THE RICHARD C. HOLBROOKE FORUM
FOR THE STUDY OF DIPLOMACY
AND GOVERNANCE

September 2017

NET REACH

TECHNOLOGY COMPANIES AS FOREIGN POLICY PLAYERS

By Adam Segal

In 2010, the University of Southern California political scientist Ernest Wilson III could legitimately argue that, compared to their agricultural or industrial counterparts, technology companies played a very limited role in shaping US foreign policy.[1] The first generation of information and communication technology entrepreneurs were generally libertarian in their political outlook, saw policy as a distant concern—if not an outright impediment—and their primary focus was on satisfying domestic consumers, not reaching foreign markets.

Less than a decade later, the reach of American technology companies is global, and their market position almost monopolistic, both domestically and abroad. Within the United States, Google has close to 90 percent of market share in advertising, and Facebook has 77 percent of social mobile traffic.[2] In Europe, Google has close to 90 percent of the search market (compared to 70 percent in the US), and has businesses that upset book publishers (Google Books), media (YouTube and Google News), and car manufacturers (driverless cars). The top three phone apps in India are owned by Facebook, and almost all of India's mobile phones run on either Google's Android or Apple's iOS operating system. Revenue growth for US firms is faster in the rest of the world than at home.

The enormous stake technology companies have in foreign markets means that they not only shape US policy, but also, to some extent, have become relatively autonomous foreign-policy actors. In February 2017, Denmark announced it was appointing a "digital ambassador," who would not only interact with states and international organizations but also with technology giants such as Facebook and Alphabet (Google's holding company). In his statement on the new position, Minister for Foreign Affairs Anders Samuelsen explained, "Companies such as Google, IBM, Apple, and Microsoft are now so large that their economic strength and impact on our everyday lives exceeds that of many of the countries where we have more traditional embassies."[3]

Until the National Security Agency contractor Edward Snowden released documents in June 2013, revealing the scope of Washington's surveillance practices, technology companies acted as a multiplier of US power. The fact that the majority of the world relied upon software and hardware developed by US companies, and that much of the world's internet traffic passed through the United States, gave US intelligence agencies an unmatched reach. Former National Security Agency (NSA) director Michael Hayden put it bluntly when justifying some of the NSA's activities, telling the *National Journal*, "This is a home game for us. Are we not going to take advantage that so much [data] goes through Redmond, Washington? Why would we not turn the most powerful telecommunications and computing management structure on the planet to our use?"[4]

Technology companies' reputations and legitimacy rests on claims of economic growth and innovation, tied to social goods such as "making the world more open and connected" and "organizing the world's information," all while protecting user's data, rights, and privacy. After the Snowden disclosures, in order to try to regain trust, companies actively worked to distance themselves from the US government through the widespread implementation of encryption technology and legal challenges to US surveillance practices.[5] But since the companies' business models remain tied to surveillance (for advertising, not law enforcement or intelligence), suspicion remains high, especially in Europe, where the use of the acronym "GAFA"—Google, Apple, Facebook, and Amazon—reflects unease with the size and dominance of the American firms.

Technology firms have so far wielded little of the traditional power of making others do what they do not want to do. Instead, they have had significant capability in agenda-setting and indirect influence; they have been exploited by populist movements, such as the Brexit campaign. As the physical and digital worlds increasingly converge, and as some of the largest technology firms become dominant in artificial intelligence (AI), their coercive power over small states may significantly increase. They may also spark a backlash that brings them into direct conflict with powerful regulatory states.

TECH FIRMS & INTERNATIONAL POLITICS

Large companies have, of course, influenced foreign policy in the past. The 1661 Charter of the East India Company granted it sovereign territory and the power of declaring and waging war against non-Christian peoples. The United Fruit Company received land concessions from several Caribbean governments and lobbied the Eisenhower administration to support the overthrow of the democratically elected Guatemalan government of Colonel Jacobo Arbenz Guzmán, in 1954. Throughout the 1970s and 1980s, most of the largest multinational firms were American, which meant that policymakers in other nations often viewed them as an extension of US hegemony. Today, ExxonMobil operates in some two hundred nations and territories and has a foreign policy that does not always overlap with US interests. Any US company with operations in foreign markets, especially those in minerals, petroleum, or other extractive resources, have to pay special attention to their relationship with foreign governments.

The power of technology companies is, however, qualitatively different. Tech companies challenge nation-state sovereignty across multiple issues simultaneously. Any change that Facebook makes to its news feed, privacy settings, advertising methods, or encryption standards can affect a country's politics, civic engagement, cybersecurity, counter-terror strategy, tax revenues, and innovation. The decision to roll out end-to-end encryption, for example, has severely limited the ability of law enforcement and intelligence agencies to collect data on criminals and terrorists. Proprietary algorithms determine which news stories citizens read, and artificial intelligence is used to identify and block terrorist postings. Private companies such as FireEye and CrowdStrike have also played the role of intelligence agencies, identifying state-backed hackers in the attacks on Sony, the *New York Times* and other news outlets, and the Democratic National Committee.

In a few instances, the companies have directly challenged states. During the January 2011 protests against President Hosni Mubarak, the Egyptian government shut down the internet to stop activists from communicating with each other and the outside world. While the United States and others deliberated on how to actively support a longtime ally or to shift support to protesters, Google, in cooperation with Twitter, soon rolled out a product called speak2tweet, which allowed Egyptians with mobile-phone access to record voicemails, which were then posted on Twitter. Jigsaw, an incubator within Google, now builds technology to thwart online censorship, mitigate the threats from digital attacks, and counter violent extremism.

Technology companies have also taken a lead in defining and developing new norms of state behavior in cyberspace. In February 2017, Brad Smith, chief legal officer of Microsoft, gave a speech at the RSA cybersecurity conference calling for a Digital Geneva Convention "that will commit governments to protecting civilians from nation-state attacks in times of peace." Smith noted that one of the defining characteristics of the digital age is that cyberspace is produced, owned, secured, and operated by the private sector, and so the targets in cyberwar are private property owned by civilians. As a result, the tech companies act as "first responders" to nation-state attacks. In addition to deploying technical solutions such as encryption to fight state hacking, Smith called for the companies to "commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."[6]

The companies are also colonialists of the mind, hijacking attention and interest, and normalizing specific behaviors and outlooks. They have had a broad cultural impact, spreading a positive, almost utopian view of technology and influencing attitudes toward surveillance ("If you're not paying for the product, you are the product"), innovation ("fail fast, fail often"), and regulation ("move fast and break things"). Moreover, the biases and causal logic of algorithms and artificial intelligence are opaque, making it difficult for consumers and policy makers to understand their influence on health care, financial and insurance markets, and the media. Yuval Noah Harari argues that Silicon Valley is creating a narrative that legitimizes the authority of algorithms and big data and challenging traditional sources of authority.[7]

While US companies have been the dominant face of this new foreign-policy activism, they will not be alone, especially as new global technology firms emerge in China.[8] Alibaba, China's biggest e-commerce group, handles more transactions then EBay and Amazon combined. Valued at $275 billion, Tencent, a social media and gaming company, is one of the most active investors in startups in India and Silicon Valley. Baidu, the search-engine giant, has over a dozen apps used by more than 300 million people outside of China. Chinese companies are also beginning to take a political role. Jack Ma, Alibaba's founder, is the head of a Chinese government initiative on cyberspace governance known as the Wuzhen Initiative and, in 2016, convinced the G20 to adopt a proposal for an "electronic world trade platform" to make it easier for small businesses to trade across borders.[9]

The tech companies are also reworking the sources of military power. During the Cold War, the government drove the development of space, stealth, and aviation technologies, but, over the last three decades, national defense capabilities have grown increasingly reliant on private-sector innovation. Military strength is now highly dependent on the ability to collect, sort, analyze, and distribute data more accurately and quickly than the adversary. The sensors, cameras, communication devices, computers, networks, and algorithms that do this work are, however, no longer designed and developed exclusively by the Pentagon. If they were, it would take years to test and acquire, and once the product finally arrived, it would be out of date. Instead, the Defense Department acquires commercial, off-the-shelf technologies and modifies them for military use.

Reliance upon the private sector for military technology will intensify with AI and robotics. The "third offset" strategy, the Pentagon's plan to retain military advantage over China and Russia, is built on the exploitation of intelligent machines. The plan calls for $18 billion over five years (2017-2022), and will follow a model of investing in advanced technology like AI, automation, big data, and 3-D printing to reassert the United States military's operational edge and, in the words of Deputy Secretary of Defense Robert Work, "strengthen convention deterrence."[10] As a result, policymakers are looking at new methods of strengthening connections to technology companies, through initiatives like Defense Innovation Unit Experimental, which has outposts in Silicon Valley, Austin, and Boston.[11] China is also trying to strengthen ties between the military and the private sector, promoting a plan of civil-military fusion, and opening up defense procurement to small start-ups developing drones and artificial intelligence.[12]

THE STATE STRIKES BACK

This is not to suggest that states, at least those with big domestic markets and technological sophistication, cannot strike back. While the technology firms prefer a free, open, and global internet, the trend has been toward a fragmented internet. According to Freedom House, internet freedom around the world declined in 2016 for the sixth consecutive year.[13] Moreover, the ability to move data around, however, is increasingly under threat, as more states assert "cyber sovereignty" and demand that firms localize data storage. LinkedIn abandoned the Russia market rather than comply with a law that it store all Russian user data within the country, and Apple, despite its promotion of user privacy and security, removed anticensorship tools from its app store in China so as to comply with Beijing's new cybersecurity law.

Moreover, states are forcing the platforms to police content. Google, Facebook, and Twitter have moved to control extremist content in part because of threats from France, Germany, and the UK to impose significant fines if the companies did not take action to remove harmful action. German lawmakers, for example, are considering a bill that requires social media companies to delete "evidently unlawful" content within 24 hours, and less "evidently unlawful" content within seven days, or face fines of up to €50 million. Lawmakers in the United States are considering revisions of Section 230 of the Communications and Decency Act, which granted them exemption from liability for hosting illegal content. This and other regulatory moves suggest that the days of considering the technology companies as engines of growth, with their innovative edge uniquely endangered by regulation, may be coming to an end.[14]

The platforms themselves can be hijacked to serve nation-state goals. In April 2017, Facebook acknowledged that it had become a platform for nation-state information operations, or efforts to spread misleading information in pursuit of political goals. Facebook researchers found during the 2016 presidential election "malicious actors leveraging conventional and social media to share information stolen from other sources, such as email accounts, with the intent of harming the reputation of specific political targets."[15] A research team at Oxford University has found Twitter bots—computer programs that automate the posting of messages and which can tweet from 500 to 1,300 times a day—being used in numerous countries to spread propaganda and manipulate public opinion.[16]

States may simply resist the requests of the technology companies. In the wake of the WannaCry ransomware attack, Microsoft and other technology companies criticized the vulnerabilities equities process (VEP), the method through which the US government decides whether to reveal vulnerabilities to the private sector or to hold on to them for intelligence gathering or offensive cyber-operations. WannaCry, which encrypted data and held it captive until a ransom was paid, exploited a vulnerability that was allegedly developed by the NSA and was offered online by a group known as Shadow Brokers. How this vulnerability and other tools made their way to Shadow Brokers, which is assumed to be a cover for Russian intelligence, is unknown.

Microsoft's Smith held WannaCry up as evidence that the government cannot safely stockpile vulnerabilities. "An equivalent scenario with conventional weapons would be," according to Smith, "the US military having some of its Tomahawk missiles stolen."[17] The proper response, Smith continued, must be for the government to no longer stockpile, sell, or exploit vulnerabilities, and instead report them to vendors immediately. There is very little chance, however, that Washington will accept these proposals. Beijing and Moscow have no similar programs, and the US is unlikely to disclose all of its exploits unilaterally.

CROSSROADS

As machines exceed human intelligence and skill in more areas of work, the technology companies will remake national economies. Many prominent technologists and entrepreneurs believe the widespread adoption of AI will be like the shift from steam to electricity, transforming transportation, manufacturing, healthcare, finance, and other sectors.[18] For every new industrial robot introduced into the workforce, six jobs are eliminated, and a PricewaterhouseCoopers report predicts that automation will place 38 percent of the US labor force at high risk in the next 15 years.[19]

The confluence of these technologies threatens to increase the capabilities gap between large and small powers in the international system and to heighten inequality within already highly polarized societies. So far, the development trajectory of AI suggests that the powerful technology companies will be even more dominant players in international affairs. They control the vast majority of data needed to build artificial intelligence, attract the most skilled talent to their labs, and are the largest funders of research and development in the field. They could essentially monopolize the inputs to the next wave of innovation, and, as a result, could be the sole suppliers to governments of essential technologies and services, with power and influence flowing from their ability to turn on and off the flow.

Yet the need for big data for innovation may be transitory. Efforts to make public-sector data more widely available could help new companies as much as the larger ones. In addition, smaller AI firms are already developing machine-learning software that requires significantly fewer examples to learn.[20] Government efforts to regulate, and possibly break up, the largest firms may result in AI becoming a widely available utility like electricity; today electric power and transmission companies wield no independent foreign-policy power.

No matter the development trajectory of AI, the pervasive reach of data into all aspects of life means that technology firms will continually be at the center of states' concerns about sovereignty. The biggest states will still be able to constrain the technology companies, but their indirect power and influence, particularly vis a vis small nations, will remain considerable.

NOTES

[1] Ernest Wilson, “Google, China and US Foreign Policy,” Huffington Post, April 2, 2010, http://www.huffingtonpost.com/ernest-j-wilson/google-china-and-us-forei_b_443741.html

[2] Jonathan Taplin, “Is It Time to Break Up Google?” New York Times, April 22, 2017, https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html?_r=0

[3] Peter Baugh, “‘Techplomacy’: Denmark’s ambassador to Silicon Valley,” Politico, July 20, 2017http://www.politico.eu/article/denmark-silicon-valley-tech-ambassador-casper-klynge/amp/

[4] Michael Hirsch, “How America’s Top Tech Companies Created the Surveillance State,” National Journal, July 25, 2013, http://www.nationaljournal.com/magazine/how-america-s-top-tech-companies-created-the-surveillance-state-20130725

[5] Adam Segal, Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (PublicAffairs, 2017).

[6] Brad Smith, “The need for a Digital Geneva Convention,” https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[7] Yuval Noah Harari on big data, Google and the end of free will, Financial Times, August 16, 2016, https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c

[8] Paul Mozur, “The World’s Biggest Tech Companies Are No Longer Just American,” New York Times, August 17, 2017, https://www.nytimes.com/2017/08/17/business/dealbook/alibaba-sales-revenue-first-quarter-profit.html

[9] Louise Lucas, “Alibaba kicks off ambitious plan for frontier-free global trade,” Financial Times, March 22, 2017, https://www.ft.com/content/590d815a-0ec6-11e7-a88c-50ba212dce4d

[10] “Defining the Offset Strategy,” CSIS, October 28, 2016 (at ~39:00), https://www.csis.org/events/assessing-third-offset-strategy

[11] Dan Lamothe, “Pentagon chief overhauls Silicon Valley office, will open similar unit in Boston,” Washington Post, May 11, 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/05/11/pentagon-chief-overhauls-silicon-valley-office-will-open-similar-unit-in-boston/

[12] Charlie Clover, Emily Feng, and Sherry Fei Ju, “China enlists start-ups in high-tech arms race,” Financial Times, July 9, 2017, https://www.ft.com/content/5883d3d2-62cd-11e7-91a7-502f7ee26895

[13] Freedom on the Net 2016, https://freedomhouse.org/report/freedom-net/freedom-net-2016

[14] Rana Foroohar, “Big Tech can no longer be allowed to police itself,” Financial Times, August 27, 2017, https://www.ft.com/content/ce1d6a00-89a0-11e7-bf50-e1c239b45787

[15] Jen Weedon, William Nuland and Alex Stamos, Information Operations and Facebook, April 27, 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

[16] Samuel C. Woolley & Philip N. Howard, “Computational Propaganda Worldwide: Executive Summary.” Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk

[17] Brad Smith, The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#zKiyEOFe1dxIx1zB.99

[18] Andrew Ng, Artificial Intelligence is the New Electricity, Medium, April 28, 2017 https://medium.com/@Synced/artificial-intelligence-is-the-new-electricity-andrew-ng-cc132ea6264

[19] Eshe Nelson, “Why American jobs have a higher risk of automation than jobs in Germany, the UK, and Japan,” Quartz, March 24, 2017, https://qz.com/941163/pwc-study-automation-risk-is-higher-for-american-jobs-than-for-workers-in-germany-the-uk-and-japan/

[20] Natasha Lomas, “AI report fed by DeepMind, Amazon, Uber urges greater access to public sector data sets,” TechCrunch, April 24, 2017, https://techcrunch.com/2017/04/24/ai-report-fed-by-deepmind-amazon-uber-urges-greater-access-to-public-sector-datasets; Tom Simonite, “Algorithms That Learn with Less Data Could Expand AI’s Power,” MIT Technology Review, May 24, 2016, https://www.technologyreview.com/s/601551/algorithms-that-learn-with-less-data-could-expand-ais-power/

ADAM SEGAL is the Ira A. Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations (CFR).

The American Academy in Berlin
Hans Arnhold Center

Am Sandwerder 17–19 · 14109 Berlin · Germany · americanacademy.de

Richard C. Holbrooke Forum
holbrookeforum@americanacademy.de

Design Concept: Carolyn Steinbeck · Gestaltung