Some Reflections on a Match made in Hell: Authoritarianism and Technology

Luisa Morettin

Abstract: This article is a reflection on Ruth Ben-Ghiat’s chapters two ‘Military Coups’ and nine, ‘Resistance’, from Strongmen. How They Rise, Why They Succeed, How They Fall, where the author discusses military coups and resistance. More specifically, how strongmen can both secure their hold on power and silence the opposition. Here I expand on that idea by throwing light on the relationship between authoritarianism and technology.

Keywords: strongmen, authoritarianism, technology, resistance, coups

Introduction

As authoritarian regimes have no mechanism in place to transfer power, coups d’état are the common way to topple undemocratic leaders. As Ben-Ghiat rightly argues, ‘many strongmen who come to power by coup leave it in the same fashion.’ Therefore, it is no surprise that what authoritarian leaders fear the most is political upheaval.

Putsches may come in many forms and each one is unique in its planning and execution details. However, as Edward Luttwark’s valuable Coup d’État: A Practical Handbook clearly points out, typically all coups can be reduced to three major considerations: first, power is seized at maximum speed by a political faction, the armed forces, or a dictator who will then need to neutralise those forces that oppose the seizure. Second, for the coup to be successful such a mode of political change relies heavily on the passivity of both the populace and the government’s bureaucrats. Third, the coup should be organized in such a fashion that control of the centre is sufficient as decentralised systems pose too many co-ordination issues for the plotters.

In the past, the only means that illiberal leaders had to counter the ever-present threat of a likely putsch was by creating a complex and sophisticated network of informants, spies, agents, and officers who over time infiltrated every walk of life to ensure that the people would become and remain submissive, so that the regime maintained its grip.

on power. For example, towards the end of the Communist regime in East Germany, the powerful secret police *Staatssicherheitsdienst*, commonly known by its abbreviation Stasi, ‘had 102,000 full-time officers and non-commissioned personnel on its rolls, including 11,000 members of the ministry’s own special guards’ regiment. Between 1950 and 1989, a total of 274,000 persons served in the Stasi. […] The ratio for the Stasi was one secret policeman per 166 East Germans.’ Likewise the Soviet KGB (Committee for State Security), whose major directorates were foreign intelligence and technical intelligence, expanded in the 1960s to include a department dedicated to the surveillance of the domestic intelligentsia and the churches, thus becoming the (in)famous “sword and shield of the Communist Party”.

Fast-forward to the twenty-first century and coups are not as frequent as they used to be. Their heyday was in the mid-1960s. Ben-Ghiat notes that ‘two-thirds of dictators were removed by coups between 1950 and 2000.’ More specifically the American Centre for Systemic Peace highlights that ‘in 1980 there were 19 coups or attempted coups around the world, or roughly one every 19 days. In 2020, by contrast, the world went 230 days without one.’

One of the reasons behind this trend, apart from the improvement in countries’ economic conditions and growth rates, can be found in entirely new methods and tools for political control. They include, but are not limited to, online censorship, device hacking, and artificial intelligence (AI) powered mass surveillance, which autocracies widely use to enable or enhance their authoritarian governing practices, limit freedom of expression, and manage repression. Even if anti-government protests may have increased, autocrats manage to suppress them and stiffen controls by developing or acquiring technical mechanisms to spy on citizens, track their movements, monitor their text messages, read their emails and social media posts, and censor online information. Such digital repression allows undemocratic governments to adopt a subtle approach: rather than indiscriminately repressing many, a course of action that could cause a backlash, it is now possible to clearly identify and target the few political dissidents. Modern surveillance system and

---

4 Ben-Ghiat, p. 37.
coup-proofing strategies are now much easier and more efficient and require fewer resources and manpower than in Stasi or KGB times.

A textbook case showing how autocrats can easily use technology to retain power is the 15 July 2016 plot to topple Turkey’s President Recep Tayyip Erdoğan. One of the possible reasons why the coup attempt failed is because, as per Edward Luttwark’s list of variables and obstacles to a coup, the plotters did not neutralise Erdoğan by securing proper control of the media. The technology savvy president, instead, immediately harnessed social media to rally his aides and crowds of supporters. Taking to FaceTime to reach a television presenter, he sent his first message to the nation calling on people to take to the streets to resist the “narrow cadre” behind the uprising, and promised punishment to those responsible. In the meantime, his aides used WhatsApp to communicate with each other and avert the dangerous situation, while the prime minister tweeted to his followers to help regain control of a police department in Istanbul. Reaching a wide audience in a short time and asserting his control allowed the President to gain time and assemble the forces that foiled the coup, thus preserving his repressive power.

The plotters fatally miscalculated the digital transformation of Turkish society. But if the government managed to repress the coup thanks to modern tools of virtual communication, the crackdown it employed in its wake though relied on very traditional, “real life” means. Erdoğan declared a state of emergency, allowing himself to sign laws without prior parliamentary approval and to close down many independent media. According to official statistics and NGOs (non-governmental organizations), more than 107,000 people were removed from public sector jobs, among them soldiers, civil servants, journalists, judges, at least 5,000 academics and more than 33,000 teachers. Educators were targeted not only because schools and universities are hubs for critical thinking, but also because ‘younger people […] have the most to lose from living with leaders who use them as baby-making machines or cannon fodder and are often among the first groups to organise for action.’

More than 50,000 people were imprisoned pending trial. Human rights group Amnesty International reported how detainees were tortured.

---

7 Ben-Ghiat, p. 196.
and raped in jail. There were also a large number of dismissals in the private sector. The state of emergency was lifted only two years later after Erdoğan was re-elected.

At the same time, maintaining control over access to the internet, broadband and information within a country’s sovereign borders is of fundamental importance for despots. President Vladimir Putin, for instance, never made a mystery of his views on the subject: ‘The government […] is an owner and the media that belong to the government must carry out our instructions.’

The Russian leader also granted the secret service extensive monitoring powers and ‘the persecution of government critics has reached levels not seen for two decades’, according to data collected by Reporters Without Borders, an independent NGO with consultative status with the United Nations, UNESCO, and the Council of Europe. Fearing the emancipatory potential of knowledge through the Internet, which allows individuals to circumvent tightly controlled TV and newspapers, many other repressive governments such as Burma/Myanmar, China, and Iran rely heavily on blocking, filtering and censoring the Internet thanks to common DNS tampering, IP blocking, keyword and packet filtering strategies. Sophisticated technology allows governments not only the tightening of Internet control within their countries, but also to gain access to communications in others - as Russia’s cyber-meddling in the 2016 US presidential election has proven-, thus shaping ‘the legal architecture of what Russian strategists like to call the “information space”’.

That there is a global market for digital technologies and surveillance tools is nothing new. China, for instance, is no longer a rising power as far as technology is concerned, but a leading player in developing and exporting tools in areas such as facial and voice recognition, predictive policing systems and the drone market. China's expansion of its public


security apparatus has been most evident in Xinjiang, where Beijing has interned about one million Uighurs, a mostly Muslim ethnic group. The situation was described by a UN human rights panel as “mass surveillance disproportionately targeting ethnic Uighurs.” Those of them lucky enough not to be detained in the so-called “reeducation” camps actually live in towns equipped with facial recognition software gates. The tool is based on precog algorithms, such as a video-based recognition system, which automatically recognizes faces in a crowd verifying them against a database of enrolled persons. The result is then immediately communicated to the access control system, which either grants entry or raises an alert if the individual is not authorised, thus staving off potential harmful actions in real time. China is building a sinister high-tech authoritarian future proving that George Orwell’s Nineteen Eighty-Four is no longer science fiction. In fact, we are facing a real and unprecedented political stranglehold.

Following China’s example, many other repressive regimes around the world are relying on such advanced technologies to undermine adversaries, engineer crackdowns against targeted individuals or populations by monitoring their physical and digital activities and controlling information. Chinese companies export their surveillance technology to illiberal countries such as Iran, Kenya, Uganda, while Latin America, in particular, has become a ‘core economic interest’ region for Beijing. Venezuela’s President Nicolas Maduro, for instance, introduced a new national identity card system that, after grading citizens based on behaviour including financial solvency and political affiliation, logs them in a database purchased from ZTE, the Chinese telecoms giant.

China is not the only country supplying advanced surveillance tech worldwide. However, if it can be expected that illiberal governments support each other trading surveillance AI. What is extremely worrisome,

is that companies incorporated in democracies also sell a high volume of AI powered systems. Surveillance was an important contributor to the repression that culminated in the 2011 crisis and ensuing civil war in Syria. Despite a European embargo against the Bashar al-Assad regime, in 2011, AREA, an Italian company, sold technology and monitoring systems capable of capturing internet traffic, tapping conversations, and tracking targets through GPS to the Syrian Telecom Establishment; the government-owned provider. Italian engineers were flown into Damascus to install the technology and train the officers who would monitor it.\footnote{AREA struck a deal with the Egyptian government, too, but allegedly the Italian Ministry of Economic Development revoked its authorisation for the same company to sell its surveillance technology to Egypt in 2017, only after protests from a charity that defends and promotes the right to privacy across the world.\footnote{Ben Elgin and Vernon Silver, ‘Syria Crackdown Gets Italy Firm’s Aid With U.S.-Europe Spy Gear’, Bloomberg, 3 November 2011, \url{https://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear} [accessed 24 April 2021]. See also: ‘Italy Cancels Surveillance Export to Egypt But New Undercover Documentary Shows Surveillance Industry Brazenly Continues to Export to Repressive Regimes’, \textit{Medium}, 23 January 2017, \url{https://medium.com/privacy-international/italian-authorities-urged-to-act-following-reports-of-internet-surveillance-system-being-exported-c1defc3afe46} [accessed 24 April 2021].} AREA struck a deal with the Egyptian government, too, but allegedly the Italian Ministry of Economic Development revoked its authorisation for the same company to sell its surveillance technology to Egypt in 2017, only after protests from a charity that defends and promotes the right to privacy across the world.\footnote{Trevor Timm, ‘Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA’, \textit{Electronic Frontier Foundation}, 21 February 2012, \url{https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa} [accessed 8 May 2021].}

Italy is not alone in prioritising corporate profits over human rights. Other countries are aiding authoritarians around the world. Given its significant technological knowledge and experience, Israel is one of the leading countries in developing, producing, and selling unmanned systems, such as patrol vehicles, ground robotic systems, and loitering munitions, that were purchased by China, South Korea, Turkey, Uzbekistan, and Azerbaijan.\footnote{Liran Antebi, ‘Artificial Intelligence and National Security in Israel’, Institute for National Security Studies, February 2021, \url{https://www.inss.org.il/publication/artificial-intelligence-and-national-security-in-israel/} [accessed 24 April 2021].} The German interceptions firm Trovicor, a former subsidiary of Nokia Siemens, is another Western company that, in total disregard for human rights abuses that occur through the use of their surveillance tools, sold spy technology to a dozen of actual and would-be autocracies in the Middle East and North Africa.\footnote{Ben Elgin and Vernon Silver, ‘Torture in Bahrain Becomes Routine With Help From Nokia Siemens’, Bloomberg, 22 August 2011, \url{https://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking} [accessed 22 April 2021].} US tech firms have also exported facial recognition technology to Saudi Ara-
bia and the United Arab Emirates, while others such as Facebook and Twitter are conniving in information control in countries like India, where Prime Minister Narendra Modi is poised to remake India into a Russian-style “managed democracy” – one retaining all the trappings of democracy while operating as a de facto autocracy.21

Such conduct based on commercial interests is serious not only because of human rights contraventions, but also because it may have disastrous implications for the future of democracy. That is happening at a time when the international liberal order seems to steer slowly, but steadily towards authoritarianism thus threatening global stability. According to The Economist’s Democracy Index 2020, ‘only about half (49.4%) of the world’s population live in a democracy of some sort, and even fewer (8.4%) reside in a “full democracy”’.22

The outcome should not come as a surprise given the fact that the global trend in recent years has been of a persistently slow decline in democracy.23 The NGO Freedom House’s latest ‘Nations in Transit’ report, which covers twenty-nine countries from Central Europe to Central Asia, also laments that ‘a growing number of leaders in Central and Eastern Europe have dropped even the pretence of playing by the rules of democracy’.24 The potential stakes are, therefore, extremely high because the risk that innovative technology will usher in a new wave of authoritarianism is now more tangible than ever.

In spite of that, established democracies seem unconcerned by the fact that using twentieth century rules to govern twenty-first century emerging innovations is not fit for purpose. Apparently liberal states are running headlong into the ideologies of authoritarianism, ethnic nationalism, and corruption without fully grasping the long-term challenge posed by democratic decay and emboldened populist politicians across the globe. ‘How to find ourselves again?’, Ben-Ghiat asks, quoting an Italian writer who fought against Mussolini’s regime. ‘For millions,’ she sug-

---

gests, ‘acts of resistance have been a path to the recovery of the self, and the affirmation of dignity, empathy, and solidarity.’

So, what does that mean, practically, for current democratic governments who turn a blind eye to those strongmen? The governments and regulatory agencies in democratic states need to promote legitimacy and trust in new technologies, ensuring that all internet-related practices adhere to international human rights standards, while cutting the ties between intelligence agencies and private companies. At the same time leaders have to strengthen crucial alliances with like-minded governments and work with the World Trade Organization towards the adoption of steep fines, clear chains of accountability, and more stringent and consistent export control regulations that will prevent companies from exporting their technology to repressive regimes. The ultimate aim is for states to be held accountable for extraterritorial human rights violations caused by those companies whose technological innovations violate principles of transparency and informed consent, and impact a wide range of fundamental rights, such as rights to privacy, freedom, and non-discrimination. Although such reforms may be no easy task for liberal leaders, they must persist because strongmen are here for the foreseeable future.

Works Cited:


Ben-Ghiat, Ruth, Strongmen. How They Rise, Why They Succeed, How They Fall (London: Profile Books, 2020)


25 Ben-Ghiat, p. 197.
Democracy Index 2020: In Sickness and in Health?, The Economist Intelligence Unit, (2021), [https://www.eiu.com/n/campaigns/democracy-index-2020/] [accessed 18 April 2021]


'Democracy Index 2020: In Sickness and in Health?', The Economist Intelligence Unit, (2021), [https://www.eiu.com/n/campaigns/democracy-index-2020/] [accessed 18 April 2021]


Nebehay, Stephanie, 'U.N. calls on China to free Uighurs from alleged re-education camps’, 30 August 2018, Reuters, [https://www.reuters.com/article/uk-china-rights-unidU8KCN1LFIE0] [accessed 6 May 2021]

Reporters without Borders, [https://rsf.org/en/europe-central-asia] [accessed 28 April 2021]


**Luisa Morettin** (BA Padua, Italy; MA University of Westminster; PhD University of Reading) has held teaching and research positions at the University of Edinburgh, King’s College London, and the University of Reading. Her latest monograph is titled *A Blood Border: Trieste Between Mussolini and Tito* (New York: Nova, 2019).