE THE DIGITAL ENVIRONMENT - NOT CONTENT

The practice of using legislation to protect the integrity of information in the public space is not new. The French law on freedom of press of 1881 has been prohibiting the publication, diffusion or reproduction of false news for over 130 years. Laws against defamation have also existed for decades and provide precedent in the area of curtailing one's free speech to protect the reputation of others. Broadcasting and publishing laws also define the terms on which information can be put out in the public space in traditional media. It is no surprise, then, that political leaders have been turning to legislation to protect information integrity in the new digital environment.

Germany, for example, approved in June 2017 the [Network Enforcement Act \(NetzDG\)](#), whereby large online platforms have 24 hours to remove unlawful content, as per the Criminal Code, lest they may face fines of up to 50 million EUR. In France, a [law on information manipulation](#) approved by the National

Assembly in July 2018 seeks to oblige social media platforms to name advertisers who are financing content and allow for an expedient judicial review – and eventually removal – of potentially manipulative information during electoral periods. In the UK, the [Interim Report](#) of the House of Commons' investigation on fake news clearly states that “in this rapidly changing digital world, our existing legal framework is no longer fit for purpose”.

The industry's reaction to these legislative initiatives has been less than welcoming, and some media outlets have started documenting how the new laws are – or could be – unduly curtailing their freedom of speech. The UN Special Rapporteur on Freedom of Opinion, David Kaye, also raised concerns that the German and French laws, respectively, place upon private companies the responsibility to regulate the exercise of freedom of expression without judicial oversight, and allow for censorship based on criteria that are vague, ambiguous and/or incompatible with international law.

Participants to the Roundtable loudly echoed these concerns, insisting on the primary importance of freedom of speech in democratic societies and the dangers of giving any single actor, whether public or private, a legal monopoly on truth. The general reticence to online content legislation contrasted, however, with a general appetite for a greater regulation of the online environment. Various measures were put forward as desirable to increase accountability and trust in the digital environment – measures such as increasing the transparency of content algorithms, reducing anonymousness in online posting and advertizing, and streamlining public oversight over the digital environment – and their enactment would require legislative or regulatory change.

The legislation needed to bring about these

changes in the online environment will depend on each country's current legal framework. The following legislative measures were discussed during the Roundtable in relation to specific countries, but they may provide useful guidelines for an analysis of recommendable legislation to protect information integrity in other countries as well:

- Amend **publishing law** to include social media platforms, thereby applying to social media platforms the same rules that already apply to publishers in terms of duty of care, advertizing and the sharing of anonymous content;
- Enact new **legislation to increase online transparency**, making it mandatory for social media platforms and online news outlets to inform users about content algorithms;
- Amend **other existing laws**, such as electoral law, competition law and laws on advertizing, to explicitly apply to the digital environment the same rules that currently apply outside of it;
- Create a **regulatory agency** for the digital environment and adjust the institutional mandates and structures of other public agencies, such as public broadcasters and electoral commissions, to reflect their necessary role in information integrity protection.

### 3. ENCOURAGE VOLUNTARY ACTION

As an alternative to legislation, Roundtable participants considered the option of encouraging online platforms and social media companies to take voluntary action to meet the objectives of increased transparency, reduced anonymousness and easier access to information presenting alternative viewpoints. The European Commission's [Code of Practice on Disinformation](#), finalized in September 2018, provides an example of such a voluntary action scheme.

While many Roundtable participants applauded the flexibility of voluntary action measures, which they saw as less threatening of democratic rights than online content legislation, others expressed doubt as to their efficacy, underscoring that online platforms and social media companies are profit-driven entities whose business model leaves democratic interests to the side. "Move fast and break things" was, as one participant reminded us, Facebook's motto. The potential for these companies' practices to change through voluntary action is, in this view, limited.

There are, however, two arguments in favor of a more optimistic prognosis for the efficacy of voluntary action. The first, underscored by a Roundtable participant, is that a distinction must be made between the newest and most disruptive online platforms and social media companies, and the more mature IT companies whose operations pose fewer threats to information integrity yet who have the possibility to contribute to the solution

through voluntary action, either by developing new digital tools – such as the NewsGuard tool that provides a detailed assessment of the reliability of news sources in a newsfeed – or through corporate social responsibility programmes.

Secondly, the EU's *Code of Conduct on Countering Illegal Online Hate Speech* provides a successful precedent for voluntary action to address online behavior. Adopted in May 2016 by the four largest online platforms in the EU, it has been reported to have led to satisfactory improvement in the four companies' processes and preparedness to address illegal online hate speech, resulting in the prompt removal of 70 percent of all illegal hate speech notified to them. Information integrity may be a more complex issue – contrarily to hate speech, not all threats to information integrity are illegal – but the EU's relative success of voluntary action to address online hate speech gives grounds for optimism regarding the willingness of online platforms and social media companies to engage to a useful extent.

### 4. SUPPORT THE PUBLICATION OF RELIABLE INFORMATION

Legislation and voluntary action schemes put on online platforms and social media companies the onus for creating an environment in which information integrity is protected. However, Roundtable participants also underscored the importance of engaging other actors, pointing to the particular role of civil society groups and journalists in developing and disseminating information



with high standards of integrity.

In the Baltic countries, who sit on the frontline of Russia-based disinformation campaigns, civil society groups – the so-called Baltic Elves - are continuously monitoring the online information environment, detecting and denouncing fake news and developing counter narratives. Similar initiatives also exist or are being considered in numerous other countries, either as permanent mechanisms, as recommended by the [July 2018 report](#) of the Expert Group on Disinformation and Fake News in Belgium, or as targeted efforts in particularly sensitive political periods such as election campaigns, as Italy did in 2018. Roundtable participants expressed broad support for the importance of these civil society initiatives to provide counter narratives, and called for public authority to provide financial and political support for their work.

The problem with fact-checking and counter-narrative, however, is that various studies point to their limited efficiency. Political beliefs have been shown to persist even when confronted with corrective information - and this persistence tends to be even stronger when the political belief holds a strong emotional importance. It follows that political views rooted in fake news and reinforced by echo chambers may be hard to counter by exposing the individual to facts, counter-narratives or alternative views post facto. While the importance of identifying fake news and providing counter narratives is undeniable, it may not be sufficient to significantly limit their impact on political processes.

This underscores the importance of ensuring that the information that reaches citizens in the first place is accurate, balanced and complete, so as to allow political beliefs to develop based on a nuanced consideration of reality. The role of journalists and news outlets

in developing, publishing and disseminating such information is crucial. The advent of social media as an alternative source of information has radically transformed the business environment for traditional news outlets, diverting away a large share of their advertizing revenues and pushing consumers' preferences towards short, attention-grabbing news items. Roundtable participants insisted on the importance of supporting investigative journalism, both financially and through capacity-building programmes, and called upon public authorities to treat information as a public good. It was pointed out that countries with strong public broadcasters are, on average, more resilient to information integrity threats, which suggests that investing in public broadcasters is a recommendable approach to protect information integrity.

While most of the Roundtable discussions focused on national policy approaches, one participant underscored the importance of local news outlets in shaping political beliefs, particularly in small, isolated rural communities. Initiatives to support investigative journalism and responsible news outlets should not disregard the local level.

## 5. EDUCATE CITIZENS

Finally, there was broad consensus among Roundtable participants around the importance of educating citizens to become responsible and discerning users of the information they receive online. The examples of Sweden and Finland, where digital literacy and critical news analysis are being integrated as part of the school curriculum, were particularly mentioned as good practices to be followed – but they are not the only ones. Civic education campaigns outside the classroom have also

been found to be useful. The Baltic Centre for Media Excellence, for example, produced short films to raise public awareness on the power of information manipulation, while the NATO Strategic Communications Centre of Excellence created a video game, hosted on Facebook, that simulates the balance sheet of a newspaper as the editor (the player) makes right or wrong decisions regarding what real or fake news to publish.

The consensus around the need for digital education and media literacy goes beyond the policy fora concerned with information integrity. Concepts of digital citizenship and digital empowerment, referring to an individual's capacity to thrive in the digital environment and make positive contributions to the social fabric through digital platforms, are also at the core of numerous civil society organizations and think tanks' actions. Most acknowledge, however, that these concepts refer to long-term processes whose effects in addressing short-term issues, like threats to information integrity, are likely to be very limited.



Inaugural Address by Vaira Vīķe-Freiberga, President of the WLA-CdM, former President of Latvia (1998-2007), Roundtable on Global Governance for Information Integrity, Riga (Latvia), 27 September 2018

# LOCUS OF POLICY-MAKING FOR INFORMATION INTEGRITY PROTECTION

## LIMITS OF THE NATION STATE

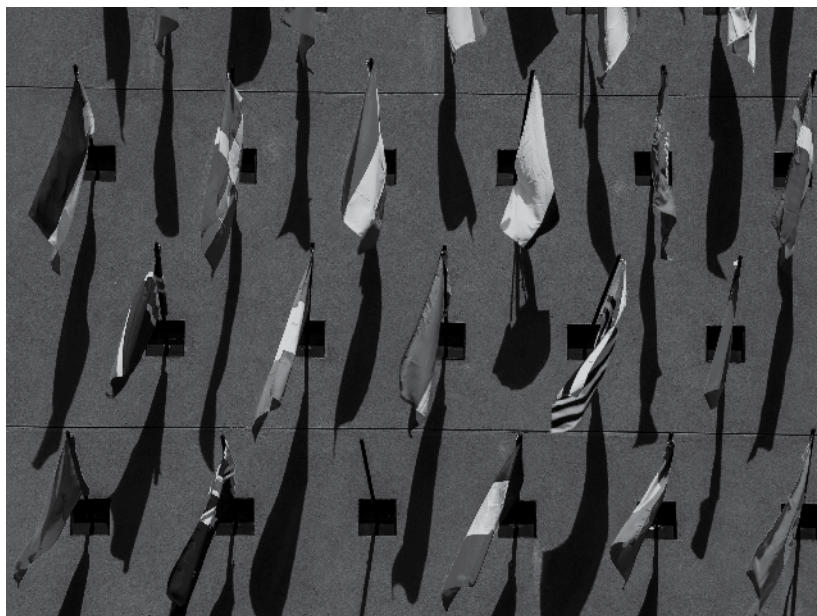
The first part of the Roundtable discussions looked at initiatives implemented or contemplated within national jurisdictions. However, online information circulates beyond national borders and threats to its integrity often have transnational dimensions – online disinformation campaigns are often listed among the tools of hybrid warfare, that is, military strategies that blend conventional warfare, cyberwarfare and other influencing methods.

The companies that host information on their social media and online platforms are also, for the most part, multinational corporations with complex webs of operations that juxtapose global corporate policies with country-specific set-ups. If national legislation forces them to change their practices in one country, they may respond by adjusting their country-specific set-ups or by modifying their global corporate policies. It follows that measures taken in one country to protect information integrity can affect the way online information circulates in other countries too.

This suggests that some degree of global coordination is desirable to ensure that measures adopted to protect information integrity adequately address transnational information flows and respond to a global

consensus on the ethics of online limitations to freedom of speech. As the final report of the EU High Level Expert Group on Fake News and Online Disinformation points out, international cooperation can also limit the extent to which information integrity protection leads to a country-based fragmentation of the internet, and help ensure that the free circulation of information on the internet is accompanied by an open market for fact-checking.

International structures for information integrity protection could provide an important safeguard against the risk that national governments or private actors like IT companies might come to have, de jure or de facto, a monopoly on truth. According to a Center for Strategic and International Studies' [brief](#) on Russian interference in the 2017 French presidential election, the legitimacy of an intervention to protect information integrity in sensitive political moments depends on the existence of an “administrative, independent and non-political authority” who can act without the perception of political partiality – something that is difficult for national institutions but may be easier for international structures.



Yet, at this time, the international community lacks permanent structures to deal with information integrity. The UN has appeared hesitant to tackle the issue directly, preferring to address it under the broader umbrella of digital cooperation, for which UN Secretary-General appointed a High-Level Panel in July 2018. Private initiatives, like the Kofi Annan Commission on Democracy and Elections in the Digital Age and the Alliance of Democracies' Transatlantic Commission on Election Integrity, have been multiplying, but their capacity to effect policy change remains to be demonstrated.

How are global actors positioning themselves on information integrity? What regional structures and communities of practice offer early examples of multi-stakeholder cooperation to protect information integrity? How are information integrity issues affecting other dimensions of international relations and foreign policy? These are the questions that were discussed in the second part of the Roundtable.

## INTERNATIONAL COOPERATION FOR SOCIETAL RESILIENCE

**T**here was broad agreement among participants that information integrity is relevant to both international security and foreign policy discussions. Hybrid warfare – defined as the use of non-military tools to achieve military objectives – has long been using disinformation as a tool, and the advent of online communications and social media has allowed this practice to grow exponentially.

The efficiency of information warfare, however, depends largely on underlying socio-economic factors that increase societies' vulnerability. Rapid disruptions in traditional ways of life brought about by globalization, economic uncertainties related to the automation of production, mounting household debt and widespread austerity policies, and a declining trust in public institutions in the face of corruption scandals and inefficiencies in service delivery, have all been mentioned as conducive to a climate of fear that allows information warfare to effectively affect political processes.

Addressing these root causes on a global scale requires diplomatic efforts, strategic public policies and foreign aid; and it can be done on a global level, through existing structures for international cooperation, such as those related to the implementation of Agenda 2030.

## INTERNATIONAL COOPERATION FOR INFORMATION INTEGRITY PROTECTION

**B**eyond increasing basic resilience in the face of information warfare, however, Roundtable participants painted a grim picture of the prospects for formal international cooperation for information integrity protection. The fundamental importance of democratic values in the information integrity debate – values such as freedom of expression and ideological pluralism – makes it difficult to bring together democratic and non-democratic countries to discuss information integrity protection. This rules out

as potential international fora for information integrity protection any organizations that include countries with little or no democratic credentials, such as the UN and the Council of Europe.

Among democratic nations, different paradigms shaping domestic and foreign policy – post-Cold War versus post-colonial approaches, multilateralism versus unilateralism – are also likely to make it difficult to find common ground on information integrity protection. Even within the EU, agreement on policy action has been hard to reach. The European Commissioner for the Security Union, supported by the Directorate General for Communications Network, Content and Technology, have taken the lead on developing policy to coordinate information integrity protection – but calls for other, dedicated European structures, including those formulated by the EU Expert Group on Fake News and Disinformation, remain to be answered. The EU's adoption of a voluntary Code of Practice on Disinformation confirms the general reluctance to legislate on sensitive issues like media regulation.

Despite these difficulties, however, Roundtable participants have identified the EU, possibly joined by a handful of other countries with strong democratic credentials, as the most promising forum for international cooperation on information integrity protection. Short of an agreement on policy action to directly tackle the threats to information integrity, there may be scope for cooperation in the informal exchange of views and good practices, particularly in areas such as citizen education for digital and media literacy, support for civil society groups and responsible journalism.

## WAY FORWARD

In summary, addressing the threats to information integrity in the digital environment is a complex task for policy makers, riddled with technical complexities and sensitive considerations related to freedom of speech, truth ownership, a disputable locus of liability and the lack of consolidated global structures and time-tested resources from which to draw.

For the WLA-CdM, the Roundtable on Global Governance for Information Integrity allowed for the identification of a number of potential approaches to information integrity protection where the counsel of our Members – democratic former Heads of State and Government from over 70 countries – could help steer policy action. Convening a global dialogue around digital rights, advising legislators on how to regulate the digital environment to protect information integrity, and advocating for the inclusion of digital and media literacy education in global, regional and national development agendas, are all options we can explore as we define our future engagement in this policy area.

An additional complication is the rapid pace of change in the digital environment. Not only must government intervention to protect information integrity respond to the threats known today, but it must also anticipate the evolving nature and type of threats likely to emerge in the near future. This underscores the importance of agile decision-making processes and makes it expedient to multiply interactions between the politically savvy and the technically knowledgeable.



# ABOUT THIS REPORT

This Report was prepared by the World Leadership Alliance-Club de Madrid based on Chatham House discussions held at the **Roundtable on Global Governance for Information Integrity** organized jointly with the Ministry of Foreign Affairs of the Republic of Latvia in Riga on 27 September 2018, on occasion of Latvia's 100th anniversary of statehood, with the collaboration of the NATO Strategic Communications Center of Excellence and the Latvian Association of Political Scientists.

Policy discussions at the Roundtable were informed by the interventions of five democratic former Heads of State and Government who, through their membership in the World Leadership Alliance-Club de Madrid, remain committed to supporting democracy that delivers.



**Vaira Vike-Freiberga**  
President of the WLA-CdM  
President of Latvia  
(1999-2007)



**Alfred Gusenbauer**  
Chancellor of Austria  
(2007-2008)



**Mehdi Jomaa**  
Prime Minister of Tunisia  
(2014-2015)



**Tsakhiagiin Elbegdorj**  
President of Mongolia  
(2009-2017)



**Valdis Birkavs**  
Prime Minister of Latvia  
(1993-1994)

The views expressed in this paper do not necessarily represent the views of individual World Leadership Alliance-Club de Madrid members, partners or Roundtable participants.



## WORLD LEADERSHIP ALLIANCE - CLUB DE MADRID

The World Leadership Alliance - Club de Madrid is the largest, worldwide assembly of political leaders working to strengthen democratic values, good governance and the well-being of citizens across the globe. As a nonprofit, non-partisan, international organization, its network is composed of more than 100 democratic former presidents and prime ministers from over 60 countries, together with a global body of advisors and experts practitioners, who offer their voice and agency on a pro bono basis, to today's political, civil society leaders and policymakers. The WLA - CdM responds to a growing demand for trusted advice in addressing the challenges involved in achieving 'democracy that delivers', building bridges, bringing down silos and promoting dialogue for the design of better policies for all. This alliance represents an independent effort towards sustainable development, inclusion and peace, not bound by the interest or pressures of institutions and governments, by providing the experience, access and convening power of its Members.

Visit our website!

[www.clubmadrid.org](http://www.clubmadrid.org)



Follow Us

Twitter: @CLUBdeMADRID

Facebook: [facebook.com/ClubMadrid/](https://facebook.com/ClubMadrid/)

Email: [clubmadrid@clubmadrid.org](mailto:clubmadrid@clubmadrid.org)

# Protecting Information Integrity

## National and International Policy Options