C1: Global Freedom

Democracy is in freefall:

Max Boot, 12-12-2020, "Opinion," Washington Post, <https://webcache.googleusercontent.com/search?q=cache:PKW_novxhZ0J:https://www.washingtonpost.com/opinions/2020/03/04/new-report-shows-freedom-is-declining-established-democracies-including-ours/+&cd=4&hl=en&ct=clnk&gl=us>

*democratic erosion is now the norm across the world. The “Freedom in the World 2020” survey, released Wednesday by Freedom House, reports that 2019 saw the 14th year in a row of political deterioration, with 64 countries experiencing a loss of liberties, while only 37 experienced improvements. Some of the worst repression is occurring in China as a result of what the report rightly describes as “the Chinese Communist Party’s ongoing campaign of cultural annihilation in Xinjiang.” But you expect repression from a communist regime. What is truly disheartening is to read that during the past year, “25 of the world’s 41 established democracies experienced net losses” of freedom. The worst offender is the world’s largest democracy, India. The recent anti-Muslim pogroms in New Delhi — which killed 46 people and were carried out with the connivance of senior police officers — are sadly indicative of the country’s illiberal direction under Prime Minister Narendra Modi and his Hindu nationalist party, the Bharatiya Janata Party (BJP). As Freedom House notes: “While India continues to earn a Free rating and held successful elections last spring, the BJP has distanced itself from the country’s founding commitments to pluralism and individual rights, without which democracy cannot long survive.” Less dramatic but nevertheless depressing is the erosion of U.S. democracy. Since 2009, the United States has fallen eight points on Freedom House’s 100-point scale. With a score of 86, we are now ranked behind countries such as Greece, Slovakia, Italy and Mauritius. Freedom House points out some alarming trends of late, which include “an ongoing decline in fair and equal treatment of refugees and asylum seekers,” Trump’s declaration of “a national emergency in order to redirect Defense Department funds to the construction of a wall along the southern border,” his attempt to “extract a personal political favor from Ukrainian president Volodymyr Zelensky,” and his orders to “current and former officials to defy all congressional subpoenas for document and testimony about the matter.” This is only a small part of Trump’s efforts to undermine checks and balances, which include an ongoing purge of officials deemed traitors to Trumpism, blatant political interference with the administration of justice, and frivolous libel suits against The Post and the New York Times intended to silence critics. Similar erosion is occurring in one of the United States’s closest allies, Israel, where Prime Minister Benjamin Netanyahu has emerged from the latest election on Monday in a strong position to form a new government despite his indictment on corruption charges. Freedom House notes that “Netanyahu has taken increasingly drastic steps to maintain the loyalty of far-right groups, entrenching and expanding West Bank settlements at the expense of the moribund Palestinian peace process, banning foreign activists based on their opposition to such policies, and enacting a discriminatory law that reserved the right of self-determination in Israel to the Jewish people.” There is a real danger that countries such as India, the United States and Israel may now be going down the same road that Hungary and Poland have already traveled.*

Indiscriminate wide-scale NSA Surveillance erodes privacy rights and violates the constitution:

Sinha, 2014, G. Alex Sinha is an Aryeh Neier fellow with the US Program at Human Rights Watch and the Human Rights Program at the American Civil Liberties Union, July 2014 “With Liberty to Monitor All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy” Human Rights Watch, <http://www.hrw.org/node/127364>//EZG

*The current, large-scale, often indiscriminate US approach to surveillance carries enormous costs. It erodes global digital privacy and sets a terrible example for other countries like India, Pakistan, Ethiopia, and others that are in the process of expanding their surveillance capabilities. It also damages US credibility in advocating internationally for internet freedom, which the US has listed as an important foreign policy objective since at least 2010.As this report documents, US surveillance programs are also doing damage to some of the values the United States claims to hold most dear. These include freedoms of expression and association, press freedom, and the right to counsel,*

Surveillance enables authoritarianism:

Dr. Kat Hadjimatheou Prof. Martin Scheinin, 2015, Ethics and surveillance in authoritarian and liberal states Seventh Framework Programme, <https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.4-Ethics-and-surveillance-in-authoritarian-and-liberal-states.pdf>//

*A number of the arguments put forward in support of the claim that the use of surveillance invites or opens the door to authoritarian government claim that there is a slippery slope from the former to the latter. These arguments take the following form: the use of power for authoritarian purposes is unacceptable; surveillance leads to the use of power for authoritarian purposes; therefore surveillance is unacceptable.3Slippery slope criticisms of surveillance do not object to surveillance on the ground that it is intrinsically or always itself an authoritarian exercise of power. On the contrary, they often allow that some measures of surveillance would be legitimate or justified when viewed in isolation. However, they claim that even these measures of surveillance are nevertheless unacceptable, because in practice they lead to authoritarian uses of power. The strongest form of slippery slope argument claims that surveillance necessarily or inevitably leads to authoritarian government. Weaker versions claim that surveillance removes or diminishes barriers to authoritarian government. Some slippery slope arguments treat all kinds of surveillance techniques as cumulatively responsible for driving us down the slope (Kateb, 2001). More commonly, arguments focus on the use of mass databases (such as ID card registration schemes, DNA databases, the storage of electronic communication records)because these databases store information that can be used for a broad range of purposes, including authoritarian ones(Clarke, 1994; Balkin, 2008).Five slippery slope arguments are discussed in this section. The first claims that surveillance makes people more tolerant of authoritarian uses of state power and thus removes one important barrier to its realisation. The second claims that surveillance encourages governments to see and treat people as mere conscripts to their purposes, denying their autonomy. The third claims that surveillance powers will inevitably be used for illiberal ends. The fourth claims that surveillance powers will eventually fall into, and strengthen greatly, the hands of authoritarian regimes. The fifth claims that surveillance powers willbe used in authoritarian ways against minority groups.2.1 Surveillance makes people more tolerant of authoritarian uses of state powerThis argumentstates that the proliferation ofsurveillance techniquesnormalises their use andreducesopposition to their application for authoritarian purposes.4It begins by pointing out that being monitoredand having one’s information collected, shared, and analysed without one’s full knowledgeor meaningful consent has becomethe normin many modern societies.*

The Second impact is Totalitarianism, the loss of autonomy due to surveillance enables “turnkey totalitarianism,” destroying democracy.

Haggerty, 2015, Kevin D. Professor of Criminology and Sociology at the University of Alberta, “What’s Wrong with Privacy Protections?” in A World Without Privacy: What Law Can and Should Do? Edited by Austin Sarat p. 230 //EZG

*NSA senior executive – says the security surveillance infrastructure he helped build now puts us on the verge of “turnkey totalitarianism.”67 The contemporary expansion of surveillance, where monitoring becomes an ever-more routine part of our lives, represents a tremendous shift in the balance of power between citizens and organizations. Perhaps the greatest danger of this situation is how our existing surveillance practices can be turned to oppressive uses. From this point forward our expanding surveillance infrastructure stands as a resource to be inherited by future generations of politicians, corporate actors, or even messianic leaders. Given sufficient political will this surveillance infrastructure can be re-purposed to monitor – in unparalleled detail – people who some might see as undesirable due to their political opinions, religion, skin color, gender, birthplace, physical abilities, medical history, or any number of an almost limitless list of factors used to pit people against one another. The twentieth century provides notorious examples of such repressive uses of surveillance. Crucially, those tyrannical states exercised fine-grained political control by [were] relying on surveillance infrastructures that today seem laughably rudimentary,comprised as they were of paper files, index cards, and elementary telephone tapping.68 It is no more alarmist to acknowledge such risks are germane to our own societies than it is to recognize the future will see wars, terrorist attacks, or environmental disasters – events that couldthemselves prompt surveillance structures to be re-calibrated towards more coercive ends. Those who think this massive surveillance infrastructure will not, in the fullness of time, be turned to repressive purposes are either innocent as to the realities of power, or whistling past a graveyard. But one does not have to dwell on the most extreme possibilities to be unnerved by how enhanced surveillance capabilities invest tremendous powers in organizations. Surveillance capacity gives organizations unprecedented abilities to manipulate human behaviors, desires, and subjectivities towards organizational ends*

Totalitarianism opens the floodgates for mass murder.

R.J. Rummel, xx-xx-1994, "20TH CENTURY DEMOCIDE (Genocide and Mass Murder)," University of Hawaii, <https://www.hawaii.edu/powerkills/DBG.CHAP1.HTM> //EZG

*Power kills, absolute Power kills absolutely. This new Power Principle is the message emerging from my previous work on the causes of war*[*1*](https://www.hawaii.edu/powerkills/DBG.CHAP1.HTM#1) *and this book on genocide and government mass murder--what I call* [*democide*](https://www.hawaii.edu/powerkills/DBG.CHAP2.HTM)*--in this century. The more power a government has, the more it can act arbitrarily according to the whims and desires of the elite, the more it will make war on others and murder its foreign and domestic subjects. The more constrained the power of governments, the more it is diffused, checked and balanced, the less it will aggress on others and commit democide. At the extremes of Power*[*2*](https://www.hawaii.edu/powerkills/DBG.CHAP1.HTM#2)*, totalitarian communist governments slaughter their people by the tens of millions, while many democracies can barely bring themselves to execute even serial murderers.*

C2: Unpatched

The NSA uses zero-day exploits for surveillance.

Michelle Drolet, 9-12-2016, "Does the NSA have a duty to disclose zero-day exploits?," CSO Online, https://www.csoonline.com/article/3118735/does-the-nsa-have-a-duty-to-disclose-zero-day-exploits.html //EZG

This dichotomy exacerbates tensions between both various branches of government and between government and private industry. Within government, the NSA [is] withholding zero-day exploits for their own use in spying and other offensive maneuvers conflicts with agencies tasked with protecting Americans from attack, like the Department of Homeland Security.

Trey Herr, xx-xx-xxxx, "Taking Stock: Estimating Vulnerability Rediscovery," Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

When combined with an estimate of the total count of vulnerabilities in use by the NSA, these rates suggest that rediscovery of vulnerabilities kept secret by the U.S. government may be the source of up to one-third of all zero-day vulnerabilities detected in use each year. These results indicate that the information security community needs to map the impact of rediscovery on the efficacy of bug bounty programs and policymakers should more rigorously evaluate the costs of non-disclosure of software vulnerabilities.

No Author, xx-xx-xxxx, "," No Publication, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf>

Stockpiling may be beneficial for those offensively focused, and technically

sophisticated vulnerability researchers likely prefer to stockpile vulnerabilities they

find, rather than disclose them. Defenders will always be vulnerable to zero-day vulnerabilities, and likely will want to disclose and patch a vulnerability upon discovery.

Our data did not indicate that there are any vulnerabilities that are “stronger” or

“weaker” than others in terms of resilience to being discovered and disclosed. It may

be most efficient and cost-effective to develop an exploit for whatever vulnerability is

easiest to find or whatever vulnerabilities are most effective.

Finding #1: Declaring a vulnerability as alive (publicly unknown) or d

Cybersecurity Ventures, 11-13-2020, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," No Publication, <https://www.prnewswire.com/news-releases/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025--301172786.html>

SAUSALITO, Calif., Nov. 13, 2020 /PRNewswire/ -- Cybersecurity Ventures predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Joshua Kurlantzick, 11-19-2008, "Financial Crisis May Worsen Poverty in China, India," Council on Foreign Relations, <https://www.cfr.org/backgrounder/financial-crisis-may-worsen-poverty-china-india>

By year’s end, the impact of the global financial crisis of 2008 was starting to be felt in the developing world, with slowdowns expected in all emerging economies. These growth declines could have significant effects on the world’s poorest populations. The World Bank estimates that a 1 percent decline in developing country growth rates traps an additional 20 million people in poverty. Concern centers on slowing growth in India and China, the world’s two most populous nations and the largest contributors to reductions in global poverty in the last two decades, according to many academic studies. Reduced economic growth in both countries could reverse poverty alleviation efforts and even push more people into poverty, say some experts. The financial crisis has also likely made the achievement of the United Nations’ Millenium Development Goals (MDGs) on poverty--to halve the proportion of people in extreme poverty by 2015--more difficult.

C3: Drone Violence

Ending domestic surveillance collapses the NSA’s global security operations.

Sam Adler-Bell, 3-16-2017, "10 Reasons You Should Still Worry About NSA Surveillance," Century Foundation, <https://tcf.org/content/facts/10-reasons-still-worry-nsa-surveillance/?session=1andsession=1//Roy>

In the process of spying on foreigners, the NSA cannot help but collect large volumes of Americans’ communications. The intelligence community refers to this collection as “incidental,” but it including vast amounts of Americans’ conversations, email exchanges, photos, and other sensitive information.

NSA data key for drones.

Eversley, State, Oct 16/13, "Report: Documents show NSA involvement in drone program," USA TODAY, <https://www.usatoday.com/story/news/politics/2013/10/16/nsa-drone-campaign-cia/2998439/> Roy

drone campaigns -- which uses armed, unmanned aerial vehicles -- frequently presented as exclusive territory of the CIA, depends heavily on the ability of the NSA to sweep up information from e-mails, telephone calls and other pieces of signals intelligence,

It’s mass metadata.

Naughton, 2-21-2016, "Death from above, dished out by algorithm," Guardian, <https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan> Roy

the NSA hoovers up all the metadata of 55m mobile phone users in Pakistan and then feeds them into a machine-learning algorithm which supposedly identifies likely couriers working to shuttle messages and information between terrorists.

This is done without verification on the ground.

Sam Byford@345triangle, 2-10-2014, "Drones kill civilians using NSA data, Greenwald's new site 'The Intercept' reports," Verge,<https://www.theverge.com/2014/2/10/5396920/drone-strikes-have-killed-innocents-with-nsa-data> //Roy

The NSA's surveillance programs are often used to help carry out drone strikes on targets, according to a new report, and sometimes there are unintended victims. An anonymous former drone operator for Joint Special Operations Command (JSOC) [told *The Intercept*](https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/) — a new publication helmed by Glenn Greenwald, who [broke the first of many](http://www.theverge.com/2013/6/5/4400582/secret-court-order-reportedly-forces-verizon-to-hand-over-call-records-to-NSA) NSA revelations last year — that the US military and CIA use the NSA's metadata analysis and phone-tracking abilities to identify airstrike targets without confirming their veracity on the ground.

Ending surveillance will produce more tried-and-true methods.

(Stephen M. Walt is the Robert and Renée Belfer professor of international relations at Harvard University, “The Big Counterterrorism Counterfactual Is the NSA actually making us worse at fighting terrorism?”,<http://www.foreignpolicy.com/articles/2014/11/10/counterterrorism_spying_nsa_islamic_state_terrorist_cve>, November 10, 2014)

What would [if] the United States, Great Britain, and other wealthy and powerful nations do if they didn't have these vast surveillance powers? What would they do if they didn't have armed drones, cruise missiles, or other implements of destruction that can make it remarkably easy (and in the short-term, relatively cheap) to target anyone they suspect might be a terrorist? Assuming that there were still violent extremists plotting various heinous acts, what would these powerful states do if the Internet was there but no one knew how to spy on it? For starters, they'd [it would] have to rely more heavily on tried-and-true counterterrorism measures: infiltrating extremist organizations and flipping existing members,, etc., to find out what they were planning, head attacks off before they occurred, and eventually roll up organization themselves. States waged plenty of counterterrorism campaigns before the Internet was invented, and while it can be difficult to infiltrate such movements and find their vulnerable points, it's not exactly an unknown art. If we couldn't spy on them from the safety of Fort Meade, we'd probably be doing a lot more of this. Second, if we didn't have all these expensive high-tech capabilities, we might spend a lot more time [and] thinking about how to discredit and delegitimize the terrorists' message, instead of repeatedly doing things that help them make their case and recruit new followers.

Drones lead to terrorism.

Author(s): MICHAEL J. **BOYLE** Source: International Affairs (Royal Institute of International Affairs 1944-) , January 2013, Vol. 89, No. 1 (January 2013), pp. 1-29 Published by: Oxford University Press on behalf of the Royal Institute of International Affairs Stable URL:<https://www.jstor.org/stable/23479331> //Roy

Following the escalation of drone strikes in Yemen, the desire for revenge drove hundreds, if not thousands, of Yemeni tribesmen to join Al-Qaeda in the Arabian Peninsula (AQAP), as well as smaller, indigenous militant networks.

Quantification for Terror

Michael **Jetter**, 2019, Military Intervention via Drone Strikes, IZA Institute of Labor Economics,

<http://ftp.iza.org/dp12318.pdf> //Roy

This paper introduces an empirical strategy to isolate the causal effects of drone strikes in Pakistan on subsequent terrorism, anti-US sentiment, and radicalization, employing wind as the key IV. We hypothesize that wind decreases the likelihood of the US military employing a drone strike, conditional on observable characteristics, whereas wind is otherwise orthogonal to terrorist activities. Both assumptions receive support in our sample of 4,018 days from 2006 to 2016. Results from 2SLS estimations suggest drone strikes increase the number of terror attacks in Pakistan in the upcoming days and weeks. This finding prevails in a host of alternative estimations and robustness checks. Extending the timeframe of subsequent terrorism, we find evidence indicating drone strikes do not just affect the timing of attacks (e.g., by moving forward planned attacks) but rather increase the total number of attacks. In terms of magnitude, **one drone strike** today **causes over four additional terror attacks per day** in the next seven days which implies drone strikes are responsible for 16 percent of all terror attacks in Pakistan. A back-of-the-envelope calculation suggests 2,964 people died from terror attacks because of drone strikes. We then explore mechanisms, distinguishing between insiders, i.e., those who already belong to terrorist organizations, and outsiders, i.e., regular Pakistanis. Specifically, we study anti-US sentiment in the major English-language newspaper in Pakistan, anti-US protests, and online searches for terms that may be indicative of radicalization (jihad, Taliban video, and Zarb-e-Momin). In line with the blowback hypothesis, results from 2SLS estimations suggest **[as] the general populace increasingly turns to anti-US and radical expressions after drone strikes**

Terrorism leads to civil war.

Lai, Brian, 2008 "Examining the Escalation of Terrorist Violence to Civil War," Iowa University,<https://myweb.uiowa.edu/bhlai/workshop/lailarsen.pdf> //Roy

For the period of 1950-2000, we have 559 terrorist groups. Of those 559, 65 or about 12% escalate their use of force to a civil war. Table 1 presents three sets of cross tabulations of the three main independent variables and the dichotomous escalation to civil war variable. For the number of groups, the values have been truncated to 0,1,2, and 3 or more. Looking at table 1, the goal and ideology variables seem to be supported as secession and center goals have a statistically higher percentage of cases ending in escalation than policy oriented goals. Similarly, identity and leftist ideologies produce statistically higher percentages of cases escalating than other ideologies (right wing, environmental, anarchist, etc). The final independent variable does receive as strong support as the percentages are not statistically significant and for 3 or greater, the percentage is greater than the other values, suggesting that more [as] groups may weaken the state, creating greater opportunities for groups to engage in insurgency.

Civil wars are really bad.

No Author, 10-7-2016, "Examining policy responses toward failed states, civil wars," Stanford Freeman Spogli Institute,<https://fsi.stanford.edu/news/policy-responses-examined-failed-states-civil-wars> //Roy

As for the case of Syria, Eikenberry noted that such civil wars can actually become more lethal and dangerous to global order than inter-state conflicts. These types of conflicts like that in Syria tend to escalate into high levels of violence because of the costs that the losing parties believe they will incur, he said. “This in turn leads to state fragmentation and the possibility of transnational groups with international ambitions getting involved,” he said. “Civil wars result in an enormous number of civilian casualties, which generates large scale refugee flows” and puts huge pressure on neighboring states.