Military Cyber Affairs

Volume 3 | Issue 2 Article 3

December 2018

Regaining the Technological Edge: Authoritarians, Democracies, IT Innovation's Future

Andrea Little Limbago
Virtru, alimbago@virtru.com

Regaining the Technological Edge: Authoritarians, Democracies, IT Innovation's Future[1]

Andrea Little Limbago[2]

Policy, law, and ethics lag behind technology.[3] This is a common refrain that accurately reflects the reality in democratic states, but is not necessarily the case for authoritarian regimes. Authoritarian states have much more quickly embraced technological changes and innovations to further entrench regime durability, including information control. The slipping innovation dominance, and innovation gap between authoritarian and democratic regimes, therefore, may be one of stagnant political innovation as opposed to slipping technological innovation. Authoritarian regimes have more adeptly embraced digital technologies to further their domestic and international objectives while democratic regimes' laissez-faire and myopically optimistic approach has left them scrambling to understand and influence the digital domain. The United States must reassert global leadership in shaping the future of the internet. That leadership will require a broader acknowledgement of full-spectrum cyber behavior, including the policies and laws required to benefit democratic values and norms. With that acknowledged, the U.S. risk obsolescence in shaping the future international order.

Authoritarian Policy Innovation

For decades while tech sectors and governments in democracies were singularly focused on the promises of a technological utopia, authoritarian regimes have pursued strategies exploiting internet expansion for information control. These activities often are first tested on domestic

[1] Limbago, Andrea Little, "Regaining the Technological Edge: Authoritarians, Democracies, IT Innovation's Future," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).
[2] Chief Social Scientist at Virtru
[3] https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/

populations, expanded to international targets, and at times replicated by other states. In this manner, domestic populations provide the initial testbed for data manipulation, censorship, and destructive attacks which is then applied to international targets. For instance, China tests techniques for both espionage campaigns as well as disinformation on Taiwan before deploying them to global targets.[4] Moreover, China's Great Firewall has inspired Iran's Halal Network and Russian cyber sovereignty, instigating discussions of a global splinternet as opposed to a globally integrated system.

In addition, data localization efforts that require data or domains to physically operate within borders greatly impacts cross-border data flows and international business while giving authoritarian regimes unique access to personal and commercial data. For instance, in 2005 Kazakhstan required all .kz top-level domain names to operate on servers within its borders.[5] In Iran, extensive online censorship coupled with requirements for local data storage from apps such as WhatsApp and Telegram are key components of their information control. Importantly, these tactics have expanded into weak democracies such as Turkey where the Law on the Protection of Personal Data limits the transfer of personal data out of Turkey, while requiring some data stored in country as well. In fact, a similar law a decade earlier targeting Internet-based payment services led PayPal to withdraw.

The two most prominent examples of this authoritarian, cyber sovereignty model are China and Russia. While they share some similarities, there also are some distinctions and so it is worth providing a high-level overview of their approach to data localization and cyber sovereignty as these are the models that are inspiring others across the globe.

Chinese Model

In October, Chinese President Xi Jinping thoroughly detailed his vision of Socialism with Chinese Characteristics that includes internet control to "oppose and resist the whole range of erroneous viewpoints".[6] This emphasis on cyber sovereignty reinforces China's cybersecurity law which similarly places the government as the protector and manager of online content.[7]

[4] https://www.nytimes.com/2018/10/05/opinion/china-cyberattack-hacking-us-midterm-election.html
[5] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost
[6] https://www.bbc.com/news/world-asia-china-41744675
[7] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/

https://digitalcommons.usf.edu/mca/vol3/iss2/3
DOI: https://doi.org/10.5038/2378-0789.3.2.1057

According to the law, data localization requirements focus on critical infrastructure businesses and firms with access to personal data. For over a decade, China has demanded foreign corporations turn over data, but this new law tightens the requirements and blacklists corporations who fail to comply.[8] While the definition of critical infrastructure remains vague, the law could undermine foreign intellectual property and the privacy of individual data held by corporations operating in China.[9] The law went into effect in 2017, and is expected to impact those companies leveraging big data the most, greatly increasing data processing costs and logistical challenges for companies.[10] With the larger movement toward AI and the internet of things, this law has farther reaching impact, including on companies such as social media platforms that host web content and websites in China.[11]

The repercussions of China's data localization extends beyond its own sovereign borders. For instance, China has led several efforts to integrate state internet control requirements into United Nations documents focused on global cyber norms.[12] China also seeks to control Chinese language media and content external to its borders as part of a broader strategy to garner influence abroad.[13] Domestically, China's emphasis on government control of data has enabled a nascent social credit system that perhaps best personifies the striking repercussions of competing approaches to data protection.[14] As revealed in 2014, China is developing a national system to track and rate the reputations of individuals and businesses. It will increasingly influence all aspects of life, including loan applications, dating profiles, job prospects, airplane ticket purchases, travel, and property ownership.[15] Individuals are scored based on a range of factors such as financial debt, deviation from state-approved online content, and the scores of others within your social networks.

[8] https://arstechnica.com/tech-policy/2007/11/yahoo-calls-withholding-of-info-on-chinese-arrests-a-misunderstanding/
[9] https://www.wsj.com/articles/chinas-blurry-cyber-laws-give-u-s-tech-companies-no-security-1512558004
[10] http://www.china-briefing.com/news/2018/01/04/chinas-digital-economy-shape-things-come.html
[11] https://www.theregister.co.uk/2017/06/01/china_cybersecurity_law/
[12] https://thediplomat.com/2015/12/china-brings-push-for-cyber-sovereignty-to-the-un/
[13] http://www.abc.net.au/news/2017-06-04/australian-sovereignty-under-threat-from-chinese-influence/8583832
[14] https://www.wired.com/story/age-of-social-credit/
[15] https://www.theglobeandmail.com/news/world/chinese-blacklist-an-early-glimpse-of-sweeping-new-social-credit-control/article37493300/?utm_medium=Referrer:+Social+Network+/+Media&utm_campaign=Shared+Web+Article+Links

Finally, China already blocks several U.S. internet companies, and further assists in domestic development of Chinese competitors. This too has great global impact, as Tencent passed Facebook last year in market capitalization.[16] Tencent also has ten percent stake in Snapchat's parent company Snap.[17] Other Chinese tech giants such as Alibaba and Baidu continue to expand as well. Although they are not technically state-owned enterprises, these companies influence China's capabilities for internet and data control, including a dominant role positioning China to emerge as the global leader in AI, and further strengthening localized government control of data.[18]

Russian Model

China and Russia share many similarities in their push for cyber sovereignty and data localization, including a bilateral 'nonagression pact' for mutual support of sovereignty and refraining from attacks.[19] Russia is best known for various high profile breaches and a propaganda machine of troll factories and disinformation that seeks to disrupt elections across the globe, divide societies, and weaken democracies.[20] However, there is much more to the Russian approach, including a strict focus on cyber sovereignty to simultaneously control domestic information, expand data localization policies globally, and shape the global digital infrastructure.

In 2015, a new Russian law required all data collected on Russian citizens to be stored and processed on servers in Russia.[21] This law equally applies to countries outside of Russia, and has already resulted in the blocking of websites owned by U.S. companies. Recently, Russia has pressured Facebook to detail how it is adhering to this law, and is stepping up pressure on foreign corporations for compliance.[22] Russia's 2016 information security doctrine outlines its far-reaching approach to information security, including an integration of both the technical and the

[16] https://www.telegraph.co.uk/technology/2017/11/21/chinas-biggest-social-media-company-tencent-now-worth-facebook/
[17] https://www.telegraph.co.uk/technology/2017/11/08/wechat-owner-tencent-takes-10pc-stake-snap/
[18] https://www.scmp.com/tech/china-tech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team
[19] https://www.defenseone.com/ideas/2015/08/russia-china-cyber-nonaggression-pact/119302/
[20] https://www.thenation.com/article/russias-attacks-on-democracy-arent-only-a-problem-for-america/
[21] https://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes
[22] https://www.reuters.com/article/us-facebook-russia-data/russia-asks-facebook-how-it-complies-with-data-law-ifax-idUSKBN1HJ2AB

https://digitalcommons.usf.edu/mca/vol3/iss2/3
DOI: https://doi.org/10.5038/2378-0789.3.2.1057

social and psychological components of digital information control.[23] Russia also requires foreign companies to provide source code for security products as a cost of doing business there.[24] Two pieces of legislation in 2017 further focus on data control, eliminating anonymity online and restricting tools to evade censorship, including VPNs and anonymizers.[25]

Russia has embraced many aspects of China's internet strategy, working to create its own 'Great Firewall' (dubbed the Red Web), and continues to rise in global measures for censorship and surveillance.[26] Whereas China tends to censor content based on keywords and limiting collective expression and congregation, Russian censorship focuses more on cultural control, fostering self-censorship in publications, websites, and media due to nebulous guidelines.[27] Russia often first deploys various forms of Russian information security domestically, such as fostering societal divisions through disinformation, before applying them internationally.

Additionally, as part of the broader effort to leverage data collection for domestic control, Moscow recently introduced a new facial recognition capability within a city-wide camera network.[28] While depicted as a means to capture criminals, it has massive privacy implications and contributes to the ongoing expansion of domestic surveillance. Finally, Russia is actively attempting to shape global information flows. For example, Russia recently provided the infrastructure to expand North Korean internet access, resulting in 60% more internet access thanks to this second connection.[29] Simultaneously, Russia has proposed building an independent

---

[23] https://www.forbes.com/sites/seanlawson/2016/12/09/russia-gets-a-new-information-security-doctrine/#5341a8a63fc4
[24] https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB
[25] https://www.hrw.org/news/2017/08/01/russia-new-legislation-attacks-internet-anonymity, https://www.bbc.com/news/technology-41829726
[26] http://www.slate.com/articles/technology/future_tense/2017/04/russia_is_trying_to_copy_china_s_internet_censorship.html , https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact
[27] https://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collective-expression
[28] https://techcrunch.com/2017/09/28/moscow-officially-turns-on-facial-recognition-for-its-city-wide-camera-network/
[29] https://www.forbes.com/sites/outofasia/2017/12/01/russia-is-now-providing-north-korea-with-internet-what-that-could-mean-for-cyber-warfare/#4546d300386b

internet infrastructure among the BRICS countries (Brazil, Russia, India, China, and South Africa), which includes an alternate domain name system which would allow each country greater autonomy and control over access to specific websites.[30] This alternate internet, combined with data sovereignty, is intended to grant Russia greater autonomy and control of digital information.

Democratic Responses

For the most part, democracies have not evolved at the same pace as authoritarian regimes in their digital policy innovation. In the United States, the Computer Fraud and Abuse Act from 1986 remains the benchmark bill guiding appropriate online activity. Instead, the European Union is currently the leading democratic entity shaping individual security and privacy online, and establishing appropriate behavior and access in cyberspace. The General Data Protection Regulation (GDPR) is the most prominent policy that reflects key tenets of the multi-stakeholder model, including an emphasis on individual privacy and civil liberties. At its core, the GDPR maintains a strong emphasis on individual data protections, which includes personally identifiable data (PII), but extends to content about an individual. Key data protection features within the GDPR are the right to erasure (aka the right to be forgotten), and the right for an individual to access their data and rectify incorrect data.[31] It is a far-reaching framework that impacts everything from marketing to artificial intelligence to breach notification.[32] Importantly, the GDPR introduces data standards that pertain to data of European Union citizens regardless of where the data is held.[33] Even if a corporation is not headquartered in the EU, but they have data on EU citizens, they must comply with the GDPR.

The EU's push toward individual data protection and privacy is not surprising in the wake of the increasingly unprecedented magnitude and scope of corporate data breaches. The GDPR also reinforces the values and norms of individual freedoms and humans rights that

[30] https://www.bleepingcomputer.com/news/government/russia-wants-to-launch-backup-dns-system-by-august-1-2018/
[31] https://gdpr-info.eu/art-17-gdpr/
[32] http://searchcrm.techtarget.com/feature/Accommodating-GDPR-email-marketing-regulations-a-top-priority, http://www.aitech.law/blog/data-privacy-ai-and-the-gdpr , https://gdpr-info.eu/art-33-gdpr/
[33] http://www.itsecurityguru.org/2017/01/30/impact-gdpr-outside-eu/

https://digitalcommons.usf.edu/mca/vol3/iss2/3
DOI: https://doi.org/10.5038/2378-0789.3.2.1057

are foundational to the EU.[34] In this way, data regulation frameworks intersect with and adhere very closely to their native political institutions. The GDPR reflects the political and economic union of 28 democratic members, prioritizing the data protection and individual rights that reinforce democratic institutions. In turn, with the additional emphasis on corporate responses to data breaches, the GDPR advances specific norms for security and privacy within a regulatory framework.

While the GDPR is the result of years' worth of negotiations, compromises, and corporate input, the United States lacks anything remotely similar and more so reflects a patchwork of proposals with an unknown time frame or probability for implementation.[35] The U.S. has taken a sector-specific approach to data privacy, such as the Health Insurance Portability and Accountability Act. Lacking a national policy, individual states are seeking their own solutions, such as current proposals in Georgia to modify the CFAA, or the city of Los Angeles, which required Google to store data within the U.S. as a contractual condition.[36] This recent Congressional hearings on social media manipulation and data privacy demonstrated how nascent these discussion are, wherein the idea of regulation was floated, but remains nebulous at best. The Honest Ads Act is one proposal where social media would be regulated similar to traditional media, but currently has not significantly progressed toward implementation, and does not address data privacy concerns.

Social Blowback, Technological Change & Policy Innovation

However, all is not lost for democracies. Current trajectories should not be assumed to be permanent or unwavering. Authoritarian regimes do not face the same constraints those in democracies, and have adeptly exploited this gap through digital interference at home and abroad in pursuit of regime objectives. To date, this has given them the edge and enabled innovative tactics, techniques and procedures to optimize information control. Nevertheless, the persistence of this trajectory should not be assumed. Russia's recent attempt to block the popular messaging

[34] http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_2.1.2.html
[35] https://www.accessnow.org/data-protection-in-the-united-states-where-do-we-go-from-here/
[36] http://www.legis.ga.gov/Legislation/en-US/display/20172018/SB/315 ,
https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

app, Telegram, is a case in point.[37] After Russia's censor Roskomnadzor attempted to block Telegram due to its failure to comply to Russian information laws, numerous proxies were established to circumvent the ban. In response, Russia expanded the censorship, unintentionally blocking millions of IP addresses, including those at grocery stores, taxi companies, ticket agencies, and some social media and e-commerce sites.[38] The ban led to a major backlash, referenced to as an 'internet civil war', an uptick in Telegram downloads, and igniting greater resistance against other censorship efforts. The Russian Education Ministry's Science Council even released a statement that these internet outages have locked researchers out of online services that are "extremely important for scientific work."[39] The laws have also stimulated capital flight and hindered the business environment.

In this regard, technology not only enables authoritarian regimes, but also enables social change within the authoritarian regimes as well. For example, blockchain and social media have enabled pent-up anger over sexual harassment and is showing unprecedented signs of a #metoo movement at several top Chinese universities.[40] Similarly, digital currencies reflect this dual-use nature of digital technologies. Venezuela and North Korea attempt to leverage digital currencies to circumvent sanctions, but so do domestic protesters as concern over the economic climate mounts and provides access to the global economy. Moreover, many of the digital natives are becoming more tech savvy, finding means to circumvent censors and bans via changes in geolocation tagging, or VPNs, for example. Finally, this closed-off, autarkic approach to data has been found to have a negative impact on innovation and science.[41]

Given the role of data security and privacy as a cornerstone of human rights and democracy in the digital age, the U.S. would benefit from renewed focus on innovation in the policy domain, not just technology. The internet is a socio-technical problem that for the most part has been addressed solely through a technical lens. Interestingly, there also is social change within the

[37] https://www.aljazeera.com/news/2018/04/internet-civil-war-erupted-russia-180423124936679.html
[38] https://www.bloomberg.com/news/articles/2018-04-22/putin-s-turf-war-with-telegram-escalates-as-russia-blocks-ips
[39] https://gizmodo.com/russia-is-still-trashing-its-internet-two-weeks-into-it-1825561879
[40] https://www.wsj.com/articles/chinas-universities-face-a-metoo-moment-1524394801
[41] http://www.sciencemag.org/news/2017/08/science-suffers-china-s-internet-censors-plug-holes-great-firewall

https://digitalcommons.usf.edu/mca/vol3/iss2/3
DOI: https://doi.org/10.5038/2378-0789.3.2.1057

United States demanding greater regulation for data security and privacy, which just may be the impetus required to ignite policy innovation in the digital domain.[42]

The international system is at an inflection point, and requires leadership and policy innovation by the United States. This is not to discount the diminishing technological gap, but technology and policy are interconnected. The current patchwork, sector specific and Cold War-mentality approach to the digital age in the United States is obsolete, and is hindering technological innovation as well.

This is not only a problem in digital technologies, but across the broader lens of technological innovation. For instance, China, France and the United Kingdom have new AI strategies, but nothing similar seems on the radar in the U.S.[43] Each of these directly challenge U.S. technological leadership, even though the Chinese version is based on an Obama-era document on AI research and development.[44] Similarly, cryptocurrencies and cryptomining attacks is another area where other governments have moved forward to block or regulate these exchanges, while the United States remains in discussion mode.[45] And these current challenges will pale in comparison to the imminent digital challenges, including video and voice mimicry and the proliferation of actors and attacker techniques that are directly related to data security and privacy.

Importantly, and counter to claims that data is the new Cold War, the U.S. must not focus policies honed and tuned for a Cold War environment.[46] This is not Cold War 2.0, but a new situation where technology has greatly impacted power dynamics, and will continue to do so for the foreseeable future. The U.S. must close the gap between technological and policy innovation, focusing holistically on data protections, defenses, and responses, ensuring reinforcement of democratic values. Absent any movement, the global vacuum is being filled by authoritarian

---

[42] https://www.axios.com/axios-surveymonkey-public-wants-big-tech-regulated-5f60af4b-4faa-4f45-bc45-018c5d2b360f.html

[43] https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html, https://techcrunch.com/2018/03/29/france-wants-to-become-an-artificial-intelligence-hub/, http://fortune.com/2018/04/25/uk-ai-artificial-intelligence-deal/

[44] https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

[45] https://www.reuters.com/article/us-crypto-currencies-congress/congress-sets-sights-on-federal-cryptocurrency-rules-idUSKCN1G31AG

[46] https://www.wired.com/story/opinion-new-data-cold-war

regime, shaping not only the future of the internet, but widespread technological applications that directly influence the future for security, privacy and democracy.

https://digitalcommons.usf.edu/mca/vol3/iss2/3
DOI: https://doi.org/10.5038/2378-0789.3.2.1057