DEMOCRACY AND DIGITAL TECHNOLOGY

Ted Piccone

- *The unique challenges that digital technology is presenting to democratic governments and how they, together with civil society, need to respond*

ABSTRACT

Democratic governments are facing unique challenges in maximising the upside of digital technology while minimizing its threats to their more open societies. Protecting fair elections, fundamental rights online, and multi-stakeholder approaches to internet governance are three interrelated priorities central to defending strong democracies in an era of rising insecurity, increasing restrictions, and geopolitical competition.

The growing challenges democracies face in managing the complex dimensions of digital technology have become a defining domestic and foreign policy issue with direct implications for human rights and the democratic health of nations. The progressive digitisation of nearly all facets of society and the inherent trans-border nature of the internet raise a host of difficult problems when public and private information online is subject to manipulation, hacking, and theft.

This article addresses digital technology as it relates to three distinct but interrelated subtopics: free and fair elections, human rights, and internet governance. In all three areas, governments and the private sector are struggling to keep up with the positive and negative aspects of the rapid diffusion of digital technology. To address these challenges, democratic governments and legislators, in partnership with civil society and media and technology companies, should urgently lead the way toward devising and implementing rules and best practices for protecting free and fair electoral processes from external manipulation, defending human rights online, and protecting internet governance from restrictive, lowest common denominator approaches. The article concludes by setting out what some of these rules and best practices should be.

KEYWORDS

Democracy | Internet | Human rights | Cybersecurity | Elections | Governance

1 • What the evidence tells us

a - Free and fair elections

Cyberattacks from authoritarian governments and non-state actors pose a clear and increasing threat to democracies across the world through their interference in free and fair elections. These attacks take many forms and can undermine and destabilise democratic processes and governance in numerous ways.

There are at least four ways in which cyberattacks can influence elections: (1) manipulating facts and opinions that inform how citizens vote, for example through fake social media accounts, bots and propaganda, (2) interfering with the act of voting (e.g., tampering with voter registration rolls), (3) changing the vote results, and (4) undermining confidence in the integrity of the vote.[1] These threats have emanated from countries like Russia and China and, in the past few years, have targeted nations across the democratic West. For example, the Netherlands' General Intelligence and Security Service specifically named Russia, China, and Iran as national security threats due to cyberattacks.[2] The United States of America (US) Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) released multiple statements in 2016 detailing Russia's ties to recent attacks and leaks with the intent to influence US elections.[3] In May 2017, French President Emmanuel Macron accused the Russian official media of disseminating deceitful propaganda and fake news with the intention of influencing the election results in favour of his opponent.[4]

Similar attacks are becoming increasingly frequent, with more hackings of public and private enterprises; the disruption of internet communications of the lower house of the German parliament; and the spread of disinformation campaigns and false news before the Italian constitutional referendum and the US presidential election.[5] Cyberattacks serve as both a direct and indirect threat to the integrity of the democratic process as they are often motivated by an intention to undermine popular support for democracies, their legitimacy, and their soft power.[6]

Manipulation of information sources for political discourse and decision-making is particularly insidious and difficult to combat. Distinctive characteristics of contemporary forms of Russian propaganda, which can feature polarising content delivered quickly through both social and traditional media, continuously and repeatedly with little commitment to objective reality or consistency, can be difficult for independent media and governments, let alone citizens, to counter.[7] Non-state actors from the radical right and the left, and those engaged in terrorism, are also exploiting the open nature of the internet for multiple purposes, including influencing public opinion before and during elections.[8]

b - Human rights online

The internet can be a tool for both protecting and violating human rights, with direct implications for individuals' cyber and physical security. The diffusion of digital

technology has vastly expanded citizens' opportunities to exercise their rights to freedom of expression and association, to participate in civic life, and to hold public officials accountable, all essential ingredients for holding free and fair elections. Recent technological advances also have helped shed light on human rights abuses committed across the world. Victims' groups now post, livestream, and crowdsource videos and photos of abuses on YouTube and other platforms, in hope they eventually may be used as evidence in accountability proceedings. Human rights investigators used satellite imagery to expose abuses in North Korean political prisons, ethnic cleansing in Myanmar, and potential mass graves in Burundi that otherwise could have gone undiscovered.[9]

Recent years, however, have also seen an ongoing deterioration of human rights online, despite clear declarations from the United Nations General Assembly and the Human Rights Council that offline rights established under international human rights law also are protected online.[10] International law essentially guarantees the same rights to privacy and security of one's online data as they would to the files in their home. For example, mass internet surveillance, practised even in established democracies, is a direct breach of the security of an individual's personal data, as is vague legislation with significant discretionary authority to monitor one's digital life.[11] Internet service providers and telecommunications companies are falling dramatically behind in offering consumers hardware and software products that adequately protect them from a multitude of cyberattacks.[12] The rise in the availability of licit and illicit trade of sophisticated cyber weapons and surveillance tools is facilitating these kinds of attacks, as seen in the worldwide "WannaCry" ransom attacks by hackers in 2017.[13]

Malicious exploitation of technology also can affect the physical security of individuals and of states. For starters, the increased digitisation of the past two decades has created a "chilling effect" on free speech, where citizens in certain countries feel less safe to assert their opinions, knowing that their personal data are monitored or archived.[14] Through location tracking, social media, and internet shutdowns, online security problems become physical ones as well, allowing opponents of democracy and human rights to threaten the physical safety of their alleged targets.

Internet shutdowns and other internet restrictions by governments on their own populaces are widespread, with more than 60 documented shutdowns in the first nine months of 2017,[15] justified on grounds of either "national security" or "public order."[16] These digital blackouts are particularly dangerous for human rights. For example, after both the bombing of the Istanbul airport and the detainment of 11 pro-Kurdish lawmakers in 2016, the Turkish government cut access to social media sites and messaging services such as Facebook, WhatsApp, and Twitter in order to block the circulation of news or photographs relating to these events.[17] These shutdowns did not restore order, but instead violated basic rights and provoked fear and confusion among citizens.

Not only do internet shutdowns impair democratic governance through the suppression of free speech and normal government functions, they also can cause panic and raise public

health concerns.[18] Such breaches also undermine the international rules-based system for internet governance, and encourage state competition in developing intrusive legal codes and offensive cyber capabilities. Lastly, it is important to point out that deteriorating online rights are not only a tactic of authoritarian regimes, but of democratic governments as well. The lack of effective regulatory or oversight mechanisms of private companies' role in protecting citizens' data is another element of the dilemma.

Despite these cyber threats to human rights, some countries have been at the forefront of adopting laws and codes of conduct to protect their citizens' online rights. In Brazil, the 2014 *Marco Civil da Internet* (Civil Rights Framework for the Internet) law "guarantees the right to free expression, protects users' privacy, precludes liability for web content generated by third parties, and preserves Internet neutrality."[19] Also in 2014, the Tallinn Agenda for Freedom Online was established, in which the members of the Freedom Online Coalition, including states like Canada, Ghana, and the Netherlands, pledged to promote human rights online and committed to the transparency of their governments' use and protection of citizen data. Respect for these principles, including among signatory states like Mexico and Kenya, is, however, an ongoing challenge. The Council of Europe has approved a promising Internet Governance Strategy for 2016-19 that highlights building democracy online, protecting human rights, and ensuring online safety and security.[20] These laws, strategies, and coalitions represent promising strides for human rights, and though they are not without problems, they are steps in the right direction.

c - Internet governance

Internet governance serves a crucial role in protecting human rights and sustaining healthy democracies across the globe. The internet was founded on principles of decentralised self-organisation and trans-border information flow and is run mostly by private actors as a network of networks. However, growing assertion of internet regulation by nation states, and fragmentation across jurisdictional and territorial boundaries, increasingly threaten these principles. If one country's internet access is restricted, for example, it interferes with the rest of the world's access. More than 40 governments, including China and Russia, have enacted restrictions on information, data, and knowledge on the internet.[21] According to Freedom House's 2017 Freedom on the Net study, less than 25 per cent of internet users reside in "free" countries where there are no major obstacles to access or restrictions on content.[22]

The term internet governance also refers to the international protocols governing global interoperability of the internet. The ongoing debate on internet governance models had been centred on the US desire to continue the internet's multi-stakeholder approach in which private, social, and governmental sectors are included in the governance model.[23] Because the US was the site of much of the internet's growth and innovation, it has had significant influence over its governing authority, the Internet Corporation for Assigned Names and Numbers (ICANN); this has led other countries to question whether the multi-stakeholder approach is overly biased to the advantage of the US government and private sector.[24]

To address these concerns and in the spirit of preserving an open internet, in September 2016 the Obama administration decided to not renew the US contract with ICANN, thereby relinquishing its predominant influence and making ICANN independent.[25] Nevertheless, countries like Russia, India, and China still criticise the multi-stakeholder model and advocate for a state-centric multilateral approach, which would give them greater influence because international institutions, like the United Nations, would govern the internet.[26]

Proponents of the multi-stakeholder approach, particularly in the private and non-profit sectors, fear that if a state-led multilateral model of governance were enacted, serious losses in internet freedoms and innovation would occur. The multilateral approach gives countries that do not share the same democratic values a larger say in the internet's governance, thereby allowing undemocratic tools of censorship and national internet sovereignty to be introduced more widely. China and Russia already censor the internet that they can control within their borders; giving them decision-making powers in global internet governance could lead to violations of the fundamental principles on which the internet was founded.

Brazil introduced another approach incorporating both multi-stakeholder and multilateral principles in which the private, social, and governmental components are included, along with other stakeholders such as academia and elected nongovernmental representation; this process would be governed in turn by a body that would allow countries equal say in the decision-making process.[27] Though this approach combines both governance models, it is unlikely that it will be adopted without widespread international support. As such, internet governance has increasingly become an issue on which democracies and autocracies take opposite sides, and one which, scholars argue, is of vital importance to the future safety, openness, and resilience of the internet itself.

2 • Policy implications and recommendations

In light of the current and future threats to democracy and human rights posed by irresponsible and disruptive uses of digital communications, the time for human rights defenders to mobilise on questions of digital technology is now. It is imperative that governmental actions do not take a narrow view of security in which national security, counterterrorism, and sovereignty are held above all else. Such strategies, although potentially powerful in the short term, are more likely to contribute to a deterioration of global and national security in the long term.

Protect democratic processes. The environment for free and fair elections and public opinion formation should be made more secure from foreign influence and hacking. Proposals, as in the US, to "designate the election system as 'critical infrastructure,' a move that would require cybersecurity protections for voting machines to be beefed up," would be a good start.[28]

- To ensure the integrity of their elections, democracies should update their election systems and use devices that are not connected to a digital network,[29] or have manual backups to digital systems. Cybersecurity should be continuously updated for sensitive polling place technologies related to voter registration lists, voting, and results tabulation.

- Countries should consider adopting open electoral data principles that allow electoral contestants and the public to verify the integrity of such processes as a further safeguard and as a means to establish public trust in them.[30]

- Democratic governments should work urgently to detect and punish state-sponsored and so-called "patriotic" hackings in order to stop and deter future interference in democratic systems.[31]

- They should also develop protocols to facilitate cross-border cooperation to prosecute hacking of elections infrastructure and draft a code of conduct with pledges of non-interference in each other's elections. Protecting the role of independent media from unfounded attacks is also of growing urgency.

- Democracies should work to build consensus in international forums that a deliberate cyberattack on critical election systems infrastructure is tantamount to a physical attack on its territory, violates international laws of sovereignty and non-interference in domestic affairs, and justifies responses of self-defence.

Protect human rights online. The international community should implement and promote existing human rights laws and mechanisms, and be relentless in upholding offline rights online.

- First and foremost, democracies should set a positive example by respecting such rights themselves.[32] Legislation such as Brazil's *Marco Civil de Internet*, or the European Union's new General Data Protection Regulation, and multi-stakeholder initiatives privileging security and openness such as the Freedom Online Coalition, are examples of concrete laws and initiatives that should be expanded upon and supported.[33]

- States, in partnership with civil society and the private sector, should coordinate positions to strengthen UN resolutions and mechanisms aimed at developing proper norms and monitoring, like the UN General Assembly and Human Rights Council resolutions on internet and privacy sponsored by Germany (A/C.3/71/L.39/Rev. 1 of November 2016) and Brazil (A/HRC/32/13 of July 2016).

- It is critical that private sector companies in the internet ecosystem establish much more rigorous systems, products, and protocols for protecting citizens from intrusions by states and non-state actors.

- Policies governing restrictions on content on the web and digital communications must be carefully crafted with participation by all relevant stakeholders and in accordance with international human rights law such as freedom of expression and right to privacy and due process.

Push for open internet governance. Democratic nations should take a more active and unified stance in internet governance debates, since the historical *laissez-faire* approach can no longer be sustained.[34] They should advocate that internet governance be based on values of an open, diverse, neutral, and universal internet. It should embody four key principles: (1) shared leadership, (2) the free flow of information and data while protecting intellectual property and individual privacy, (3) multi-stakeholder approaches involving emerging and established internet powers and an active civil society and private sector, and (4) industry-led approaches to counter cyberattacks.[35]

Establish a code of internet governance. A coalition of like-minded states should establish a cybersecurity working group composed of experts from government, industry, and civil society to draft and propose a voluntary code of internet governance. This code should reflect the shared values of strengthening democratic governance and transparency, promoting human rights, protecting citizens' data, and advocating on behalf of the multi-stakeholder model.

- Strategies to be considered when adopting this code should be the Council of Europe's 2016-2019 Internet Governance Strategy and the 2014 Tallinn Agenda for Freedom Online, as well as other current models.

- The working group could help coordinate specialised education and training for policymakers on the complex relationship between human rights and digital technology and look at ways to assist members with developing a stronger cybersecurity capacity for protecting democratic processes.

- Upon establishing such standards, the working group should consider consequences for blatant offenders, including conditioning bilateral cooperation on cybersecurity compliance. They must pose the question: how should democracies address nations that attempt cyberattacks on their core democratic processes?

NOTES

1 • Jakob Bund, *Cybersecurity and Democracy – Hacking, Leaking and Voting* (Paris: European Union Institute for Security Studies, 2016): 3.

2 • Kingdom of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service, *Annual Report 2015: A Range of Threats to the Netherlands* (Zoetmeer: General Intelligence and Security Service, 2016).

3 • "GRIZZLY STEPPE - Russian Malicious Cyber Activity," U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), 2016, accessed June 4, 2018, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf. More recently, the U.S. Senate Intelligence Committee concluded that cyberattacks from Russian government sources gained access to restricted elements of election infrastructure. "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," Richard Burr, May 8, 2018, accessed June 4, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf

4 • Michel Rose and Denis Dyomkin, "After Talks, France's Macron Hits out at Russian Media, Putin Denies Hacking." Reuters, May 28, 2017, accessed June 4, 2018, https://www.reuters.com/article/us-france-russia-idUSKBN18P030.

5 • Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, December 8, 2016, accessed June 4, 2018, https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html; Anne Applebaum, "The Dutch Just Showed the World How Russia Influences Western European Elections." The Washington Post, April 8, 2016, accessed June 4, 2018, https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/b427602a-fcf1-11e5-886f-a037dba38301_story.html?utm_term=.79384727c9c9; Jason Horowitz, "Spread of Fake News Provokes Anxiety in Italy." The New York Times, December 2, 2016, accessed June 4, 2018, https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html.

6 • Jakob Bund, "Cybersecurity and Democracy - Hacking, leaking and voting." EUISS, November 2016, accessed June 4, 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_30_Cyber.pdf; Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, December 8, 2016, accessed June 4, 2018, https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html.

7 • Christopher Paul and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model* (Arlington: Rand Corporation, 2016): 4, accessed June 4, 2018, http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

8 • Alice Marwick and Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, 2017): 19, accessed June 4, 2018, https://datasociety.net/output/media-manipulation-and-disinfo-online/.

9 • Christoph Koettl, "These Images Don't Lie: Exposing North Korea's Dirty Little Secret." Amnesty International, December 5, 2013, accessed June 4, 2018, http://blog.amnestyusa.org/asia/these-images-dont-lie-exposing-north-koreas-dirty-little-secret/; "Burundi: Satellite Evidence Supports Witness Accounts of Mass Graves," Amnesty International, January 28, 2016, accessed June 4, 2018, https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/; "Burma: 40 Rohingya Villages Burned Since October," Human Rights Watch, December 17, 2017, accessed June 4, 2018, https://www.hrw.org/news/2017/12/17/burma-40-

rohingya-villages-burned-october.

10 • David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." United Nations General Assembly, A/71/373, September 6, 2016, accessed June 4, 2018, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc; "Silencing the Messenger: Communication Apps Under Pressure. Freedom on the Net Report 2016," Freedom House, November 2016, accessed June 4, 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2016; Antonio Segura-Serrano, "Internet Regulation and the Role of International Law," *Max Planck Yearbook of United Nations Law* 10 (2006): 191-272.

11 • David Kaye, "Report of the Special Rapporteur," 2016.

12 • Toomas Hendrik Ilves, "A Plan for Making the Cyber World Safe." World Economic Forum, p. 2, September 20, 2016, accessed June 4, 2018, https://www.weforum.org/agenda/2016/09/making-the-cyber-world-safe-will-require-more-collaboration-than-ever-before/.

13 • WannaCry is a name for a prolific hacking attack known as "ransomware" that holds one's computer data hostage until a ransom is paid. Ian Sherr, "WannaCry Ransomware: Everything You Need to Know." C|net, May 19, 2017, accessed June 4, 2018, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

14 • Eileen Donahoe, "Human Rights in the Digital Age." Just Security, p. 1, December 23, 2014, accessed June 4, 2018, https://www.justsecurity.org/18651/human-rights-digital-age/.

15 • These include Bangladesh, Brazil, Burundi, Tajikistan, India, Ethiopia, Algeria, Congo, Pakistan, Syria, and Iraq. "#KeepItOn," Access Now, 2017, accessed June 4, 2018, https://www.accessnow.org/keepiton/.

16 • David Kaye, "Report of the Special Rapporteur," 2016; Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year." Center for Technology Innovation at Brookings, October 2016, accessed June 4, 2018, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

17 • Yasmeen Abutaleb and Can Sezer, "Turkey Appears to Be in Vanguard of 'Throttling' Social Media after Attacks." Reuters, July 6, 2016, accessed June 4, 2018, http://www.reuters.com/article/us-mideast-crisis-socialmedia-idUSKCN0ZM2O3; Can Sezer and Humeyra Pamuk, "Turkey Blocks Access to Twitter, WhatsApp: Internet Monitoring Group." Reuters, November 4, 2016, accessed June 4, 2018, http://www.reuters.com/article/us-turkey-security-internet-idUSKBN12Z0H4.

18 • "POLICY BRIEF: Internet Governance and the Future of the NetMundial Initiative," Access Now, 2015, acesso em 4 de junho de 2018, https://www.accessnow.org/cms/assets/uploads/archive/docs/POLICYBRIEFInternetGovernanceandtheFutureoftheNetMundialInitiative.pdf David Kaye, "Report of the Special Rapporteur," 2016.

19 • Carl Meacham, "Is Brazil a Global Leader in Internet Governance?" Center for Strategic and International Studies, May 15, 2014, accessed June 4, 2018, https://www.csis.org/analysis/brazil-global-leader-internet-governance. More work is needed, however, to strengthen Brazil's data protection laws in line with new regulations adopted by the European Union.

20 • "Internet Governance – Council of Europe Strategy 2016-2019," Council of Europe, 2016, accessed June 4, 2018, https://edoc.coe.int/en/internet/7128-internet-governance-council-of-europe-strategy-2016-2019.html.

21 • John D. Negroponte, Samuel J. Palmisano, and Adam Segal, *Defending an Open, Global, Secure, and Resilient Internet* (New York: Council on Foreign Relations, 2013): 13, accessed June 4, 2018, https://www.cfr.org/report/defending-open-global-secure-and-resilient-internet.

22 • "Manipulating Social Media to Undermine Democracy," Freedom House, 2017, accessed June 4, 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

23 • Harold Trinkunas and Ian Wallace, "Converging on the Future of Global Internet Governance: The United States and Brazil." Foreign Policy at Brookings, July 2015, accessed June 4, 2018, p. 26, https://www.brookings.edu/research/converging-on-the-future-of-global-internet-governance-the-united-states-and-brazil/.

24 • *Ibid*.

25 • Megan Stifel, "Maintaining U.S. Leadership on Internet Governance." Council on Foreign Relations, February 21, 2017, accessed June 4, 2018, https://www.cfr.org/report/maintaining-us-leadership-internet-governance.

26 • Harold Trinkunas and Ian Wallace, "Converging on the Future," 2015, p. 19.

27 • *Ibid.*

28 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy." MIT Technology Review, August 4, 2016, accessed June 4, 2018, https://www.technologyreview.com/s/602108/what-the-dnc-hack-says-about-cyber-based-threats-to-democracy/.

29 • Sergio Hernandez, "How to Stop Election Cyberthreats." CNN, November 5, 2016, accessed June 4, 2018, http://www.cnn.com/2016/11/05/politics/voting-vulnerabilities-cyberattacks/index.html.

30 • Open Election Data Initiative, Homepage, 2018, accessed June 4, 2018, http://www.openelectiondata.net/en/.

31 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy," August 4, 2016.

32 • David Kaye, "Report of the Special Rapporteur," 2016.

33 • *Ibid*.; "POLICY BRIEF," 2015.

34 • Robert K. Knake, "Internet Governance in an Age of Cyber Insecurity." Council on Foreign Relations, 2010, accessed June 4, 2018, p. 7, https://www.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.

35 • John D. Negroponte et al., "Defending an Open, Global, Secure, and Resilient Internet," 2013; Harold Trinkunas and Ian Wallace, "Converging on the Future," 2015, p. 5.

TED PICCONE – *United States*

Ted Piccone is a Senior Fellow and Charles Robinson Chair in Foreign Policy at the Brookings Institution. He has written extensively on the foreign policy dimensions of democracy and human rights, including his most recent book, Five Rising Democracies and the Fate of the International Liberal Order. This article draws from a brief he authored for the Community of Democracies in September 2017 with invaluable assistance from Hannah Bagdasar, Carlos Castillo, Jesse Kornbluth, and Matthew Koo.

email: *TPiccone@brookings.edu*

Received in April 2018.
Original in English.