BROOKINGS

Democracy and cybersecurity

TED PICCONE*

POLICY BRIEF

SEPTEMBER 2017

Summary

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

This policy brief addresses cybersecurity as it relates to three distinct subtopics: democratic 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, in partnership with civil society and media and technology companies, should urgently lead the way toward devising and implementing best practices for strengthening free and fair electoral processes, defending human rights online, and protecting internet governance from restrictive lowest common denominator approaches.

About the Project

This policy brief is part of a series of papers on democracy, security, and violent extremism prepared for the Community of Democracies' Democracy and Security Dialogue. The project seeks to foster greater collaboration among democratic governments, donors, civil society and academics to improve security outcomes and create a more conducive environment for the strengthening of democracy around the world. For more on the project and related materials, including the final report, visit www.brookings.edu/democracy-security-dialogue.

* This brief was written with invaluable assistance from Hannah Bagdasar, Carlos Castillo, Jesse Kornbluth, and Matthew Koo, with expert feedback from Tarun Chhabra (Brookings Institution), Eileen Chamberlain Donahoe (Stanford University), Steven Feldstein (Boise State University), Patrick Merloe (National Democratic Institute), Harold Trinkunas (Stanford University), and researchers at the Institute for Security Studies, as well as members of the Community of Democracies Governing Council and its Civil Society Pillar. Brookings is committed to quality, independence, and impact in all of its work. Activities supported by its donors reflect this commitment and the analysis and recommendations are solely determined by the scholar. Support for this publication was generously provided through the Permanent Secretariat of the Community of Democracies.

What the evidence tells us:

Democratic elections

Cyberattacks from authoritarian governments and nonstate 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 destabilize 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, (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, 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 U.S. 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 U.S. 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 favor of his opponent.

These attacks were preceded in 2007 by Russian interference, for example, in Estonia's government, political parties, and banks in a cyberattack that inhibited internet usage for two weeks.[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 Dutch referendum on Ukraine, the Italian constitutional referendum, and the U.S. presidential election, all in 2016 alone.[5] Cyberattacks can 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 decisionmaking is particularly insidious and difficult to combat. Distinctive characteristics of contemporary forms of Russian propaganda, which can feature high-volume 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 to counter.[7] Nonstate actors from the radical right and the radical left, and those engaged in terrorism, are exploiting the open nature of the internet for multiple purposes, including influencing public opinion before and during elections.[8]

Human rights

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. 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 hopes they eventually may be used as evidence in accountability proceedings. Human rights investigators used satellite imagery to expose abuses in North Korean political prisons 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] Everyone is entitled to the same rights online that they have off the internet, such as to privacy, and from mass surveillance and unlawful attacks.[11] 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, practiced 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.[12] 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.[13] 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" attacks of 2017.

Malicious exploitation of technology also can affect the physical security of individuals and of states. For starters, the increased digitization 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 40 documented shutdowns in 2016,[15] justified on grounds of either "national security" or "public order."[16] These 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 provoked fear and confusion among citizens.

Not only do internet shutdowns impair national security through the suppression of free speech, they also can cause panic and raise public health concerns. By cutting access to crucial communication tools, emergency services, and reliable public safety information, shutdowns endanger the physical safety of citizens.[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 on the forefront of adopting laws and codes of conduct to protect their citizens' online rights. In Brazil, the 2014 Marco Civil da 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 is, however, an ongoing challenge, including among signatory states like Mexico and Kenya. The Council of Europe has 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.

Internet governance

Internet governance serves a crucial role in the future of cybersecurity and the sustained health of democracies across the globe. The internet was founded on principles of decentralized self-organization and trans-border information flow and is run mostly by private actors as a network of networks. However, growing assertion by national sovereignties of internet regulation, and fragmentation across jurisdictional and territorial boundaries, increasingly threaten these principles. The concept of internet governance refers to managing access to the internet, whether it be within a nation's borders, or internationally. If one country's internet access is restricted, for example, it affects the rest of the world's access. More than 40 governments, such as China and Russia, have enacted restrictions on information, data, and knowledge on the internet.[21] According to Freedom House's 2016 Freedom on the Net study, 67 percent of all internet users are subject to some form of censorship controls in their countries.

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 centered on the U.S. desire to continue the internet's multi-stakeholder approach in which private, social, and governmental sectors are included in the governance model.[22] Because the United States was the site of much of the internet's growth and innovation, it has had significant influence over its governing authority, the International 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 U.S. government and private sector.[23]

To address these concerns and in the spirit of preserving an open internet, in September 2016 the Obama administration decided to not renew the U.S. contract with ICANN, thereby relinquishing its predominant influence and making ICANN independent.[24] Nevertheless, countries like Russia, India, and China still criticize 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.[25] This debate has stimulated many productive discussions on internet governance through initiatives such as NETmundial, the IANA stewardship transition (privatizing the internet's domain name system), and the World Summit on the Information Society meetings in December 2015 (WSIS+10).

Proponents of the multi-stakeholder approach, particularly in the private and nonprofit sectors, fear that if a state-led multilateral model of governance were to be enacted, serious losses in internet freedom 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 decisionmaking 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 decisionmaking process.[26] 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.

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 democracies to act on questions of cybersecurity is now. Furthermore, it is imperative that such 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, as suggested by the literature, more likely to contribute to a deterioration of global and national security in the long term.

The Community of Democracies participant states should:

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 United States, 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]

- The Community of Democracies governments should also 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 in prosecutions of this kind 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-defense.

Protect human rights online. The Community of Democracies should protect 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, 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 U.N. resolutions and mechanisms aimed at developing proper norms and monitoring, like the

U.N. 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 stand up 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] The Community of Democracies 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.** To carry out these recommendations, the Community of Democracies 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. Another promising group to look to is the Hybrid-threat Center opening in Helsinki in 2017, which is supported by NATO and the EU to combat cyber threats and disinformation.

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

- This working group should also establish a timeline with checkpoints for countries to express concern or ask for help so that the Community can hold itself accountable for fulfilling these goals. Furthermore, 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 the Community address nations that attempt cyberattacks on its members? These combined efforts will present a united democratic front in internet governance debates and cybersecurity improvements moving forward.

Endnotes

1. Jakob Bund, “Cybersecurity and Democracy – Hacking, Leaking and Voting,” (Paris: European Union Institute for Security Studies, 2016).
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. In response, President Obama signed an executive order imposing sanctions on Russian intelligence organizations, the GRU and FSB, and expelled 35 Russian diplomats in December 2016. See U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), “GRIZZLY STEPPE — Russian Malicious Cyber Activity,” (Washington, DC: DHS and FBI, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; “Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment,” The White House Office of the Press Secretary, National Archives and Records Administration, December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.
4. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge: MIT Press, 2013).
5. Melissa Eddy, “After a Cyberattack, Germany Fears Election Disruption,” *The New York Times*, December 8, 2016, 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, 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, https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html; “Statement by the President.”
6. Jakob Bund, “Cybersecurity and Democracy”; Melissa Eddy, “After a Cyberattack, Germany Fears Election Disruption.”
7. Christopher Paul and Miriam Matthews, “The Russian ‘Firehose of Falsehood’ Propaganda Model,” (Arlington: Rand Corporation, 2016), 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), 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, 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, https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/.
10. David Kaye, United Nations General Assembly, A/71/373 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, September 6, 2016; “Silencing the Messenger: Communication Apps Under Pressure. Freedom on the Net Report 2016,” *Freedom House*, November 2016. 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. “Right to Privacy in the Digital Age,” U.N. Human Rights, Office of the High Commissioner, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.
12. David Kaye, *Report of the Special Rapporteur*.
13. Toomas Hendrik Ilves, “A plan for making the cyber world safe,” *World Economic Forum*, September 20, 2016, https://www.weforum.org/agenda/2016/09/making-the-cyber-world-safe-will-require-more-collaboration-than-ever-before/.
14. Eileen Donahoe, “Human Rights in the Digital Age,” *Human Rights Watch*, December 23, 2014, https://www.justsecurity.org/18651/human-rights-digital-age/.
15. These include Bangladesh, Brazil, Burundi, Tajikistan, India, Ethiopia, Algeria, Congo, Pakistan, Syria, and Iraq.
16. David Kaye, *Report of the Special Rapporteur*; Darrell M. West, “Internet Shutdowns Cost Countries $2.4 Billion Last Year,” (Washington, DC: The Brookings Institution, 2016), 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, 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, http://www.reuters.com/article/us-turkey-security-internet-idUSKBN12Z0H4.
18. “POLICY BRIEF: Internet Governance and the Future of the NetMundial Initiative,” (New York: Access Now, 2015), https://www.accessnow.org/cms/assets/uploads/archive/docs/POLICYBRIEFInternetGovernanceandtheFutureoftheNetMundialInitiative.pdf; David Kaye, *Report of the Special Rapporteur*.
19. Carl Meacham, “Is Brazil a Global Leader in Internet Governance?” *Center for Strategic and International Studies*, May 15, 2014, https://www.csis.org/analysis/brazil-global-leader-internet-governance.
20. “1.6 Internet Governance – Council of Europe Strategy 2016-2019,” (Strasbourg: Council of Europe, 2016), 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), https://www.cfr.org/report/defending-open-global-secure-and-resilient-internet.
22. Harold Trinkunas and Ian Wallace, “Converging on the Future of Global Internet Governance,” (Washington, DC: The Brookings Institution, 2015), https://www.brookings.edu/research/converging-on-the-future-of-global-internet-governance-the-united-states-and-brazil/.

23. Ibid.

24. Megan Stifel, “Maintaining U.S. Leadership on Internet Governance,” *Council on Foreign Relations*, February 21, 2017, https://www.cfr.org/report/maintaining-us-leadership-internet-governance.

25. Harold Trinkunas and Ian Wallace, “Converging on the Future.”

26. Ibid.

27. Mike Orcutt, “What the DNC Hack Says about Cyber-Based Threats to Democracy,” *MIT Technology Review*, August 4, 2016, https://www.technologyreview.com/s/602108/what-the-dnc-hack-says-about-cyber-based-threats-to-democracy/.

28. Sergio Hernandez, “How to Stop Election Cyberthreats,” *CNN*, November 5, 2016, http://www.cnn.com/2016/11/05/politics/voting-vulnerabilities-cyberattacks/index.html.

29. National Democratic Institute, USAID, and Google, “Open Election Data Initiative,” http://www.openelectiondata.net/en/.

30. Mike Orcutt, “What the DNC Hack Says about Cyber-Based Threats to Democracy.”

31. David Kaye, *Report of the Special Rapporteur*.

32. Ibid.; “POLICY BRIEF: Internet Governance and the Future of the NetMundial Initiative.”

33. Robert K. Knake, “Internet Governance in an Age of Cyber Insecurity,” (New York: Council on Foreign Relations, 2010), https://www.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.

34. John D. Negroponte et al., “Defending an open, global, secure, and resilient Internet”; Harold Trinkunas and Ian Wallace, “Converging on the Future.”