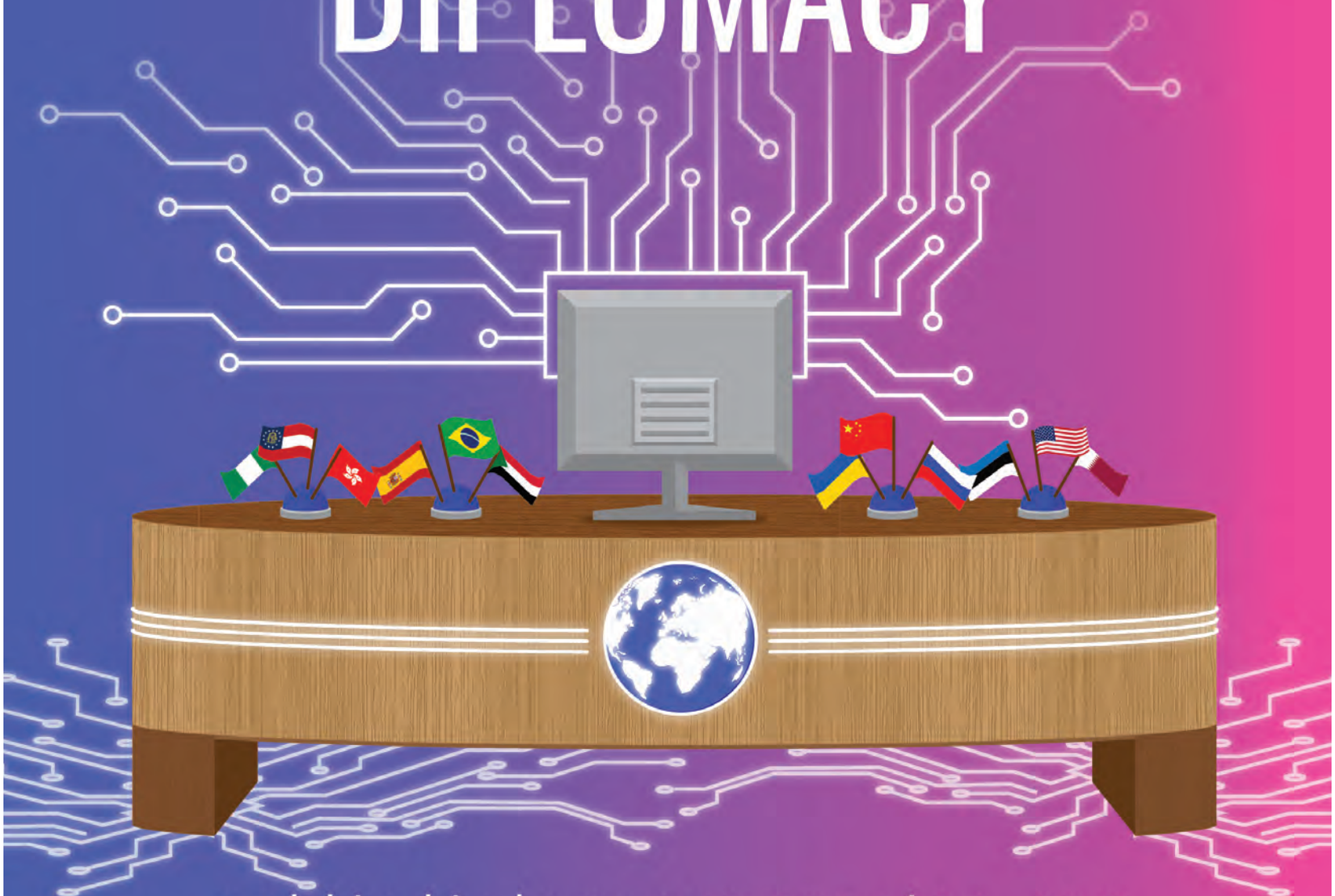
UNIVERSITY OF SOUTHERN CALIFORNIA

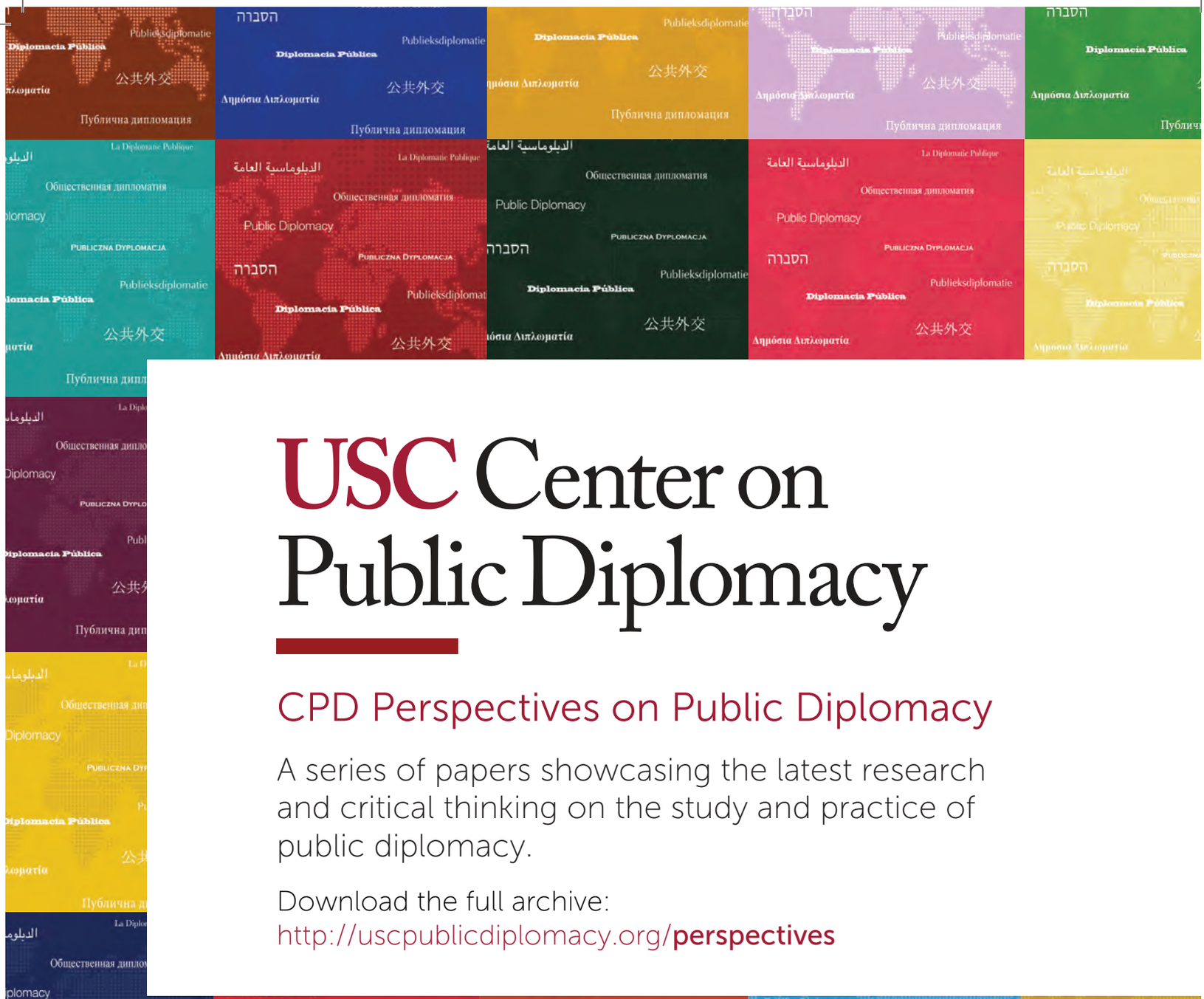
PUBLIC DIPLOMACY MAGAZINE

ISSUE 22 WINTER 2019

CYBER DIPLOMACY



publicdiplomacymagazine.com



USC Center on Public Diplomacy

CPD Perspectives on Public Diplomacy

A series of papers showcasing the latest research and critical thinking on the study and practice of public diplomacy.

Download the full archive:
http://uscpublicdiplomacy.org/**perspectives**

Letter from the Editor

Learn to *lead* in cyber affairs now.

The inspiration for CyberDiplomacy was sparked in Spring 2019 when I was enrolled in a Master of Public Diplomacy course on Hard Power, Soft Power, and Smart Power. In one of our preliminary lectures, Dr. Ernest Wilson III, professor of the course, took an Expo marker and wrote in sprawling letters across the classroom white board: "CYBER SPACE." Afterwards, he turned around and asked our class matter-of-factly: "What is it?" No one in the room had an immediate answer. Our silence was a unanimous consent to our intimidation of the cyber sphere – its vastness was simply overwhelming.

Not wanting to succumb to the fear of the unknown, Dr. Wilson led our class into a deep-dive of the cyber realm. Together, we discovered the great potential and power it contained to help nations better connect with people around the globe. When I realized the importance of extending these conversations beyond our classroom, I decided to dedicate the twenty-second issue of the Public Diplomacy Magazine to gathering what local and international experts had to say about harnessing the power of cyber for nations' greater good.

Our brilliant authors were courageous enough to address cyber issues head-on. Among them are USC students; academics from China, Georgia, Spain, Qatar; the U.S. Department of State's Senior Advisor to the Helsinki Commission; and members of the following think-tanks: Access Now, DiploFoundation, European Institute for International Studies, National Endowment for Democracy's International Forum for Democratic Studies, Pacific Council on International Policy, Oxford Digital Diplomacy Research Group, Simon Wiesenthal Center, and the USC Center on Public Diplomacy.

Nina Hachigian, Los Angeles' first Deputy Mayor of International Affairs, told our class in a meeting later that spring semester, "If you're going to bring a leader bad news, bring solutions." I am proud to say that in every section of our magazine, there are proven policy recommendations coming from expertise in academic, private, and public sectors. While cyber threats like hacking and disinformation may seem insurmountable, our magazine hopes to inspire innovative solutions that will aid future diplomats in enhancing states' cybersecurity and narrative-sharing abilities on the web.

This issue also includes a brand-new Special Features section, "'CYBER HACKS': GETTING AHEAD." Showcased here are other recommended readings, research and career databases, podcasts, courses, web discussions, seminars, and conferences that will guide our readers to a wealth of cyber-diplomacy resources both on and offline.

Our issue concludes with the wise words of Dr. Nicholas J. Cull, founding director of USC's Master of Public Diplomacy Program: old fundamentals are needed now more than ever before. Listening, recognizing our own biases, and admitting to our weaknesses are the guiding principles that Dr. Cull believes will help diplomats to succeed in any age, including a digital world.

I would like to thank our Managing Editor, Devin Villacis, for her great support in assisting me in publishing the 10th-year edition of our magazine this winter. I would also like to acknowledge the dedication of our Editorial Board, Staff Editors, and Staff Writers. This magazine was a true collaborative effort of students who hope to leave you with this final message:

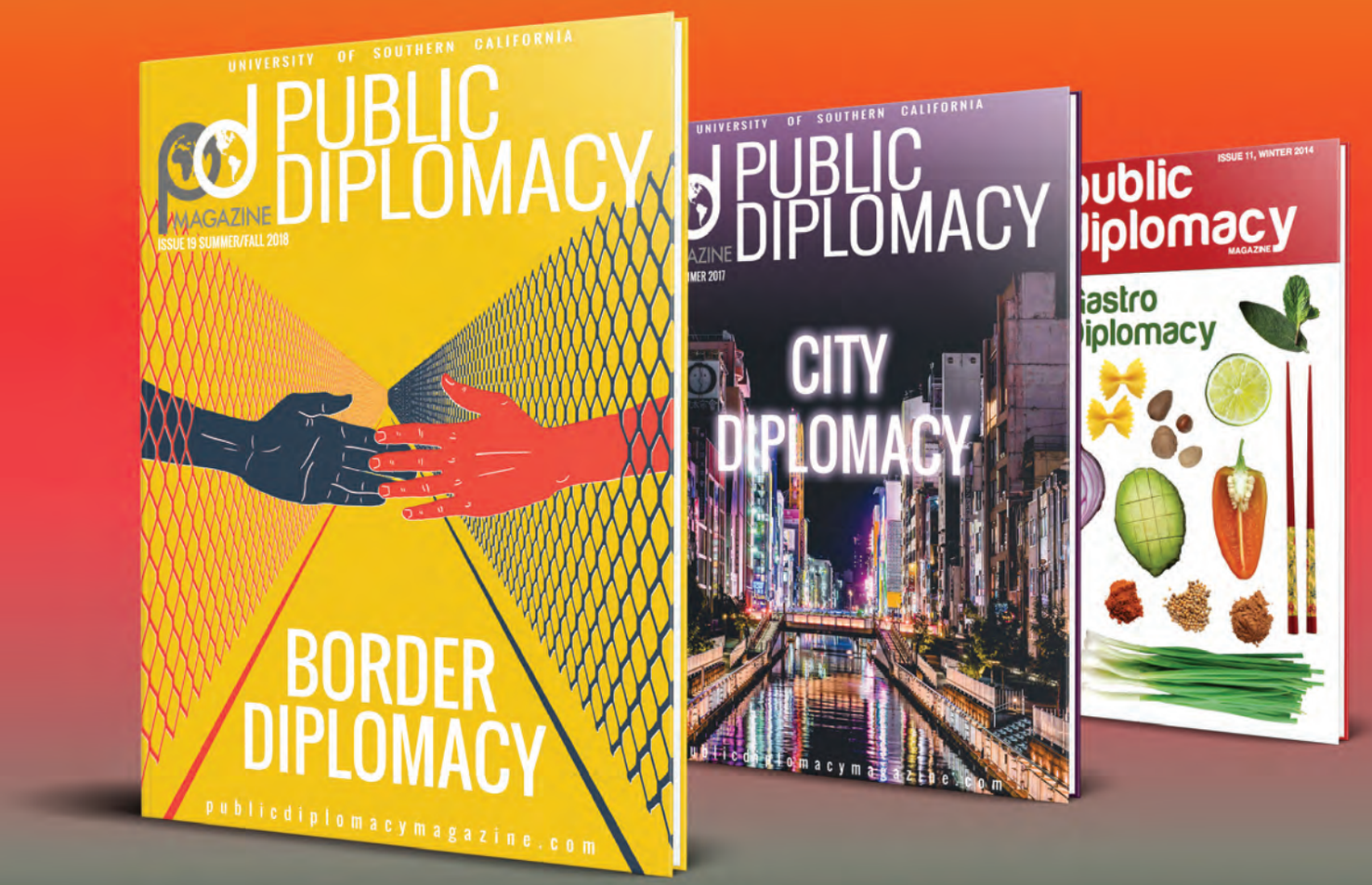
You don't have to be intimidated by cyberspace. Learn to *lead* in cyber affairs now.

Jasmine Kolano
Editor-in-Chief

CELEBRATING 10 YEARS OF

PUBLIC DIPLOMACY MAGAZINE

Beginning Winter 2009, the magazine's unique mission has been to provide a common forum for the views of both scholars and practitioners from around the globe, in order to explore key concepts in the study and practice of public diplomacy.



VISIT

WWW.PUBLICDIPLOMACYMAGAZINE.COM

TO READ PAST ISSUES

SUBSCRIBE

TO BE THE FIRST TO KNOW ABOUT
PD MAGAZINE SUBMISSION AND PUBLICATION DATES

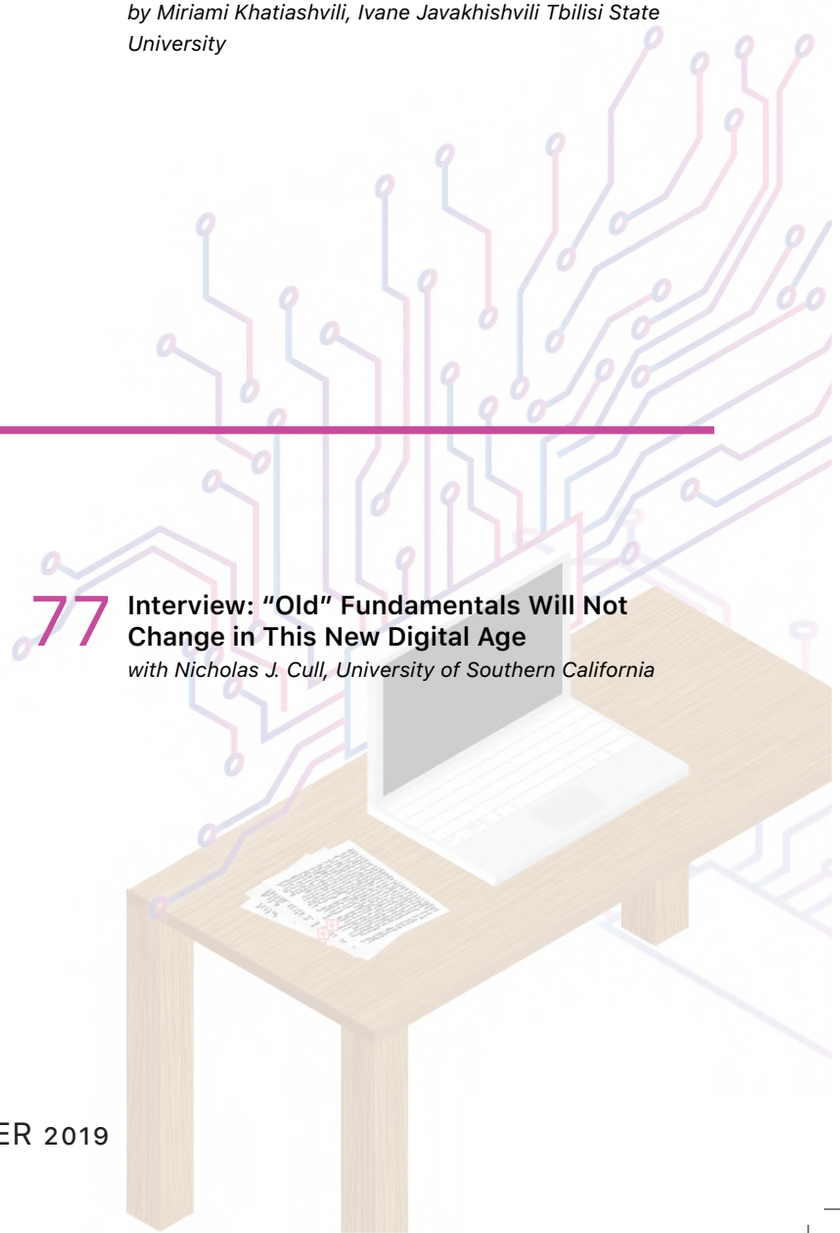
Editorial Board

Table of Contents

1
EQUIPPING DIPLOMATS FOR THE CYBER AGE

2
CYBER-DIPLOMACY'S RISING STARS

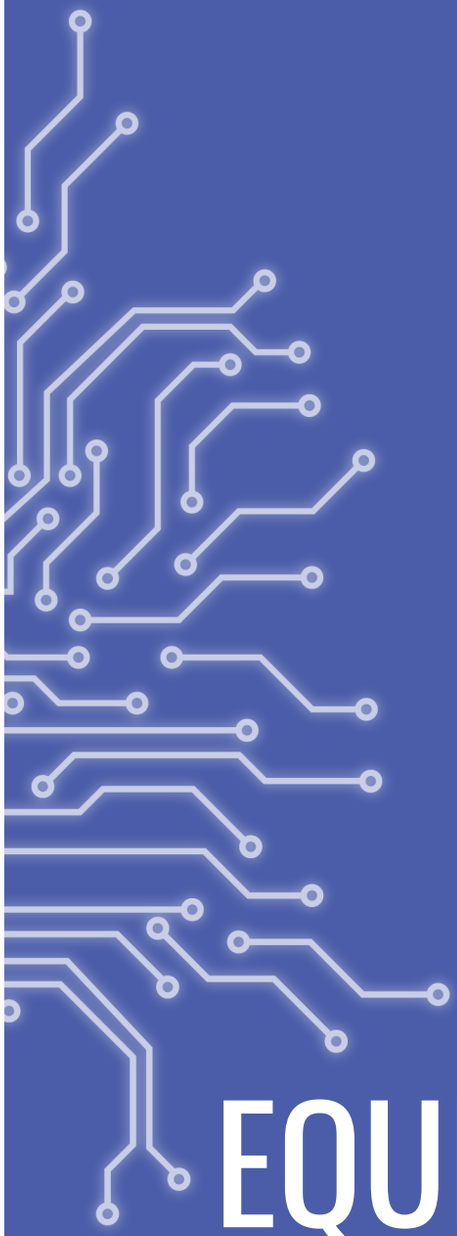
5
PREPARING FOR THE CYBER FUTURE



3
OVERCOMING DISINFORMATION

4
SOCIAL MEDIA: A POWERFUL CYBER ALLY

6
"CYBER HACKS:" GETTING AHEAD



EQUIPPING DIPLOMATS FOR THE CYBER AGE

Cyber-diplomacy: Why Diplomats Need to Get Into Cyberspace

Shaun Riordan

French Prime Minister Clemenceau once argued that war was too serious to leave to soldiers. By the same token, cyberspace is too serious to leave to technicians. And yet that is what we have done. There is a feeling that cyberspace was designed by technicians, therefore technicians should be able to sort out its problems. And yet the main problems in cyberspace, whether in internet governance or cybersecurity, are not technical but human. More specifically they are political and geopolitical. The problems of internet governance are not technical issues about how to manage the internet, but highly political debates about how we manage society and global public goods. The problems of cybersecurity are not technical issues about how to prevent cyber penetrations, but political and geopolitical questions about the motivations of those responsible for the penetrations and about how we can limit what they do.

If digital diplomacy is the application of digital technologies to diplomacy, then cyber-diplomacy is the application of diplomacy to cyberspace. One way of thinking about cyberspace is to focus on the different levels essential to its functioning: the physical (cables, switching stations etc), the logical (the protocols that ensure that data arrives at its destination), the data (the content of webpages, emails, etc) and the social (in which humans and, increasingly, devices interact). All of these levels are political and geopolitical. Deciding whether a not-for-profit private company operating under Californian state law (ICANN) should continue to manage the assignment of domain names, or whether these functions should be brought within an international organisation, reflect political differences about how international society should be organised. The danger that state or non-state actors may seek to disrupt or subvert the physical structures on which the internet operates is a geopolitical risk. Arguments about the protection of data, the contents of web pages, or the behaviour of different actors interacting in cyberspace are both political and geopolitical.

The problems of cybersecurity are not technical issues about how to prevent cyber penetrations, but political and geopolitical questions about the motivations of those responsible for the penetrations and about how we can limit what they do.

The role of the Chinese company Huawei in the roll out of 5G telephone networks illustrates how technical issues can quickly become political and geopolitical. The focus of U.S. arguments against Huawei's participation lie in concerns about security, and the extent to which Huawei may cooperate with Chinese intelligence services in building back doors into 5G technologies. But the more interesting debate is about Huawei's role in setting 5G industrial standards. Until now, the international industrial standards for mobile telephony have been set by companies in the U.S. or its allies. International standards setting meetings were dull affairs, attended only by technicians. No more — in the future, these meetings will become geopolitical battle grounds as countries compete for primacy in new technologies. Without diplomats managing the conflicts, we risk returning to the days of multiple technologies with incompatible standards.

General Hayden, former head of the NSA, once commented that there is no international law in cyberspace. Other governments, especially European

governments, disagree. But what is clear is that international law cannot be applied in its entirety, and without amendment, to cyberspace. Many concepts, such as neutrality or arms control, make no sense in cyberspace in their traditional form. New challenges, such as attribution of cyberattacks or the risk of escalation through unintended consequences arise. The traditional security dilemma is worse in cyberspace because it is almost impossible to distinguish between offensive and defensive operations. A cyber penetration intended to ascertain a rival's capabilities and intentions is impossible to distinguish from one preparing for future cyberattacks. The traditional diplomatic skill of identifying the intentions of rivals becomes even more important.

The key figures in developing international norms of behaviour have traditionally not been international lawyers, but rather diplomats. Writing up international norms with your friends is easy; but to be effective they must be shared by your rivals. It is the diplomats who painstakingly identify the shared preferred outcomes with countries who do not share their values or ideologies, which then become the building blocks for new norms or restraints on international behaviour. The lawyers simply write up the outcome. The same is likely to happen in cyberspace. A series of international rules for cyberspace have been proclaimed among friends, from the Budapest Convention to the Tallinn Manual. But if these are to have wider effect, and if cyberspace is not to become a Hobbesian war of all on all, diplomats will need to identify the preferred outcomes shared with rivals and those who do not share our values. Norms in cyberspace can be built upon these shared outcomes. Shared outcomes might include restrictions on attacking critical civilian infrastructure, rules on cyber retaliation, understandings of what is, and is not, acceptable espionage, or agreements to collaborate on cyber crime.

We so far have seen only one clear example of a cyber attack resulting in permanent physical damage: the so-called Stuxnet attack on the Iranian nuclear programme. But that does not mean it will be the only one. We have seen plenty of disinformation, disruption and espionage operations carried out by state actors, not to mention the plethora of criminal cyber attacks. Technical solutions are necessary but not sufficient. We need diplomats to engage with the geopolitics of cyberspace, and for cyber issues to move to the heart of Foreign Policy.

Shaun Riordan

Shaun Riordan is Director of the Chair for Diplomacy and Cyberspace at the European Institute for International Studies. He is the author of "Cyberdiplomacy: Managing Security and Governance Online" (Polity 2019) and "The Geopolitics of Cyberspace: A Diplomatic Perspective" (Brill 2019).

Exploring the Threats and Opportunities of Cyber Diplomacy at PolicyWest

Justin Chapman

As the world undergoes the Fourth Industrial Revolution, foreign governments and publics are becoming intertwined and interdependent like never before. What does this mean for diplomacy and international relations going forward? What role can public diplomacy play in this evolving dynamic?

Klaus Schwab, founder and executive chairman of the World Economic Forum, first introduced the term "Fourth Industrial Revolution" in a Foreign Affairs article in December 2015. While the Third Industrial Revolution encompasses the digital revolution, the Fourth Industrial Revolution is characterized by "a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres," Schwab wrote.

Those disruptive technologies include the internet of things, virtual and augmented reality, artificial intelligence, robotics, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, energy storage, and quantum computing, among others.

Cybersecurity, the digital revolution, and the evolving roles of Silicon Valley and the U.S. government in national security and technology were all major and recurring themes at the Pacific Council on International Policy's annual global affairs conference, PolicyWest. The event was held on October 4, 2019, in Beverly Hills, California, and featured a keynote discussion on Ukraine, a debate on defense spending, and several panels of experts discussing the most pressing global issues of our time.

Glenn Gerstell, general counsel for the National Security Agency (NSA) and Central Security Service (CSS), delivered a TED-style talk on the Fourth Industrial Revolution. He implored the private sector to work with the U.S. government to help confront the growing cyber threats from the United States' adversaries.

"Is there a danger that we will underestimate and thus not be prepared for the impact of technology? This is an unacceptable risk in the area of national security," he said. "The digital revolution will present many benefits in the way we work, communicate with friends and family, shop, and travel. But it also presents risks and threats to the fundamental duty of government: to keep us safe and secure. We must be able to understand and stay ahead of the technological progress of our adversaries, whether they're other countries, terrorists, or common criminals. This is not an area where we can play catch-

up."

He said technological development is going to alter the balance between the private sector and the federal government in terms of responsibilities and capabilities relevant to national security. This is not just a domestic issue, considering the seemingly unstoppable influence of multinational corporations. Gerstell argued that the private sector has more data, increasingly more social responsibilities, and is directly exposed to the threat posed by a rising China.

Image Courtesy of the Pacific Council on International Policy

Caption: Glenn Gerstell, general counsel for the National Security Agency (NSA) and Central Security Service (CSS), delivered a talk on the Fourth Industrial Revolution at PolicyWest (October 4, 2019)

"For the first time since the United States became a global power, it must now confront an adversary that presents not just a political or military threat, but also a fundamentally economic one," he said. "But in this economic area, the playing field is not even. It's our private sector that will bear the brunt of the effects of a cohesive, competitive China."

He also argued that the cyber world exploits a unique gap in responsibility, and that that responsibility as well as technological capability is shifting from government to the private sector.

In the 20th century, he pointed out, "it was government that led the way in technological development and had the expertise, and it was often the private sector that was trying to learn from it and catch up with government. Now, in many critical areas, that's exactly switched 180 degrees and we see that it's the private sector that has a much greater level of technical capability, is spending billions of dollars on research and development, and has the expertise in key areas."

Perhaps the best way to do that is through new or deeper public-private partnerships in figuring out how to handle data, collaborating to combat cyber malevolence, and confronting China in an integrated way.

He posed the question: How must we adapt to this altered balance to achieve our goal of national security? He called for the "melding together of the relative strengths and positions of the two sectors. Perhaps the best way to do that is through new or deeper public-private partnerships in figuring out how to handle data, collaborating to combat cyber malevolence, and confronting China in an integrated way."

The only way that is possible is if the U.S. government articulates a consistent policy regarding China and communicates that policy to its allies and their publics around the world. Like previous growing adversaries, the United States cannot confront the likes of China and Russia—who are quickly gaining ground in terms of cyber capabilities—on its own. It needs to win the hearts and minds of Europeans, Africans, South Americans, and Central, South, and Southeast Asians, to name a few major players in this sphere. In other words, it needs to change course.

In a disheartening and potentially dangerous trend, the Trump administration has been dismantling existing cybersecurity protections put into place by the Obama administration. According to a recent Axios article, "at least a dozen top or high-level [White House] officials have resigned or been pushed out of a cybersecurity mission that was established under Barack Obama to protect the White House from Russian hacking and other threats."

Because of these advances in technology, public diplomats have unprecedented opportunities to reach a virtually limitless audience around the world.

Not to mention the cybersecurity threats to our elections, only increasing and becoming more sophisticated as we round the bend to 2020. The Trump administration has done virtually nothing to prevent another intrusion into our elections by Russia or anyone else. As American

democracy falters, so too does the image of the United States in the eyes of the world, making the job of the public diplomat that much more difficult and elusive.

At PolicyWest, Antonio Mugica, CEO of Smartmatic, a company that specializes in technology solutions for electronic voting systems, said our society's failure to catch up with election technology is "shameful" and has "caused a lot of confusion." He suggested the United States learn from the small Baltic nation of Estonia, which doubled down on and strengthened financial and election security through technology after a devastating cyber-attack from neighboring Russia in 2007.

The digital revolution will present many benefits in the way we work, communicate with friends and family, shop, and travel. But it also presents risks and threats to the fundamental duty of government: to keep us safe and secure.

During a panel at PolicyWest on the intersection of Silicon Valley and national security, Sarah Sewall, executive vice president of policy at In-Q-Tel, a not-for-profit venture capital firm, said the questions we are facing today about technology combine "the hard security pieces with the human rights and values pieces."

"When we think about the changing nature of power, what undergirds the United States' ability to be a leading power in the globe and a force for good, we're seeing a shift in the sources of that power toward technology," she continued. "Technology is becoming the currency in which power is accrued and exercised. Who is going to be the most innovative and advanced in not just thinking about AI but adopting and using and implementing AI? Who's going to own the biotech revolution, which has the ability to transform everything? Some of the United States' adversaries have the view that this is the race for global leadership and power."

Because of these advances in technology, public diplomats have unprecedented opportunities to reach a virtually limitless audience around the world. But they also need to stay vigilant against the threats posed by technology: facial recognition, deep-fakes, lifelike online bots, machine learning, and automated micro-targeting, to name a few, all have unprecedented pros and terrifying cons.

And they also shouldn't forget the lessons of the past. There are some foundational elements of public diplomacy that reliably work no matter the medium, such as listening and approaching cultural relations in a cooperative, rather than self-interested, manner. The long-lasting impact and reach of soft power should not be underestimated.

There are countless tools for today's public diplomats to utilize in cyberspace in order to articulate U.S. foreign policy objectives to international audiences, strengthen relationships between the American people and publics around the world, and exchange and celebrate diverse cultures. Virtual exchanges, digital broadcasting, and e-sports—in addition to social media and multimedia—are all areas that have a lot of potential for achieving public diplomacy objectives.

But first, the U.S. government must make its own cybersecurity and that of the private sector—as well as U.S. allies—a top priority again.

If the tenor of the discussions at PolicyWest are any indication, we're not there yet.

Justin Chapman

Justin Chapman is the Communications Officer at the Pacific Council on International Policy. He was the youngest elected member of the Altadena Town Council at age 19. He received a Master's degree in Public Diplomacy from the University of Southern California in 2018 and a Bachelor's degree in Mass Communications/ Media Studies from UC Berkeley in 2009. At USC, he served as the editor-in-chief of Public Diplomacy Magazine. He has written for over 20 print and digital publications, frequently for the Pasadena Weekly. His book about his travels through Africa, Saturnalia: Traveling from Cape Town to Kampala in Search of an African Utopia, was published by Rare Bird Books in January 2015. As a professional child actor, he performed in dozens of commercials, television shows, and movies.

If You Can't Beat Them, Join Them:

The Story of Hackers as Non-State Actors Affecting Geo-Politics

Sanya Budhiraja

The onset of hyper-globalization and heavy diffusion of information technologies into society has changed the manner in which the mass-public is incorporated in wider power structures. 'Power' may still be accumulated by political aristocracies at the very top of the global pyramid, but those closer to the base now have more say in how it is exerted upon their daily lives. There is possibly no better example of non-state actors who affect global security and the sanctity of governing bodies than 'hackers.'

Hackers are people with a deep knowledge and a thorough understanding of computer hardware, software, and network interactions. They might 'hack' i.e. gain illegal access to a computer system[s] for multiple reasons, such as curiosity, economic gain, political agenda, technological challenge or even pure boredom (Sigholm, 2016, pp 15).

These actors possess is 'cyberpower' i.e. the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain (Nye, 2010). Cyberpower exists inside 'cyberspace' but can be used to produce favorable results both within that space and other domains, using cyber instruments.

Cyberspace itself, can be understood as an operational domain wherein interconnected systems and their associated infrastructure are used to exploit information (Nye, 2015). There isn't one homogeneous global 'cyberspace' but many 'cyberspaces' (Kern, 2015, pp 89). These cyberspaces have become new battlegrounds wherein 'cyberattacks' can be carried out for political or military gain by state or non-state actors (often on the nation's behalf) by employing cyberpower capabilities (Sigholm, 2016, pp 6).

Operating in cyberspace gives state and non-state actors distinct advantages that are lacking when exploiting other geographical resources. These include low barriers to entry and anonymity. These unique features make it possible for smaller actors to exercise more power in cyberspace than in more traditional domains of world politics; an epitome of 21st-century global politics which is marked by the democratization of power (Nye, 2010).

Hackers are usually classified, by the intent of their actions, as: 'white hat,' 'black hat' or 'grey hat.'

White hat hackers, also known as ethical hackers, are usually employed by governments and companies for functions of information security as they specialise in penetration testing. These individuals alert external actors of vulnerabilities in their software and advice on possible solutions (Sigholm, 2016, pp 16).

Black hat hackers, on the other hand, partake in cyberspace operations, called 'cyberactions,' which are only executed for personal gain. According to former National Reconnaissance official Mike Theis, any attack that would be committed in the real world has a virtual equivalent (Tennant, April 2009). For instance, a black-hat hackers could cyber-blackmail a victim by extorting money or demanding other benefits in return for not disclosing damaging information about an actor[s] found in cyberspace. The perpetrator could also install a back door or 'loader' on a machine and then sell it to the highest bidder. This crime, called 'cyberslaving,' allows the buyer to then install any software on that machine without detection (Tennant, April 2009).

Grey hat hackers are somewhere in the middle. Their functions are mostly motivated by ethical reasoning of cybersecurity improvement for external actors, but the method employed may be deemed illegal (Sigholm, 2016, pp 16).

A subgroup of hackers who commonly have a linear intent but can wear different colored hats based on particular operations are known as 'patriot hackers.' As their name may suggest, the main motivation of patriot hackers is to aid or support their own government in an ongoing conflict or war (Sigholm, 2016, pp 16). Some critics, argue that this subcategory should no longer be classified as a "non-state actors" as most such individuals have been pursued by the state to function as decentralized network actors in its greater cyberpower strategy (Tennant, April 2009).

Given that cyberspaces are connected through networks, hackers are able to exert their influence both locally and globally. 'Intra-state' hacking influences functions within a nation-state's borders for/or against its government and/or its citizens while the 'inter-state' hacking influences affect hard and soft power capabilities of an actor[s] on the international stage.

'Inter-state' hacking can increase hard power proficiencies of states if they establish a strong relationship with their 'hacker' population and utilize these actors as decentralized nodes for cyberattacks. This gives the state benefit of 'plausible deniability' (Sigholm, 2016, pp 24). The 'North Korea hacks Sony' scandal is an example of 'patriot hackers,' called 'Guardians of Peace,' working in favor of the government. The group hacked servers at Sony Pictures Entertainment's headquarters causing damage worth $15 million because they were offended by Kim Jong-un's representation in 'The Interview' (Barrett, Sept 2018).

Since it is legally difficult to find evidence and build a case against the nation on behalf of said actors, the country often faces very minimal repercussions for these operations. Additionally, through cyberspace and 'patriot hackers,' a nation-state, like North Korea, which has particularly weak physical world presence, has a chance to exert itself as 'dominant' player in current geopolitics.

On the other hand, if a nation-state is oblivious to international hacker operations, its cybersecurity strategy may fail to guard critical information as hacking techniques evolve as quickly as protection technologies.

Similarly, on an 'Intra-state' level, hackers can increase or decrease nation-states hard power capabilities depending on how intricately their capabilities and operations are ingrained into the government's cybersecurity initiatives. If the government is vigilant about hacking operations, it can take preventative measures such as involving 'white-hat' hackers to test the cybersecurity system for breaches. For example, the

U.S. Department of Defense launched a program called 'Hack the Pentagon' which later extended to 'Hack the Army' and 'Hack the Air Force' that ended up rewarding $300,000 in total to bounty hunters who discovered any by vulnerabilities in the system (Bergal, May 2018).

On the other hand, a cybersecurity plan that ignores hackers can leave the state unprepared for 'black and grey hat' hacker attacks. An example of this is the recent publication of files containing personal information of thousands of federal agents and law enforcement officers by a hacker group that exploited flaws on the FBI's chapter website to download the content of each web server. The group, motivated by experience and money (Whittaker, April 2019), has remained unidentifiable until now and is said to have hacked more than 1,000 sites. The data is now being structured to be sold.

With regards to soft-power, hackers can either improve or worsen foreign players' attraction to a state based on the classification and proficiency of the state's hacker[s]. Israel is an example of a nation that has become known as a cybersecurity power-hub after the country appropriately began recruiting hackers from their teenage years, and funneling them into the army's 'Elite Cyberwarfare Units' (Awad, May 2018). These 'white hat hackers' are usually trained to create cyber offense and defense technology and later go on to join private sector companies that specialize in cybersecurity. Israel is able to capitalize on the talents of its hacker population to position itself as an attractive ally to other nation-states, as well as, a foreign investment center to private companies.

Rather than create an enemy of its local hacker population, which a country then must spend resources to defend against, states should try to form partnerships with national hackers that could ultimately help protect the state against future national and international hacks.

Israeli hackers have also initiated cyberattacks on enemy states through illegal activities, most famously the 'Stuxnet Virus' (2010) which was created by unidentified American and Israeli engineers to damage Iranian nuclear development. Careful coding allowed both the nations to abdicate responsibility for the attacks. It wasn't until 2013 that proof became available implicating the US and Israel in the creation of this worm, but even then legal irregularities made it difficult to construct a concrete case against the nations.

Involving hackers in national initiatives can, however, have a detrimental effect on a nation-state's soft power if they are openly used for cyberattacks on other states. For instance, a Russian hacker group that called itself 'Fancy Bear' hacked the 'World Anti-Doping Agency' after Russian athletes were banned from Olympic and Paralympic games due to illegal drug use. The hack, mostly acknowledged as a revenge plot, published UK and US athletes' (so far legal) drug use and severely damaged Russian national character when the government publicly condoned the attack (Vincent, 2017, pp 10).

In both cases, Russia and Israel used 'patriot hackers' with the intention of strengthening national cybersecurity. These hackers used nefarious and illegal methods in the name of national security. But the Russian government damaged its reputation, reducing its soft power on the global stage, by disclosing their associations. Essentially hackers who are discreetly integrated into the states cybersecurity strategy can help increase or maintain a nation's soft power, but evident collusion between states and hacker groups, especially associations with cyberattacks, can damage a nation-state's position on the global front.

On an 'intra-state' level hacker groups functioning as 'hacktivists' can also reduce a nation-state's soft power capabilities. 'Hacktivism' is electronic civil disobedience which uses hacking techniques to disrupt a target's network for a particular cause (Sigholm, 2016, pp 14). Such incidences are usually reported heavily in the media bringing publicity to both the hacktivist[s] and their cause. Hacktivism negatively affects a nation-state's soft power as it brings to the forefront the discontent of citizens with their government. If 'soft power' is measured by how attractive a nation-state is to national or international actors, cyber expression of dissatisfaction with the government or its policies can greatly affect the potential it has to rally support for future policy initiatives. An example of this is the reduction in soft power that came right after Snowden Leaks, which revealed surveillance operations undertaken by national governments of countries such as the US and UK and resulted in great local mistrust in political power[s] at the time.

Additionally, hacktivism can increase a nation-states soft power on the international front if it is done for the purposes of human rights protection. An example of this is American interference with the Chinese Firewall so as to promote free flow of information regarding human rights violation.

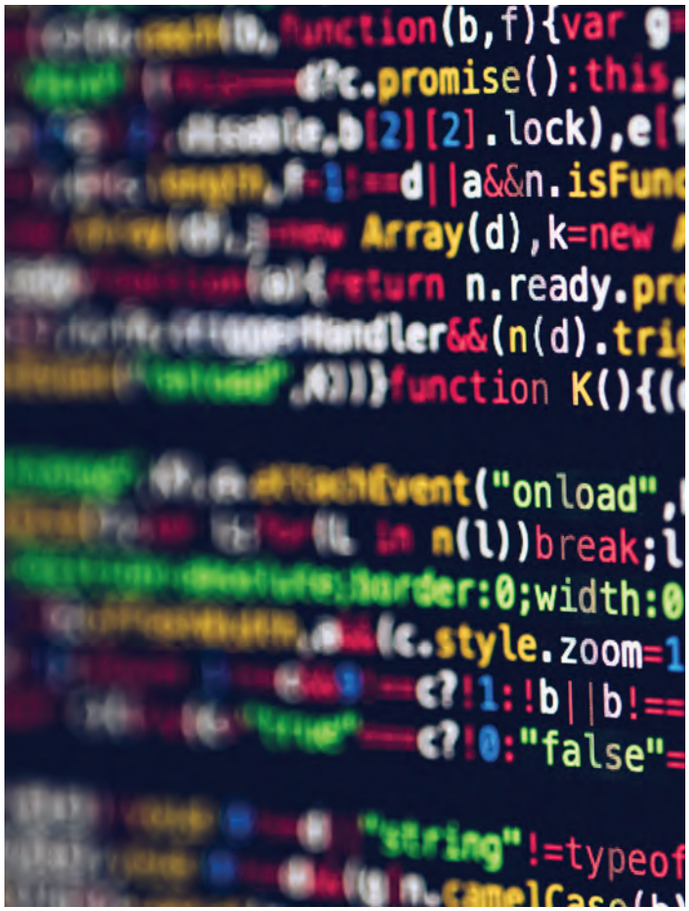
On a policy level, then, it is important to recognize that nation-states are still central players in the field of power

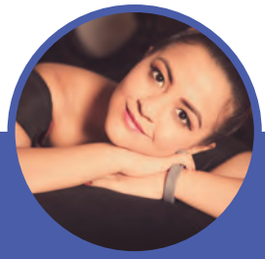
politics. Though now smaller national and transnational actors are also able to mobilize cyberpower to influence the network because of low barriers to entry and anonymity associated with cyberpower (Sheldon, 2011). Technological evolutions that have helped in diffusion of power are unlikely to change direction in the future to a more centralized network; this means that nation-states should consider NSAs carefully in any subsequent cybersecurity strategy.

States would benefit by incorporating fresh perspectives towards ancient cyber strategies through new cyber policies. Other benefits of new cyber strategies to governments include, plausible deniability, legal uncertainties and the possibility of rapid attack by proxy (Yang, March 2018). Plus, as with China, if a nation's hacker population shares a cordial relationship with the government it is unlikely to go against it to damage the nation's hard or soft power capabilities (Yang, March 2018).

Rather than create an enemy of its local hacker population, which a country then must spend resources to defend against, states should try to form partnerships with national hackers that could ultimately help protect the state against future national and international hacks. Some strategies that have been used to begin forming this sort of partnership have included: hacking competitions into government security systems for monetary rewards, and consultation workshops with government officials that help improve vulnerabilities identified.

These partnerships should be kept private from other international actors if the government hopes to benefit from 'plausible deniability.' It is important to be critical of what such a relationship would mean for both the parties involved. In particular, nation-states must be vigilant of certain drawbacks of incorporating hackers in their cyber security operations, such as no direct control over the non-state actors, risk of unintended collateral damage, escalation of operations to a full-blown warfare and, probably the most important, backlash from the international community, which can lead to a reduction in soft power.





Sanya Budhiraja

Sanya Budhiraja is a double master's graduate from the MSc/MA Global Media and Communications program between the London School of Economics and Political Science and the University of Southern California. Before beginning her master's education, she studied Journalism at Cardiff University in the UK. Her interests range from international policy to news media. She was written both a dissertation and white-paper on reconciliation in Bosnia and Herzegovina as a post-conflict society. She hopes to further contribute to enticing discussions about appropriate global development and the role international news media can play in it throughout her career.

Training Diplomats For An AI-Driven Future

An Interview with Dr. Katharina E. Höne and Dr. Tereza Horejsova of DiploFoundation

Interview by Nikki Burnett

Similar to how its technological predecessors have previously disrupted economies, communications, and ways of life, artificial intelligence (AI) is poised to transform the world, and governments are taking notice.

Since 2017, more than 20 governments have put forward national strategies outlining how they plan to play a role in AI's growth. These plans have touched on a range of approaches.[1] Canada, the first to issue a national plan, wants to expand research and cultivate talent; India intends to use AI to improve social inclusion through an #AIforAll strategy; and Denmark hopes to drive business growth and wealth by investing in AI, big data, and the Internet of Things. In February 2019, an Executive Order issued by the U.S. White House prioritized AI dominance, writing that American leadership in AI is of "paramount importance."

With governments around the world embarking on this new frontier of strategic planning, AI's impact is sure to be felt among the diplomats who represent their countries' strategic interests. Although we more frequently hear about the impact of technological development on industries such as manufacturing and consumer technology, AI also has the potential to impact diplomatic practice.

As a Graduate Student Fellow with USC's Center on Public Diplomacy (CPD), I traveled to Brussels, Belgium early in 2019 to attend "DiploCamp," an annual Digital Diplomacy Camp by the Dutch Ministry of Foreign Affairs.[2] There, I attended a session organized by DiploFoundation (Diplo), a non-profit created by the governments of Malta and Switzerland. The session raised an increasingly important question in the field of diplomacy: how much should diplomats know about AI?

Diplo has sought to address this question and a few months prior, it had launched its AI Lab, a "multifaceted initiative that includes research and analysis on AI policy, capacity development in the field of AI and related areas, reports from main events and discussions on AI, analysis into the impact of AI on diplomacy, and much more."[3] Since its launch, the AI Lab has produced a comprehensive report commissioned by the Ministry for Foreign Affairs of Finland and initiated a new online course to educate diplomats, policymakers, and more.[4]

Diplo has sought to address this question and a few months prior, it had launched its AI Lab, a "multifaceted initiative that includes research and analysis on AI policy, capacity development in the field of AI and related areas, reports from main events and discussions on AI, analysis into the impact of AI on diplomacy, and much more."

Nearly a year after DiploCamp 2019, I caught up with Dr. Katharina E. Höne, a senior lecturer, researcher and project manager with Diplo, and Dr. Tereza Horejsova, project development director with Diplo, to discuss the AI Lab's work and outlook on AI and diplomacy.

Nikki Burnett (NB): DiploFoundation was established by the governments of Switzerland and Malta. What led to this partnership? Can you speak to how the Foundation works to increase the role of small and developing states on the world stage?

Dr. Katharina E. Höne and Dr. Tereza Horejsova (KH and TH): At Diplo, we focus a big part of our work on training and capacity development for diplomats from developing countries. We focus on two aspects: traditional topics of diplomatic practice—such as multilateral diplomacy, economic diplomacy, and negotiation skills—as well as topics at the intersection of diplomacy and new technology. Regarding the second category, some of the most important topics covered by us include Internet governance and digital policy, cybersecurity, e-commerce, and of course, artificial intelligence. We reach a lot of people through our highly-interactive online courses which focuses on collaborative learning. A typical course has no more than 25 participants, which are in daily interaction with the lecturers and the course team. While we recognize the importance of online training, we also emphasize the need for broader capacity development approaches. These combine an online training phase, a policy research phase, and an in-situ policy immersion phase.

The Swiss-Maltese partnership was a result of coincidences which opened the way for going forward from a project idea—providing online learning for diplomats and looking at the intersection of diplomacy and technology—to a full-fledged organization, working on issues that were of close relevance for governments of both of these countries.

NB: September marked the one year anniversary of the launch of the AI Lab. What have been the Lab's most exciting achievements in the past year? What are you looking forward to in the future?

(KH and TH): A lot has been going and it is a challenge to summarize everything. Let me highlight four examples. First, with support from the Finnish Ministry for Foreign Affairs, we completed a study on "Mapping AI's challenges and opportunities for the conduct of diplomacy," which we published in January.[5] Here, we broadly map the relationship between AI and diplomacy and add concrete recommendations for ministries of foreign affairs (MFAs). In the months following the publication of the report, we briefed various MFAs and diplomatic communities in Brussels, Washington D.C., Ottawa, Helsinki, Barcelona, Berlin, Vienna, and Geneva. The dialogues we entered on these occasions were crucial to put our findings in context and get a sense of the needs and questions of practitioners.

> "Last but not least, we are currently finalizing research on the potential use and impact of AI applications in the context of international conflict mediation."

Second, building on this, we developed a 10-week, highly interactive online course on Artificial Intelligence: Technology, Governance, and Policy Frameworks.[6] We launched this course for the first time in May and, due to a high-level of interest, are currently offering it again and have plans to make a regular course that can be taken as part of our Master or Postgraduate Diploma in Contemporary Diplomacy.

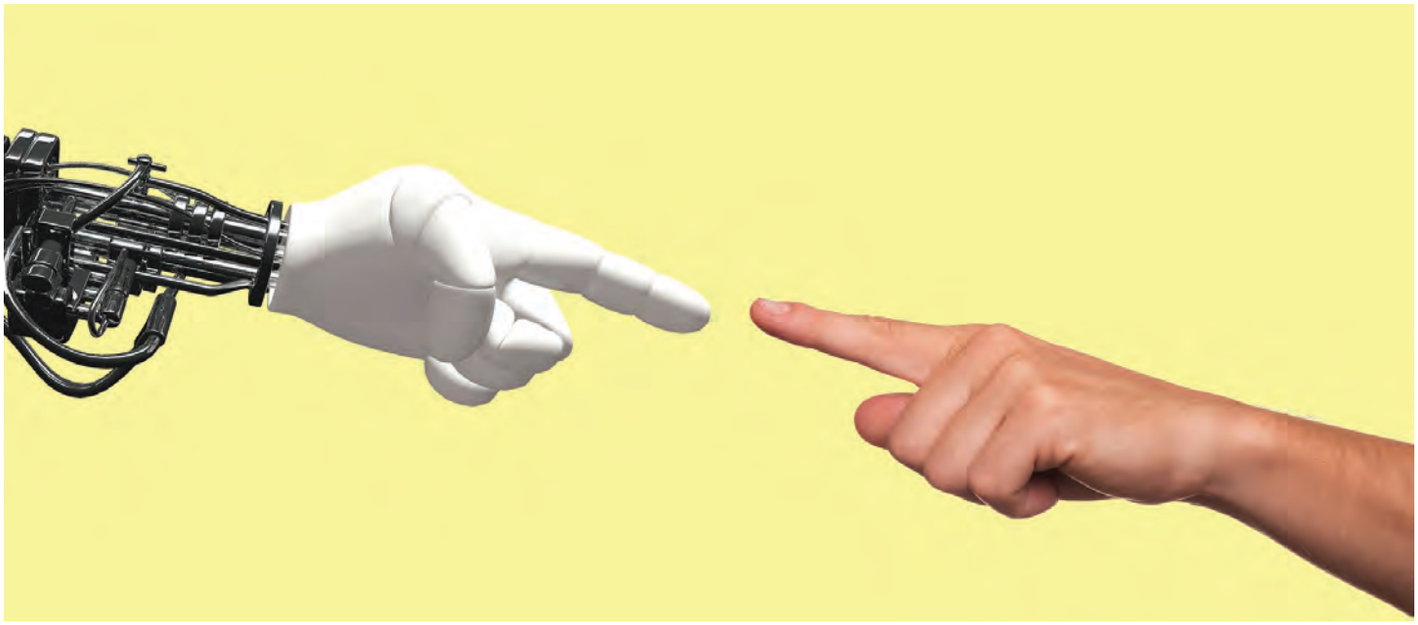
Third, we used our research to contribute to the consultations towards the Maltese AI strategy which was published in October.[7] Last but not least, we are currently finalizing research on the potential use and impact of AI applications in the context of international conflict mediation. This comes under the broad term #CyberMediation, which looks at the impact of new technology on mediation processes. We work as part of a consortium of organizations, including the UN Department of Political Affairs, the Centre for Humanitarian Dialogue, and swisspeace.

Underlying all of this is the work of our Data Team, which is based in Belgrade. Our colleagues there explore various AI applications, which, in turn, informs our approach to AI research. They, for example, gave advice on how to interact with technological companies when looking for off-the-shelf or custom AI solutions in the area of sentiment analysis. They also explore, in a very practical way, some of these tools in order to map the global conversation on AI. As part of this, they worked with Microsoft Azure, Open Calais, and IBM Watson to explore the potential of these tools for key topics in diplomatic practice. Currently, our data team is monitoring the media reporting on AI (for the time period 2017-2019) from over 100 English-language media sources. By the end of 2019, we'll have analyzed over ten thousand news articles and the results will be published in early 2020.

> "Last but not least, one of the most important soft skills to cultivate is probably the art of listening."

NB: The report you mentioned, "Mapping AI's challenges and opportunities for the conduct of diplomacy," situates AI as topic relevant to diplomacy, a tool for diplomatic practice, and a factor that alters the environment within which diplomacy is conducted. What are some of the ways you have seen diplomats start to use AI-powered tools in their day-to-day jobs?

(KH and TH): While some MFAs and other foreign policy actors have begun to explore AI applications for their work, it is important to stress that is not part of their day-to-day practice. The tools we have seen are either



still in the exploration phase or are explored as part of dedicated units such as the Open Source Unit in the UK Foreign Office. It is also important to be aware of that AI is an umbrella term. We have seen examples where social media is analyzed to better understand sentiments at home and abroad and to identify opinion leaders. Similarly, there are examples of automated media analysis to keep up to date in a crisis situation. Humanitarian organizations have started to engage with automated analysis of satellite images. We have also heard of examples of developing chatbots to offer a first point of contact in consular matters. Last but not least, there are nascent developments to have AI-powered assistance that can help with specific elements of research in preparation for negotiations, such as rules of origin in trade negotiations.

NB: While at the annual Digital Diplomacy Camp ("Diplocamp") in Brussels in February 2019, Diplo led a discussion on AI and diplomacy, including to what extent diplomats should understand artificial intelligence. How has this discussion evolved since earlier this year? Have you observed any patterns in what diplomats want to know about AI?

(KH and TH): At the moment, there is a lot of focus on national AI strategies. We saw the first strategies emerge in 2017 and a number of countries are currently trying to catch up. So, the analysis of these strategies is a key area of interest.

Related to this are concerns about "a race for AI" between the U.S. and China and the geopolitical implications for other countries. There are concerns about a new Cold War. A number of countries wonder how to position themselves in relation to the U.S. and China. The EU, for example, focuses on being a leader in developing norms around the ethical use of AI.

Diplomats from developing countries tend to raise concerns about the potential for a widening gap between developed and developing countries due to AI applications and the automation of many industrial processes. There are also concerns about the lack of capacities to develop national AI strategies that are specific to the country context. Further, questions around data ownership and who gets to profit from data are also raised in debates with diplomats from developing countries.

Last but not least, diplomats based in Geneva will be very quick to point to discussions about Lethal Autonomous Weapons Systems of the Group of Governmental Experts of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons.

NB: Many of Public Diplomacy Magazine's readers are current students, and many are aspiring diplomats. As part of an organization that trains diplomats, do you have any advice on how we can prepare ourselves for the evolving field of diplomacy?

(KH and TH): The traditional diplomat is a generalist. So, it is useful to develop the outlook of a generalist and cultivate a number of interests, ranging from the arts to the sciences. For traditional and "new diplomats" alike, a good knowledge of international relations and multilateral institutions is of course essential. Similarly, a good diplomat will be attuned to the use of language and how to skillfully use language to create common ground. For us, as an organization that works at the intersection of diplomacy and new technology, it is crucial to stress that especially young diplomats need to pay close attention to how new technology—be it

social media or fake news—are impacting the topics on the diplomatic agenda, changing the tools at the disposal of diplomats, and causing geopolitical shifts. Last but not least, one of the most important soft skills to cultivate is probably the art of listening. In a fast-paced world that seems to be increasingly dominated by aggressive rhetoric, we need good listeners that are able to overcome perceived differences and find common ground wherever it presents itself.

Katharina (Kat) E. Höne

Dr. Katharina (Kat) E. Höne is a senior lecturer, researcher, and project manager with DiploFoundation, a non-profit foundation established by the governments of Malta and Switzerland that works to increase the role of small and developing states.

She researches, writes and teaches on a number of issues in the area of diplomacy, global governance, and the impact of technology on international relations. Over the last few years, she has focused on research at the intersection of diplomacy and technology. In addition, she has more than ten years of experience delivering in-situ, blended and online training to diplomatic practitioners. Kat holds an MA in Diplomatic Studies (University of Leicester, UK) and a PhD in International Politics (University of Aberystwyth, UK). In her work, she is driven by her aim to level the playing field at international negotiation tables through capacity development, and to provide out-of-the-box thinking and inspiration by drawing on her passion for science-fiction.

Tereza Horejsova

Dr. Tereza Horejsova is Project Development Director with DiploFoundation. Originally from the Czech Republic, Dr Tereza Horejsova is currently based in Washington, D.C., serving as Director of Project Development for DiploFoundation and Executive Director of Diplo U.S. Joining Diplo in 2012, Tereza has had an international career in academia and the non-governmental sector in the Czech Republic, the United Arab Emirates, and Switzerland. During her stay in Geneva (2012–2016), she coordinated the activities of the Geneva Internet Platform. She holds an MA in International Area Studies and a PhD in European Studies, both from the Charles University in Prague. Tereza has conceptualized and coordinated numerous global and regional projects in digital policy capacity development.

Nikki Burnett

Nikki Burnett is a master's candidate in USC's Public Diplomacy program ('20) and a Graduate Student Fellow for Public Diplomacy with USC's Center on Public Diplomacy (CPD). She holds a B.A. in international relations from American University in Washington, D.C.

When High-Tech Is Not Enough

Why soft power is critical for the U.S. to maintain a free and open internet

Jasmine Kolano

Author and social commentator Frank Furedi observed this of authority: "Historically, authority depends on the capacity of certain people to gain the voluntary obedience of people to their commands and beliefs."[1] The crux of Furedi's definition of authority lies in the word *voluntary*. In effect, Furedi was talking about soft power, a state's ability to wield influence over foreign publics without the use of coercion by force or persuasion, two symptoms that political theorist Hannah Arendt suggests are telling of a state's *non-authoritativeness*.[2]

Soft power, a term coined by Joseph Nye, has been the subject of growing critical study since the 1980s, with think tanks converging to produce annual reports measuring the attraction-ratings of nations around the world. The Soft Power 30 Index is the culmination of their findings, ranking countries based on the following 6 objective indices: Government, Culture, Global Engagement, Education, Digital, and Enterprise.[3] In their annual 2018 report, the United States was ranked 4th globally in soft power, a "downward mover" that had fallen from its no. 1 position in 2016. This is not surprising considering that the U.S. has recently had difficulty re-establishing itself as an authoritative voice amidst a global citizenry suspicious of its power – namely its Chinese assailants.

Although the U.S. ranked first in the 2018 Soft Power 30 digital sub-index, China has long been critical of the U.S., especially of American policies aimed at preserving an open cyber world.[4] China has regarded Facebook chief executive Mark Zuckerberg's vision of "making the world a more open place" as dangerous and impractical, arguing that an unregulated internet space could lead to a rise in terrorist activities, violent separatist movements, and encourage a plethora of other destabilizing forces that could mobilize public support online.[5] China has a pool of cases they can reference for arguments' sake, the most recent being the 2018 Facebook and Cambridge Analytica scandal in which Facebook was accused of partnering with the British consulting firm to sell American users' personal data to Cambridge Analytica's political clients, skewing election results.[6]

The Chinese Communist Party (CCP)'s response has been to block U.S. social media sites and promote China's social media platforms (WeChat, Sina Weibo, Tencent QQ) operated by tech-monopolies like Tencent and Baidu. Unbeknownst to many Chinese netizens, however, these platforms are heavily regulated by the central government; users' data are continuously collected by the CCP to form algorithms that teach artificial-intelligence (AI) systems the patterns of human processes. These systems are used to predict individual behaviors for commercial and even malicious purposes. Hundreds of millions of Chinese have already been exploited of their basic human rights to privacy in the process.[7]

Such heavy-handed internet regulation does not remain confined within China's borders. Because of China's economic investment in neighboring countries in Central Asia as well as in the Middle East and Africa, China has exported its internet-regulatory practices to other states as well. As beneficiaries of China's Belt and Road Initiative, states like Pakistan have curbed their own citizens' internet freedoms in the name of subscribing to China's closed-internet policy that keeps out 'exploitive' Western ideology and asserts regional hegemony.

The U.S. has long attempted to curb China's influence in the cyber realm, especially when China's closed internet policies have resulted in harsh censorship rules that have victimized vulnerable Chinese minority ethnic groups like the Uyghurs. Such crises have "created a demand for authoritative solutions" that negate the employment of harder power tactics like war.[8]

While the U.S. has long been attractive to other nations because of its technological prowess, its ability to be an authoritative voice on cyber issues has weakened because of its failure to protect its own users' privacy. This has resulted in a decrease of American soft power and an increased support for closed-internet policies that dominate the current cyber sphere. Now that China is attempting to be the world's authority on the internet and data privacy, the U.S. can gain an edge on its competitors by demonstrating to foreign publics that an open internet is far better than the alternative proposed by the CCP.

Then and only then can the U.S. begin to effectively advocate for the protection of netizens beyond its own borders.

Part I: Reforming U.S. Federal Regulation of Tech

The U.S. has a moral obligation to protect American citizens' "human rights and fundamental freedoms."[9] Furthermore, as a modern democratic state, it is under contract to grant its citizens their "right to privacy" as outlined by the The International Covenant on Civil and Political Rights (ICCPR).[10] However, in today's rapidly growing cyber world, the U.S. still lacks a relevant legal framework to protect those rights, resulting in the following infringements on U.S. netizens when individual personal data is collected:[11]

- lack of individual consent
- lack of transparency
- lack of adequate restraints
- lack of anonymity
- misuse of data, resulting in the priority of corporate rather than individual interests

U.S. corporations have been able to largely evade punitive measures for these unethical practices because of a lack of accountability. DiploFoundation (2019) cited a study by UC Berkeley which found companies that owned devices tracking users' daily activities i.e., miles walked, hours slept, etc. could sell information to "the open market" that could be used by "employers, mortgage lenders, credit card companies and others" to discriminate against vulnerable populations i.e., pregnant or disabled individuals.[12]

The Federal Trade Commission (FTC) is the federally chartered agency responsible for protecting American consumers from such unlawful business practices; however, many of its rules predate the founding of modern tech giants like Facebook, resulting in the inability of the FTC to successfully regulate the cyber realm.[13] This "massive knowledge gap" became apparent in the 2018 Senate Commerce Committee's hearings of Mark Zuckerberg who appeared before senate and judiciary committees in Washington to discuss the recent data infringements purported to be incited by his social network.[14] Federal leaders at the hearings demonstrated a lack of understanding with regards to how modern tech companies operate, causing leaders like Zuckerberg to fall back on on self-regulatory practices.[15]

Thus, the first critical step towards reforming the FTC would be to overhaul its outdated regulations and replace them with the relevant terminology needed to correct tech firms' five common-place infringements on U.S. netizen's data privacy rights. Then, with the EU's General Data Protection Regulation (GDPR)[16] serving as a guide, the U.S. should adopt standards that compel American tech firms and their AI models to "meet the tests" of legality, proportionality, and necessity.[17]

In order for American tech firms to meet the tests of legality, proportionality, and necessity, they should first be required to meet the basic criteria of mutual consent and transparency. To acquire any data legally, firms should ask users for permission to collect private information and provide a sufficient statement of purpose. Next, tech firms should adhere to the legal limits of data collection. The amount of data collected on an individual should not exceed proportions that would endanger his or her preferred anonymity; as it is in the U.S., 87% of the population today can be uniquely identified by a simple "cross-reference of their zip code, gender, and date of birth."[18] This 'de-anonymization' of data is dangerous because it creates increased opportunities for identity theft.[19] Finally, tech firms should prove that data collections are necessary for causes that meet "pressing social needs."[20] Data harvested only for the benefit of the corporation(s) involved are not sufficient grounds for its gathering and should thereby be subject to FTC scrutiny.

Part II: Changing U.S. Tech Company Culture

The previous section established that the U.S. government's first priority is to protect its citizens by regulating corporations collecting personal data. This section proposes that the U.S. government should take one step further and enforce a comprehensive reform of major American tech company culture.

As of late, U.S. major tech companies have placed a disproportionate priority on expanding its customer base and increasing revenues from selling user information. This has resulted in 91% of Americans "strongly agree[ing] that consumers have lost control

of how personal information is collected and used by companies."[21] In addition to these grievances, companies like Apple, Microsoft, and LinkedIn have compromised on their original open-internet policies in order to gain access into China, an untapped frontier attractive for its 1.4 billion potential consumers.

In 2018, Freedom House reported that Apple, a premier U.S. tech giant, submitted to Beijing's standards by "removing hundreds of virtual private network (VPN) services from its online app store."[22] These VPNs were crucial for allowing Chinese netizens to 'break' through China's Great Firewall and access "uncensored news and social media services," critical for cultivating a generation of Chinese aware of the free, democratic world.[23] Additionally, Apple agreed to transfer "Chinese users' data on its iCloud service to state-owned Guizhou-Cloud Big Data in February 2018."[24] All information uploaded onto China's state-owned cloud service is subject to CCP scrutiny, and anything deemed "unlawful" by the central government can be traced back to users who may be punishable by heavy fines, decreased social credit scores, and even jail sentences.

As promulgators of the free market, the U.S. has adequately supplied substantial freedoms to tech corporations; however, it has not ensured that tech operators are exercising these freedoms with a heightened level of responsibility.[25] It is becoming increasingly crucial now, however, that U.S. tech firms to "design, develop, and deploy AI with respect for human rights above and beyond the ethical commitments" of the private sector in other nation states.[26] Companies that do so reinforce American values of individual privacy and high quality of life, two pillars of U.S. soft power. Therefore, companies committed to upholding high standards of user data privacy should be sufficiently rewarded by the FTC and emulated in the marketplace.

Without corporations committed to the American virtues of individual rights, other tech giants like Google are sure to follow in Apple's footsteps, enforcing China's censorship standards in exchange for short-term financial profits. While it is important for the U.S. federal government to promote innovation and global partnerships, it must also help corporate heads understand that partnerships with China are a delicate matter and need to be handled with extreme discretion

and foresight. China, designated the "worst abuser of internet freedom" in the world, has made no indication of changing its closed-internet policy and will require all foreign companies doing business within its borders to conform to its rules.[27] Consequently, American firms that are not coached in the value of upholding human rights are at high-risk of succumbing to China's authoritarian doctrine.

Currently, there are approximately 108 million Chinese listeners who tune into the U.S. Agency for Global Media (USAGM)'s two broadcasts in the region, Voice of America and Radio Free Asia, weekly. This demonstrates there is a growing interest and curiosity on the part of Chinese netizens for the U.S.'s democratic systems; however, if U.S. companies adopt China's closed-internet policies, the U.S. will suffer a loss of credibility to the detriment of Chinese citizens, its public diplomacy efforts in China, and a democratized cyber sphere. Companies that give in should thus be subject to penalties by an overseeing U.S. agency i.e., the FTC as it may place both Chinese and American users at risk and produce long-term losses for data privacy regulations and ultimately American soft power.[28]

Part III: Improving U.S. Public Digital Health

U.S. netizens today are largely unaware of their own data rights albeit technology was invented on American soil. Cybercrime has "entered a new era of complexity" with 30 percent of U.S. consumers reporting $16.8 billion losses due to data breaches in 2018.[29] Equally disconcerting was the fact that "[f]or the first time, more Social Security numbers were exposed than credit card numbers."[30] Increased cyber corruption will deter foreign investors who value the U.S. for its stability and security both off and online. The U.S. can reverse the status quo and increase in soft power if it becomes a global leader equipping publics with effective strategies needed to defend their data online.

This is already being executed in the EU. The General Data Protection Regulation (GDPR) mandates that all constituents within the EU and the European Economic Area (EEA) are aware their personal information is private property and should be safeguarded. The EU's high standards for cybersecurity and data protection are an important contributing factor to the high scores the United Kingdom (no. 1), France (no. 2), and Germany (no. 3) received on the 2018 Soft Power 30 Index.

While the U.S. has time to go before it creates a comprehensive data oversight agency comparable to GDPR, individual American states are taking their own initiatives to better equip their residents for assaults on their personal information. California is the first state to lead this initiative with The California Consumer Privacy Act (CCPA) which will be in legal effect January 1, 2020.[31] Inspired by the GDPR, the CCPA aims to regulate Silicon Valley by requiring for-profit entities making more than $25 million annually, collecting data from more than 50,000 individuals per year, or earning more than half its gross revenue from selling customers' information to be subject to stricter user privacy standards.[32]

In addition, the CCPA makes Californian residents aware of their following rights:[33]

- Right to know what personal information companies collect about them
- Right to know with whom their personal data is sold and/or shared
- Right to deny a company the right to sell and/or share their information
- Right to access their information after it is collected and stored
- Right to be offered a different service if they would like to withhold personal information

Californian businesses that infringe on individuals' data rights will be held liable by the CCPA and required to alter business practices.

In the cyber world, the U.S. is only as strong as the weakest link, which demonstrates the necessity of codes like the CCPA.[34] With 80% of cyber breaches linked "to the simplest vulnerabilities," it is crucial that ordinary American individuals, the 'weak links' in the ranks of U.S. cyber-power, are equipped to preserve their privacy and hold culpable corporations accountable.

Elizabeth Linder, a Soft Power 30 Index contributing author, writes that a U.S. public "trained to vaccinate as part of their yearly routines" should likewise be trained "to translate this defense mechanism to health check-ups in their digital lives, taken as seriously as the flu."[35] If the U.S. is not mandating this training, its constituents are unlikely to become immune to the others' attacks, creating a population vulnerable to large-scale risks that could severely impact their wellbeing. This will ultimately reflect poorly on U.S. governance and will result in considerable losses for U.S. soft power. Linder (Chatham House) suggests the following public diplomacy initiatives to help improve the state of overall cyber health in the U.S.:

- Inviting technology influencers to serve as ambassadors for cyber health[36]
- Galvanizing technology philanthropists to fund research

needed to understand data breaches and the best user protection responses[37]

• Creating global networks that inspire transparent dialogue between governments, corporations, technologists, and civil society leaders concerning data rights and effective regulatory practices of cyber space[38]

These three initiatives are practical methods the U.S. can implement on their path towards formulating a suitable national legal framework by which to regulate the cyber realm. In doing so, the U.S. can rise to become a moral authority on cyber policy which can serve to attract other nations looking to the U.S. as an example for developing their own cyber laws.

Conclusion

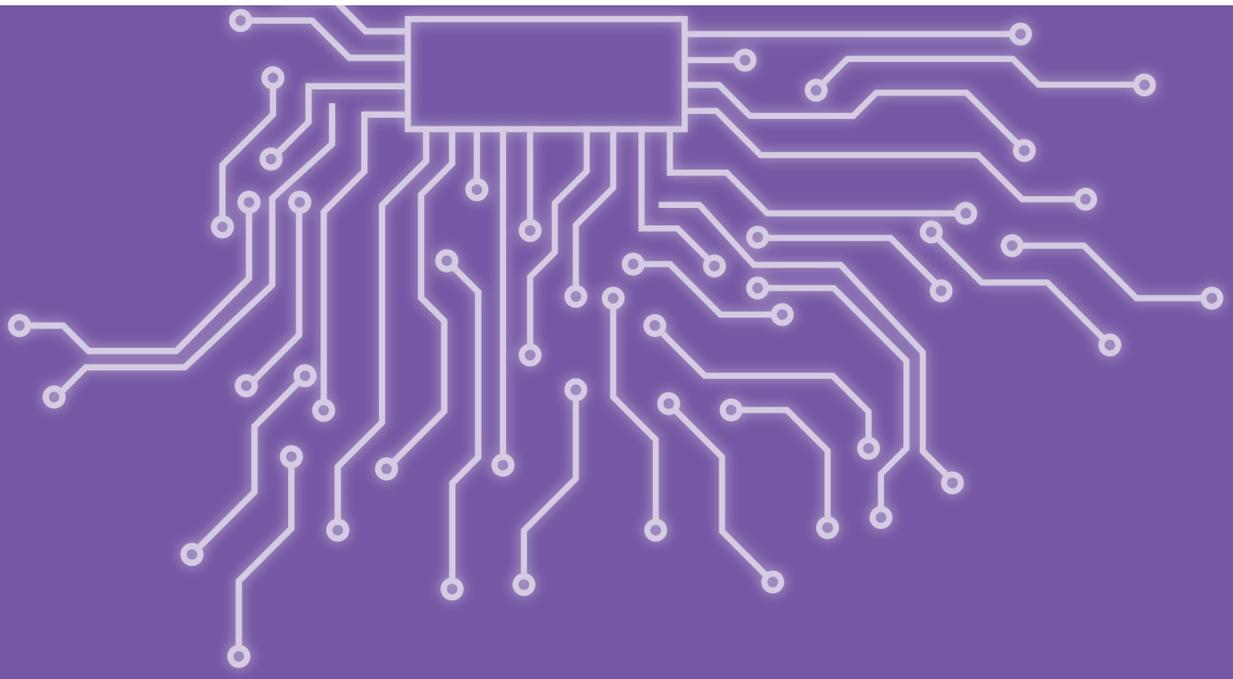
Today, China is edging out American soft power by wooing developing regions of the world with technology-infrastructure investments. Desiring to build up their economies via cyber technologies, these developing nations are looking to global powers like the U.S. and China for guidance in constructing their own cyber policies. To combat the replication of China's Great Firewall policy in those nations, the U.S. should model a successful 'open' version of the internet.

This open version internet relies on effective U.S. federal regulations to promote innovation while safeguarding individuals' basic freedoms. In addition, the U.S. should deploy ambassadors of digital diplomacy on its social media platforms to promote public digital health and the "design, development, and delivery" of ethical cyber-products.[39] Finally, in response to cyber-breaches, the U.S. should be transparent about its policy short-comings and make timely reparative measures, relying on an accountability-partnership with the EU in order to prevent future infringements.

This will demonstrate the U.S.'s commitment to making the internet more safe and more free, attracting countries to American systems of cyber governance and away from Chinese systems of digital authoritarianism.

Jasmine Kolano

Jasmine Kolano is a current Master of Public Diplomacy candidate ('20) and Editor-in-Chief of Public Diplomacy Magazine. She received her Bachelor's Degree in Communication Studies and Honors Humanities at Azusa Pacific University ('18). She is fluent in Mandarin with elementary proficiencies in Cantonese and Hebrew. In 2016, she lived abroad in Jerusalem where she engaged in field study work in Ramallah and Jordan. She wants to continue working in youth empowerment, impactful storytelling, and global reconciliation.



CYBER-DIPLOMACY'S RISING STARS

Cyber-diplomacy in Qatar: A Virtue of Necessity?

Khristo Ayad and Abed Shirzai

Delineating the term cyber-diplomacy is not without debate. Sometimes used equivalently to digital diplomacy – which is the use of digital means in exercising diplomacy – cyber diplomacy is better described as employing means of diplomacy to respond to challenges in the cyberspace. In this context, it is the small, yet influential Gulf nation of Qatar that continues to make considerable strides.

Driving an ambitious soft power strategy since the mid-nineties, Qatar did not limit itself to investing its gas-generated wealth in its own media, infrastructure, tourism and business sectors to compel foreign direct investment and advocacy. It also pursued underpinning its diplomacy early on through a diversity of investments abroad and by profiling itself as an important player in areas of global relevance. Multilateral exchanges in the interest of cybersecurity were particularly important.

Drawing worldwide attention to the risks attached to today's digital environment, the rupture between Doha and four of its neighboring capitals saw Qatar at the receiving end of a wide-scale cyberattack and disinformation campaign. In June 2017, hackers uploaded fabricated information onto the Qatar News Agency website, followed by bots which multiplied an avalanche of incendiary content on social media, all of which led up to today's incessant Gulf stalemate. Parallel to the fierce controversy around foreign meddling in the 2016 U.S. elections, the Gulf crisis placed Qatar at the center of a global cybersecurity debate involving technology experts, as well as, political, security and policy analysts. It also set a globally visible precedent for a nation-state's capability to adequately respond to

such an intrusion.

By understanding the situation as an opportunity, Doha has since accelerated its cyber-diplomacy efforts, making it a virtue of necessity. Beyond focusing on cyberdefense and cyberwarfare, Doha has also provided a platform for multilateral dialogue on how cyber ethics and cyber peace will have to be shaped in the future.

Qatar is not new to this. It had made continued investments in designing an ecosystem to incubate ideas for safeguarding the cyberspace long before the Gulf spat. Levelling up its digital environment and technological know-how, enhancing its capabilities, and developing transnational partnerships have been key components of the country's cybersecurity framework from the outset. On the verge of hosting the 2022 World Cup, Doha has been very conscious of the need for preparedness against virtual threats. Seeking to protect its networks and population, of which more than 80% are foreigners, the country initiated a number of initiatives and policies, including its National Cyber Security Strategy launched in 2014.

Long-term instruments for putting national cybersecurity strategies into play were provided by the Cyber Crimes Investigation Center, the Cybersecurity Coordination Office, as well as the Qatar Computer Emergency Response Team (Q-CERT), an official body mandated to identify and prevent cyberattacks against the government and other critical sectors. The Banking Supervision Rules initiated by the Qatar Central Bank in coordination with Q-CERT have been put in place to protect the country's financial institutions. Qatar's Ministry of Transport and Telecommunications conducts annual drills, unique to the country, engaging public and private institutions in an array of technical and educational activities, raising readiness and awareness on how to manage cyberattacks.

In October 2019, Qatar hosted the second edition of the Global Security Forum. Organized by the Soufan Center, a security-focused strategy center in New York, the conference convened government officials and experts from more than fifty countries to participate in a variety of sessions, shedding light on the security challenges posed by the proliferation of modern information warfare

in today's digitally interconnected societies.

Qatar in particular has also recognized the significance of education, science and research in enhancing cybersecurity, solidifying its position as a hub for international cybersecurity capacity. Carnegie Mellon University in Qatar, Hamad Bin Khalifa University (HBKU), and Qatar University all offer specialized study and research programs in computing and cybersecurity. HBKU's Qatar Computing Research Institute (QCRI) is dedicated to research tackling local and global cybersecurity challenges. There, international and local experts, as well as researchers and students, work hand in hand. The institute's Qatar Center for Artificial Intelligence collaborates with international partners, such as the Massachusetts Institute of Technology and Boeing to find solutions to technology challenges, including cybersecurity. Integrating the support of international partners, including Sofia University and the University of Bologna, QCRI's "Tanbih" project (Tanbih" is the Arabic word for "warning") promotes media literacy and seeks to limit the societal effects of fake news by providing an online news aggregator that uncovers stance, bias, and propaganda techniques in media coverage.

More than 130 students, researchers, and experts accounting for thirty nationalities came to Doha to take part in the Qatar International Cybersecurity Contest in October 2019. Participants sought solutions to challenges in five major areas, including measures to secure genetic data, hacking prevention, fake news detection, and competitions revolving around the ethical and legal aspects of activities in cyberspace. The event explored how actors in academia and the private sector, both locally and internationally, can collaborate to find solutions to the most pressing issues governments face in the cybersecurity arena, and how such collaborations can be emulated elsewhere in the world.

Cross-border partnerships have also played a key role in the furthering of cyber diplomacy as friendly nations exchange knowledge, expertise and assistance in times of crisis. Following the cyberattack that triggered the Gulf Crisis, Qatar developed several bilateral partnerships to enhance its cybersecurity capabilities and share knowledge internationally. A joint initiative, "Academia-Industry Cooperation on Cyber Security," dubbed "science diplomacy" between the Qatar National Research Fund and Turkey's Scientific and Technological Research Council (TÜBİTAK), was brought to life in 2017, aiming to develop innovative responses to prevalent cybersecurity needs.

In the wake of the 2017 cyberattack that sparked an unprecedented regional crisis, Qatar has managed to present itself as a calm and level-headed actor on the diplomatic stage. While there cannot be any doubt of the country's economic clout, Doha's remarkably thoughtful response and cyber diplomacy strategy may indeed have facilitated additional transnational partnerships with leading international institutions that are vital to the overarching cybersecurity debate. Having positioned itself at the forefront of this issue as a growingly digitized and complex threat environment today poses a risk to all countries, it is likely that a leadership position in cybersecurity may as well turn out to be one of Qatar's strongest soft power assets, yet.

Khristo Ayad

Khristo Ayad is a strategic communications consultant and public diplomacy analyst based in Doha. He has worked across different sectors in Germany and the Arabian Gulf region and holds an MA in Diplomatic Studies from the University of Leicester.

Abed Shirzai

Abed Shirzai holds an MA in Public Policy from Hamad Bin Khalifa University and works with an international strategic communications firm in Qatar. He has a Bachelor of Science in Business Administration with a focus on market research from Carnegie Mellon University Qatar.

Estonian Leadership in the Cyber Realm

For a country small in population, geographic size, and gross domestic product, Estonia has undertaken a massive leadership role in the cyber defense and diplomacy realm.

Daniel E. White

In 2007 Estonia bore the brunt of the largest scale cyber-attack in its history, as the government, a variety of private entities in the financial sector, and citizens themselves were targeted in the aftermath of protests following the removal of the Soviet Red Army memorial.[1] Capacity in the cyber domain, particularly in Estonia's case, has been able to scale so greatly due to the security elsewhere being shored up by NATO, the EU, and through a well-resourced diplomatic corps.

Estonian Security Situation

As a Baltic Nation, Estonia feels the pressure of Russian adventurism from all sides. Even with NATO membership, Estonia is one of the countries most vulnerable to Russia, constantly in conflict with its status as a former member of the Soviet Union, and as a nation that, less than 30 years ago, had Russian troops enforcing imperial dominance. According to the Estonian Defense Minister, an active defense that participates in consistent military training exercises with allies, coupled with NATO air-policing, decreases the threat level of a Russia invasion.[2] The benefits of heightened security not only enable, but also demand innovation in survival capabilities. Such innovation leads to dual-use technology aiding in development across a variety of sectors in society. Essentially, without the threat of cyber intrusions and misinformation campaigns, Estonia would not have made the advancements seen now in the cyber domain.

Estonian Leadership in the Military Cyber Space

It should come as no surprise that NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) was built in Tallinn, Estonia's capital, in 2008. The center focuses on research, development, training and education spanning both technical and non-technical approaches to cyber defense.[3] The CCD COE acts as a brain trust producing lessons learned, hosting conferences and establishing an ecosystem for both NATO and non-NATO members alike; including partnerships with Austria, Luxembourg, and South Korea. Estonia's military outreach and diplomacy, through its shared cyber successes, place it in a league of its own serving as a model to other countries how to both share knowledge globally and gain a strong defensive cyber capabilities.

Estonian Leadership in Global Initiatives

On the cutting edge, Estonia was the first country to offer e-Residency, a government-issued digital identity and status that provides access to Estonia's e-services and transparent business environment.[4] Historically Estonia has developed a variety of cyber options including tax collection, voting, health data all with delivery mechanisms on online platforms. Most recently, Estonia developed a Department of Cyber Diplomacy within its Ministry of Foreign Affairs, carrying the momentum from the first-ever cyber diplomacy training summit with NATO and EU diplomats.[5] That the country also created the position of Ambassador at Large for Cyber Diplomacy in the appointment of Heli Tiirmaa-Klaar, who took the mantle alongside colleagues in the U.K and Australia in similar positions, speaks volumes.[6] Nations who dedicate ambassadorships to cyber prove that it is not only a tool, but also a fundamental part of the approach to foreign policy, likening them to that of American Ambassadors at large for human rights, who should be emulated globally.

Estonia Tomorrow

Authenticity is one of the greatest issues for citizens of all countries, particularly when consuming information preceding elections. With Estonia being uniquely positioned at the United Nations Security Council as a first term non-permanent member in 2020-2021, preparing for election security should be at the forefront as it impacts all UN members.[7] With its tracked success in cyber security as a hallmark of national identity, Estonia has the capacity to use its global position on the UNSC to develop cyber norms and approaches to cyber based solutions to complex global issues. Cyber diplomacy, while nascent in concept, has an archetype in Estonia for the world to follow.

Daniel E. White

Daniel E. White is a graduate student pursuing an MPA from the School of International and Public Affairs at Columbia University, where he was an assistant editor at the Journal for International Affairs and currently, the rapporteur of the Columbia Seminar on Defense and Security. Daniel began his career as a Field Artillery Officer US Army for over five years with service in North East Asia, the Middle East and on a General Officer's staff. After leaving the Army as a Captain, he completed stints at the transatlantic think the German Marshall Fund to the United States and Lockheed Martin. Most recently, Daniel was a political-military affairs analyst at U.S. Southern Command in Miami, FL. He earned his bachelor's degree and army commission from the United States Military Academy at West Point.

Georgia's Cybersecurity Stand and March Toward Progress

Miriami Khatiashvili

Most people have only a very general idea about cybersecurity as a foreign policy dynamic and as it affects diplomatic choices. This condition might be understandable, because the idea of cyber-diplomacy is relatively new in international relations. The question of what a country should do to advance and sustain cyber-diplomacy begins with a clear understanding of its national security objectives. It can define its cyber-diplomacy approach in response to challenges to strategic interests. In the case of Georgia, for example, Georgia's cybersecurity potential was not discussed much as a foreign policy issue up until a decade ago, when cybersecurity became Georgia's foreign policy ambition and aspiration. Nowadays it is a matter of Georgia's national security, but is still not often and thoroughly perceived as a foreign policy dynamic.

The case of Georgia exemplifies how a country gradually transformed its approach to cyber issues from information security policy into the cybersecurity domain. It illustrates why Georgia's cyber-diplomacy matters for international security and why cybersecurity matters for Georgia specifically. Although cyber-diplomacy is a less articulated term in Georgia's foreign policy mainstream, cybersecurity is a widely spread concept in Georgia's foreign policy decision-making. A probable explanation for this might be that cybersecurity has not yet been fully perceived as a diplomatic tool in Georgia. It is viewed more as a factor, which affects Georgia's foreign and defense policy. The Ministry of Defense of Georgia declared the year 2019 as the year of Cyber Security in the Georgian armed forces.[1] This decision might have two implications for Georgia. On the one hand, this decision shows the level of importance the government of Georgia gives to this field. On the other hand, this decision attributes more duties to the government of Georgia to enlarge cybersecurity priorities, capabilities, infrastructure, resources, and partnerships. One of the highlights in the framework of this year was the Intermarium Cyber Security Forum 2019 in Tbilisi, attended by representatives from more than 16 countries.[2]

Strengthening cybersecurity - security of cyber space and the protection of electronic information - is one of the principal national interests of Georgia.[3] Furthermore,

one of the principal responsibilities of its foreign policy is to ensure as much cybersecurity as possible. The fact that Georgia tries to take care of cybersecurity – as an integral part of its modern foreign policy – is shown by the Global Cybersecurity Index 2018, an index that measures the commitment of countries to

cybersecurity. In this index, Georgia is ranked 9th in Europe and 18th on the global level.[4] Taking into account Georgia's short cyber-diplomacy history, these rankings seem to suggest a meaningful response regarding its cybersecurity progress.

Emergence and Urgency

Georgia started its journey in the field of cyber-diplomacy in the mid-2000s. This journey can largely be regarded as Georgia's first official attempt to define its own information security policy in the post-Soviet space. In 2005, information related challenges were acknowledged in the National Security Concept of Georgia.[5] This document identified information security policy as something vital, put front and center in Georgia's national security policy. Georgia realized that "effective public administration can only be ensured if the state information policy is cohesive and the decisions are based on credible information."[6] Concurrently, the government of Georgia was "developing the legislative basis and infrastructure necessary for the improvement of the information technologies and secure flow of information."[7] Since 2008 Georgia's interest in information related issues adapted new foreign policy realities.

Russian cyberattacks on Georgia during the Russo-Georgian War of 2008 illustrated that Georgia needed to transform its approach from information security policy to the cybersecurity domain. These cyberattacks showed Georgia the urgency of managing cyberspace as an integral part of its defense policy. It illustrated that information warfare, including elements of cyber warfare, would become a proven threat to regional and international stability. By targeting and threatening Georgia's national security interests, the cyberattacks revealed Russia's information warfare capabilities to the international community. It also showed that securing information and cyber domains would not just advance Georgia's national or foreign policy interests, but would contribute to international security. It became clear that if Georgia had a resilient cyberspace, maintaining a geopolitical advantage would be guaranteed for its Western partners.

Legislative Configuration

Consequently, many things have changed since 2008, arguably much of which have made Georgia more resistant to cyber threats. In the following years of the Russo-Georgian War of 2008, the government of Georgia developed the needed legislative basis. It was one of the first steps that would provide a fertile ground for state institutions to suggest far-reaching, successful, and well-organized information policy related efforts. Georgia's cyber-diplomacy position would reach new depths because of this; they could not arrive to their current cyber-diplomacy position without a conceptual legislative base. "Law of Georgia on Information Security,"[8] issued in 2012, did not establish a specific legislative framework of cybersecurity, but rather outlined an initial plan of action for Georgia in this field.

This law deserves specific attention because, by defining cyber-related and information security issues, it set the stage for the new cyber-diplomacy ideological strategy in Georgia and defined the four groups of priority cybersecurity threats for Georgia. Each group classifies cyber-attacks against different targets. The first group contains a cyber-attack that threatens human life and health, state interests or defense capacity of the country. The second group classifies a cyber-attack against the information systems of the critical information system subject. The third group is related to the financial resources and property rights of a state, an organization or a private person. The fourth area of cyber security threats categorizes "any other action that, based on its nature, purpose, source, scale or quantity, or the amount of resources required for its prevention, contains sufficient threat for proper functioning of the critical information system."[9] Eliminating these cybersecurity threats are primary objectives for Georgia.

In addition to the legislative basis, one of the earliest pragmatic efforts of the government of Georgia for ensuring information security was the establishment in 2010 of the Data Exchange Agency (DEA), governed by the Ministry of Justice of Georgia. Since 2011 the Computer Emergency Response Team (CERT) of the DEA has been operating in Georgia to manage incidents regarding information security in cyberspace. In Georgia's defense sector, Cyber Security Bureau (CSB), established in 2014, is responsible for developing stable, effective and secure information and communication technology. One of the primary goals of CSB, which operates under the Ministry of Defense of Georgia, is the protection of information and communication technology infrastructure from cyber threats and cyber risks.[10] Further efforts Georgia made in terms

of cybersecurity included a publication of the first National Cyber Security Strategy of Georgia in 2013.[11] By publishing this strategy, Georgia proposed "to set up a system of cyber security that will facilitate resilience of cyber infrastructure against cyber threats as well as represent an additional factor in the economic growth and social development of the country."[12]

Quartet of Partnerships

Partnerships in cybersecurity matter for Georgia more and more. United States and NATO are the chief cybersecurity partners for Georgia. Through the partnership with the United States, Georgia develops programmatic and technical cyber issues. Supporting Georgia's cyber defense at the strategic, tactical and operational levels is one of the initiatives outlined in a Substantial NATO-Georgia Package (SNGP).[13] This support includes extensive cyber cooperation initiatives[14] and providing advice and training. Georgia's cyber-defense cooperation is expanding with the Allies and other partner countries, such as Estonia and Lithuania. Each step toward partnership is mutually beneficial because it supports Georgia's goal of Euro-Atlantic integration.

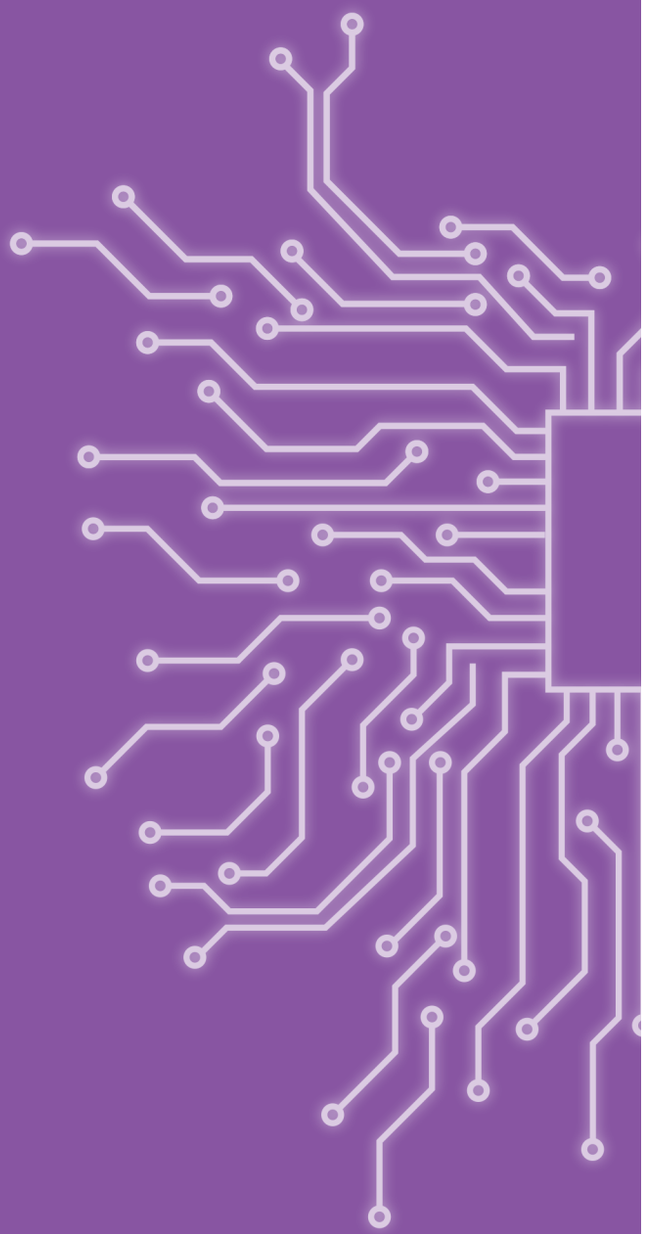
Considering a succession of both good and bad cybersecurity practices of cybersecurity partner countries prepares Georgia to more easily meet the current and upcoming geopolitical cyber-challenges, which include hybrid threats. Up until now, Georgia has issued two national cybersecurity strategies – the first in 2013 and the second in 2017. These strategies outlined four primary principles of cooperation in the field of cybersecurity. These principles include the whole-of-government approach, public-private cooperation, active international cooperation and personal responsibility. These four principles of cooperation are critical for Georgia to advance cybersecurity. However, international cooperation on bilateral and multilateral levels might have multilevel importance for Georgia. The benefits Georgia gets from international partnerships – ranging from trainings to recommendations – build up Georgia's cybersecurity capabilities and international image. These benefits assist, prepare, and strengthen Georgia so that the country will be able to respond to and counter hybrid threats. This principle of international cooperation connects the other three principles in this list and is a key component to sustaining them. International partnerships have built Georgia's present cybersecurity capabilities and collaboration will play an important role in the future of cyber-diplomacy in Georgia.

Irrefutable Future

Georgia's progress in the field of cybersecurity has been rapid in course and action. Despite this, Georgia is far from reaching its full cyber-diplomacy potential, partly because critical internal and external challenges still remain. On the one hand, Georgia should have a regular and well-ordered process of cybersecurity development to tackle these challenges; on the other hand, Georgia should find the correct balance between its cybersecurity instruments and capabilities. Cyber-diplomacy is expanding into new areas over time. In the upcoming years, cybersecurity issues will foster more intense involvement in foreign policy. Georgia has to adjust to this process. Doing so will give Georgia a better chance of meeting the cybersecurity challenges of the future.

Miriami Khatiashvili

Miriami Khatiashvili is a PhD candidate in American Studies at Ivane Javakhishvili Tbilisi State University (TSU) and a public diplomacy scholar from the Republic of Georgia. She holds BA and MA degrees in American Studies from TSU. Miriam has developed and teaches American Studies and U.S. foreign policy undergraduate and graduate courses in Georgia. In June and July of 2017, she completed the United States Department of State's exchange program Study of the United States Institutes for Scholars on U.S. Foreign Policy at Bard College in Annandale-on-Hudson, New York. Since 2017 she served as a board member of the U.S. Government Exchange Program Alumni Association of Georgia. In her free time she organizes educational and cultural programs as a volunteer speaker in American Corner Tbilisi, which she has done since 2012. Her public diplomacy areas of interest include, but are not limited to, U.S. diplomacy, Georgia's foreign policy, cultural diplomacy, and strategic communications.



OVERCOMING DISINFORMATION

Are Digital Rights Human Rights?

Ilan Manor

In 2016, the UK-based Ditchley Foundation held a two-day conference focusing on the question "Will we still have a single global Internet in 2025?" (Ditchley, 2016). This question seems increasingly relevant given that various nations have begun to segment the global Internet. One obvious example is China, who erected a great firewall in order to censor the information which is available to Chinese netizens.

Other nations are also segmenting the global Internet by limiting access to various Internet platforms and Internet-based services. Such is the case with Iran, where Internet users must use special routers in order to circumvent government blockage of Western websites. In Cuba, opposition websites are routinely blocked, while Russia and Turkey have taken to blocking social media sites such as Twitter, Facebook and, more recently, LinkedIn (BBC, 2016). Other countries that are exploring possibilities to limit Internet access include Saudi Arabia, Venezuela, Ethiopia, and Hungary.

These activities therefore bring another question to the forefront: do individuals have a basic, human right to access accurate information online given that such information shapes their worldviews and political opinions?

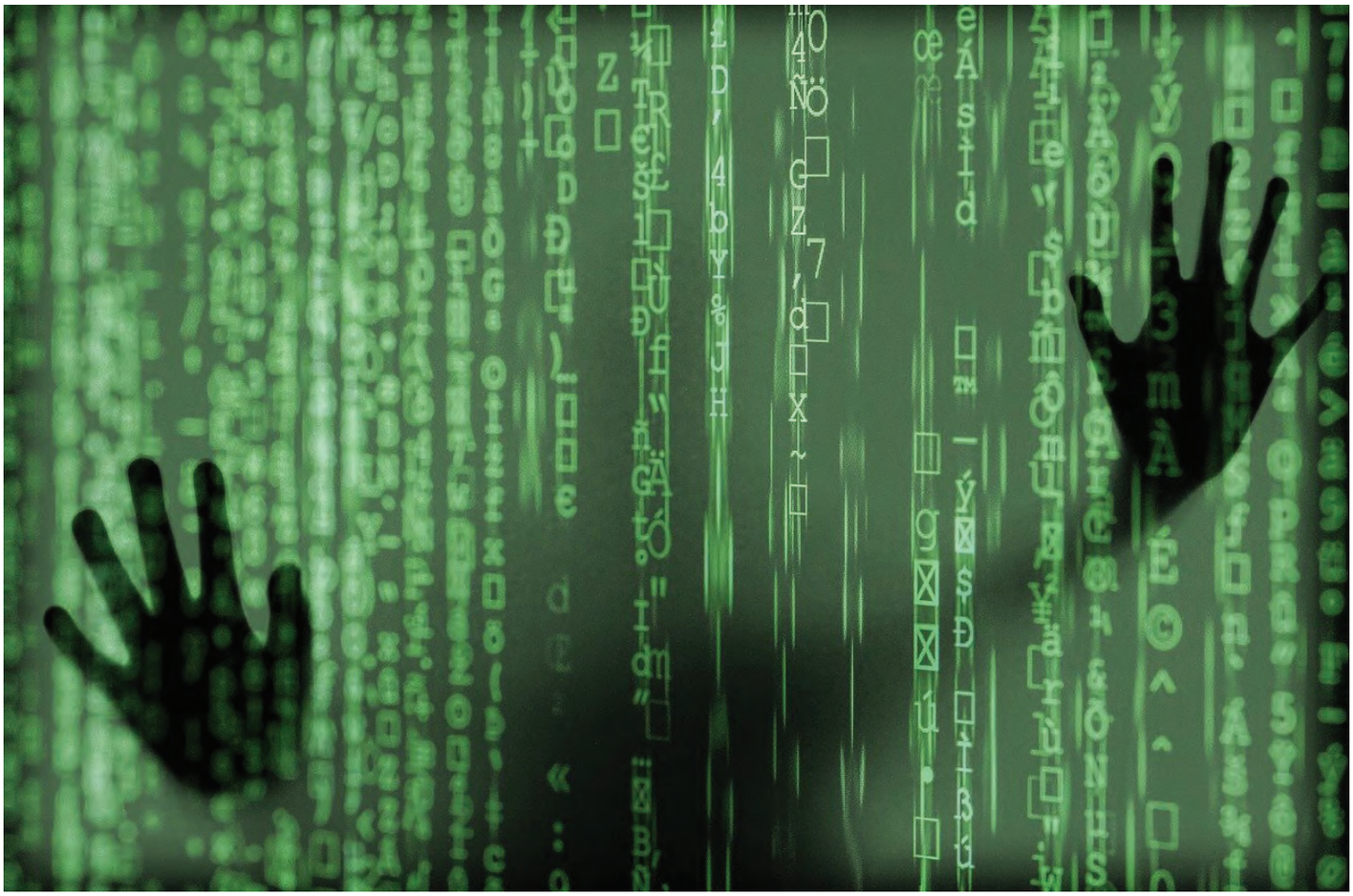
The main concern for those dealing with Internet governance is that the trend of Internet fragmentation may soon gain further momentum due to three factors. The first is the growing number of cyber-attacks against nations which may prompt governments to erect national firewalls. The second is China's building of Internet infrastructure in both Africa and Latin America. Such infrastructure may be used by countries to create their own great firewalls. Finally, the rise of right-wing governments across Europe may be seen as a rebuke to globalization. As the Internet is the medium of globalization, right-wing governments may wish to assert national control over the Internet.

In an attempt to stem the tide of Internet fragmentation and ensure the global movement of knowledge, ideas, and innovations, some have argued that Internet access is a human right. In 2011, the United Nations declared that Internet access is a human right, as it is intrinsically tied to freedom of expression and freedom of opinion (UN, 2011).

Currently, Internet governance experts and civil society groups are seeking to link Internet access to the Universal Declaration of Human Rights (UDHR). The logic behind this policy lies in the fact that the UDHR has been adopted by the majority of nations across the world and is seen as a framework that enables both democratic and non-democratic governments to discuss issues relating to the protection of human rights.

Recent years have also seen growing attempts by nations to use the Internet to fracture, assault, and contest reality. Social media platforms such as Facebook and Twitter fracture reality by nature given that the social media feeds of each user are tailored to his political views, sexual orientation, artistic taste, occupation and more. As such, a Facebook user may see news articles describing mass protests in Lebanon, while another may see an article listing luxury hotels in Beirut. In the digital age, reality is fragmented into millions of atoms. Some nations have attempted to weaponize the fractured nature of social media. Such was the case with Russian paid Facebook ads which targeted Americans during the 2016 elections. African Americans were exposed to Facebook ads that depicted police brutality against Blacks in an effort to drive down support for Hillary Clinton. Conversely, conservative users saw ads depicting America's borders as vulnerable in the face of droves of illegal immigrants, thus increasing support for Donald Trump (Manor, 2019).

Nations have also sought to assault reality using the Internet. Both Russia and Iran have created fake news sites in order to obtain foreign policy goals. Russian fake news sites depicted alleged crimes against Russian minorities in Ukraine thus attempting to legitimize the annexation of Crimea in 2014. Iranian fake news sites targeted Americans in attempts to influence their views on the Middle East and U.S.-Israeli relations (NATO



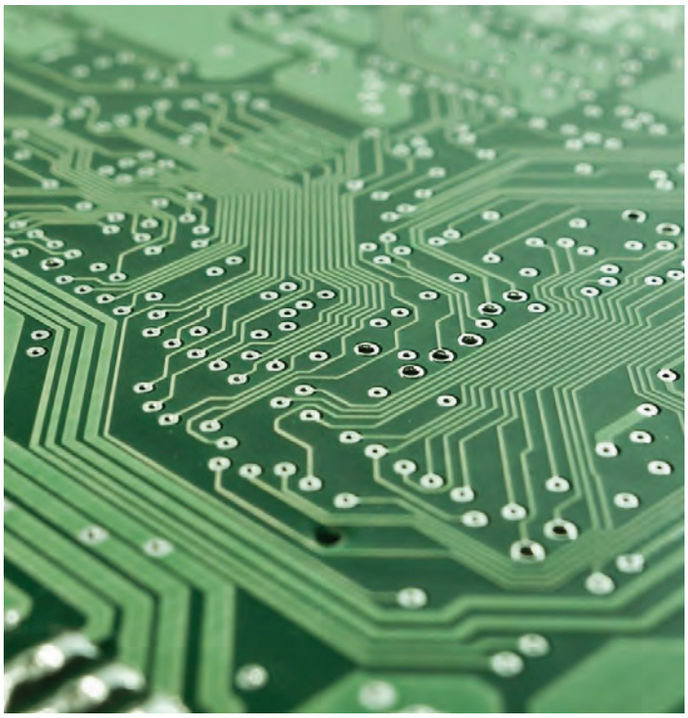
Stratcom, 2015; Tercatin, 2019). Countries such as Russia, Saudi Arabia, the Philippines and North Korea have also used bots, or computer software meant to mimic human behavior, to contest reality (Bradshaw & Howard, 2019). For instance, Russian bots published thousands of tweets in support of the Brexit, leading British social media users to assume that many of their fellow citizens were in favor of exiting the European Union (Manor, 2019).

In all of these cases, intent users were strategically misled by foreign governments. Even more importantly, in all of these cases the Internet was used to increase social friction and prey on minority groups' social frustration. These activities therefore bring another question to the forefront: do individuals have a basic, human right to access accurate information online given that such information shapes their worldviews and political opinions? Similarly, do individuals have a basic, human right to be protected from the nefarious digital activities of other nations given that such activities are detrimental to the health of their society? The answer to both these questions is yes as they stem from the basic right to access the Internet. For what good is access to the Internet if one faces a tidal wave of manipulations, half-truths and conspiracy theories?

One way to engage in a truly global conversation about the future of the internet and digital platforms may be to adopt the term digital rights and seek a universal definition of such rights, following the example of the Universal Declaration of Human Rights.

However, linking digital rights with universal human rights also poses several challenges.

Ensuring that the internet remains global and free from manipulation necessitates a global conversation. This means that nations who regard the Internet as a possible threat, or weapon, must also be seated around the negotiation table. This includes China, Russia, Iran, North Korea, and Saudi Arabia, to name but a few. However, framing the discussion about digital rights while centering on human rights might prevent these very nations from joining the conversation. This is due to the fact that they often regard the term "human rights" as a Western and democratic precept to which they do not adhere. Additionally, the issue of human rights is often employed in order to attack these nations, their governments, and



their policies in various multilateral forums.

It is therefore possible that these nations may soon come to view the discussion about digital rights as yet another pretext to attack them. This will not only prevent China from engaging in the conversation, but may actually lead to it opposing the notion of a global and trustworthy Internet and to continue blocking the free flow of information and opinion.

A possible solution may lie in the concept of 'digital rights.' One way to engage in a truly global conversation about the future of the Internet and digital platforms may be to adopt the term digital rights and seek a universal definition of such rights, following the example of the Universal Declaration of Human Rights. This term has the advantage of not provoking immediate opposition among non-democratic nations or governments who are increasingly wary of the internet's power.

Notably, Western counties also have yet to agree on a definition of the term 'digital rights.' Thus, the attempt to create a Universal Declaration of Digital Rights may require a much-warranted discussion between citizens who use the internet, their governments who are supposed to help govern the Internet, and the private sector which is the main benefactor of the Internet. For instance, does one have a digital right to understand the manner in which Google algorithms shape one's access to knowledge and news? If so, will Google be willing to adopt a policy of algorithmic transparency? Similarly, does one have a digital right to access only factual news and not fake news? If so, can we demand that Facebook review all news-related posts? Or demand that Firefox adds a toolbar for detecting fake news? Additionally, does a citizen have a digital right to determine how his or her personal data is used by his government? For instance, can a government hospital use big data gathered from citizens receiving medical aid? And may the government sell citizens' data to third parties, such as private insurance companies?

An attempt to define the term 'digital rights' and to draft a Universal Declaration of Digital Rights may be a way to bring global governments, global civil society groups, and global Internet companies to the negotiating table in order to openly discuss their respective duties and rights. It would take a true partnership between all three groups (government, civil society, and the private sector) to ensure the Internet remains global, trustworthy, and open (Cowhey & Aronson, 2017).

Indeed, such a conversation may also lead to a discussion about human rights, as the two are intrinsically linked. Yet it would do so without alienating the very nations who are fracturing and weaponizing the Internet. The only question that remains is: Which country is willing to lead this important diplomatic effort?

Ilan Manor

Dr. Ilan Manor is a member of the Oxford Digital Diplomacy Research Group, a 2019-2021 USC Center for Public Diplomacy Visiting Fellow, and blogger at digdipblog.com.

You Can't Solve Lying: Adapting to the Disinformation Age

Dean Jackson

What is the solution to disinformation?" This question hangs in the air three years after the 2016 U.S. elections, when Russian interference made disinformation the word du jour. It is a simple question with complicated, unsatisfying answers. Perhaps it is the wrong question.

Digital disinformation—which we might define here as the use of the internet and social media applications to disseminate information in order to purposefully mislead, divide, or manipulate audiences—is more widespread and less novel than commonly appreciated.[1] More than two years before the 2016 elections, the disinformation component of Russia's hybrid war against Ukraine flummoxed journalists and diplomats alike. Though the role of disinformation in this conflict captured international attention, Kenyan observers may point out that Cambridge Analytica, the now infamous digital communications firm, played a role in their elections a full year before Russian forces invaded Ukraine.[2] During the same period, the Burmese military operated a 700-person-strong unit dedicated to spreading anti-Rohingya disinformation online.[3] Before that, during the Arab Spring, the government of Bahrain hired public relations firms to shape narratives around street protests and undermine activists' online organizing.[4]

By the time of its diagnosis in 2016, digital disinformation had metastasized globally. Even before the digital age, though, disinformation was a regular feature of Cold War politics: U.S. officials were concerned enough about Russian 'information operations' to create the interagency Active Measures Working Group in 1981. (Perhaps the group's greatest success was to discredit a Soviet-promoted conspiracy theory that the U.S. military created the AIDS virus).[5]

In certain circles, it has become a cliche to note that "disinformation is nothing new," but it is a truth: disinformation is an old problem. So why does it suddenly seem omnipresent? Why does the public square seem suddenly submerged under a rising tide of conspiracy theories, half-truths, fear-mongering, and scorched-earth rhetoric?

Asking, "What is the solution to disinformation?" is like asking, "How can we solve lying?" A better (if more cumbersome) question might be, "How have changes to the public square made disinformation more potent—and how can democracies adapt?"

Disinformation is not suddenly challenging democracies because it is new; it seems more pressing now because of dramatic changes to the environment in which it is deployed. Asking "what is the solution to disinformation?" is like asking, "how can we solve lying?" A better (if more cumbersome) question might be, "How have changes to the public square made disinformation more potent—and how can democracies adapt?"

Many analysts have already done excellent work to identify and describe how changes in the media ecosystem have affected the quality of political discourse and the nature of political communications. To summarize a theory of the case: as news media moved online, the barriers to entry for new sources of information fell, as did the revenue of legacy media outlets. Social media became a leading source of news and information, and an 'attention economy' emerged in which the determinant of information's commercial value

is the amount of 'engagement,' or clicks and shares, it receives. Algorithms were developed to increase engagement, which proved to be driven less by veracity and more by outrage, fear, and political animus. While the internet gave a platform to long-underrepresented voices, it also weakened local news, investigative reporting, and the sustainability of all but the largest news outlets, while paving the way for an explosion of cheap clickbait websites peddling conspiracy theories and polemic rumors. What's more, it wasn't only marginalized, underprivileged voices which found community and reach online: political extremists and regressives also gained a bigger platform.

In many countries, especially younger democracies, these changes left the media sector as a whole more vulnerable to capture as outlets desperate for funding were purchased or bullied by monied political interests.

In many countries, especially younger democracies, these changes left the media sector as a whole more vulnerable to capture as outlets desperate for funding were purchased or bullied by monied political interests. Partisan and conspiracy outlets flourished in the vacuum left by more reputable sources of information. Social media algorithms, designed to promote engagement, steered some users toward more and more partisan content. The result of these changes is a depleted and severely fragmented information landscape in which illiberal and authoritarian actors are now able, with relatively modest investments, to hold and wield power by distracting, dividing, and otherwise manipulating public opinion, both within their own countries and across borders.

These are the changes to the public square that have made disinformation more potent, and it is to these changes that democracies—not just democratic governments, but the panoply of political institutions, journalists, private-sector actors, and civil society organizations which are essential to free societies—must adapt.

Some proposed adaptations are large in scale. A new emphasis on media literacy suggests that individuals can be inoculated against disinformation and learn to recognize when their emotions and beliefs are being manipulated; but improving the citizenry's critical thinking skills is a long-term project, likely requiring changes in national education curricula. It also may not solve the problem: many conspiracy theorists and political extremists often possess impressive critical thinking skills and media literacy.[6]

Other adaptations envision large-scale changes to the telecommunications sector and the media ecosystem. Often, they involve government regulation and broad sectoral reform; some may have great promise but almost invariably, they involve difficult trade-offs and downsides. They, too, are long-term projects.

In the meantime, journalists and civil society are forging ahead with more modest but no less critical adaptations of their own.

As concerns about digital disinformation gained steam, fact-checking efforts were a natural place to begin mounting a response. But initial efforts to fact-check disinformation failed to outpace the viral spread of sensational and inflammatory content. Later, when fact-checkers were able to append their corrections directly to misleading content on social media platforms, evidence emerged that their work was backfiring; calling attention to false claims seemed to help them spread more quickly and take root more deeply in the public imagination. Fact-checkers are consequently reexamining their practices: in June 2019, prominent fact-checkers from three continents issued a joint statement calling for "second generation fact-checking," with a greater emphasis on holding purveyors

of falsehood accountable through public pressure and appeals to standards bodies.[7]

Fact-checkers face other obstacles in the form of cognitive and political biases which make some news consumers distrust sources of information that counter their preexisting beliefs.[8] Trust—in expertise, in the news media, in political systems—has by many accounts become a rare and valuable commodity. Today, individual content creators and online "influencers" may boast as much or more social trust than many media sources. In this environment, some civil society organizations are exploring innovative ways to build and borrow trust by partnering with these influential new voices to reach much larger (and often much younger) audiences than in the past.[9]

Disinformation, like lying, is not a problem to be solved; it is a tactic that succeeds or fails depending on the circumstances in which it is used.

Independent journalists and media have made their own adjustments. When bad actors say "look over there," journalists are learning to instead point the public toward disinformation's source by making it the subject of their reporting and investigations—not chasing down misleading narratives one by one, but rather exposing to the public the process by which lies and half-truths are manufactured and spread for political ends. This was a crucial lesson for journalists covering the war in Ukraine, where repeating inflammatory falsehoods about the treatment of the country's Russian-speaking minority helped amplify divisive narratives and obscure the true nature of the conflict.[10]

Other media outlets and fact-checkers have focused on finding ways to make the virality of online information work for them by packaging their content as ready-to-share videos and memes, sometimes with spectacular results. They have partnered with organizations and hired individuals with the necessary skills and expertise to produce this content rapidly, in order to keep pace with disinformation's viral spread.

Still others are forming cross-disciplinary and cross-sectoral partnerships, working with digital marketing firms, media experts, sociologists, and psychologists to carefully segment audiences and develop specialized messaging campaigns countering illiberal and anti-democratic narratives. Audience research has been exposed as a crucial gap in capacity: often, messaging efforts are too broad (failing to account for the beliefs and concerns of the audience they hope to reach), or too focused on hard-to-reach audiences (and so disparaging of important work targeting audiences that may be reachable, but misunderstood or neglected). The prerequisite skills for this are often found in the private sector; more can be done to put them in the hands of civil society.

While governments and other institutions are making adaptations in the areas of strategic communications and public diplomacy, they can also adapt to disinformation by providing resources to independent media and civil society pursuing these and other innovative means of reaching and informing audiences. They can also explore ways to fortify independent media against the tempestuous environment for media sustainability, including capacity-building partnerships for disinformation-focused efforts, more long-term fellowships for investigative journalists, and increased public support for local news media. It is crucial that support for these efforts come in ways that do not undermine their greatest source of value: independence from political interests.

What these adaptations have in common is that none of them are compelling "solutions to disinformation." Disinformation, like lying, is not a problem to be solved; it is a tactic that succeeds or fails depending on the circumstances in which it is used. Until there are major changes to the environment for news media and political communications, disinformation will continue to be effective. In the meantime, democracies must learn to adapt.

Dean Jackson

Dean Jackson is a program officer for research & conferences at the National Endowment for Democracy's International Forum for Democratic Studies, where he coordinates analysis and activities focused on how disinformation, media, and technology impact democracy and civil society around the world. Prior to his time at the Endowment, he worked in external relations at the Atlantic Council. Dean holds an MA in international relations from the University of Chicago and a BA in political science from Wright State University in Dayton, OH.

Effectively Pushing Back Against Disinformation in Cyberspace: What I've Learned in the Trenches

Mark Toner

The views expressed in this article are entirely my own and do not necessarily reflect those of the State Department or the U.S. government.

In 2014, when Russia moved to illegally annex Crimea and launched a conflict in eastern Ukraine, many in the West saw for the first time the scale and sophistication of Russia's disinformation network. It was both nimble, able to push multiple narratives in different markets simultaneously, and overwhelming, able to muddy the waters so that reality itself became malleable and hard to pin down. While operating effectively across all media platforms, it was arguably most effective at shaping public opinion online via social media, largely by its use of "bots" and "troll farms," which could create seemingly organic public reactions and grass-roots movements out of thin air.

At the time, I was the Deputy Assistant Secretary in charge of Public Diplomacy in the State Department's Bureau of European and Eurasian Affairs. The initial U.S. response to this disinformation full-court press by the Kremlin can best be described as flat-footed and scattershot, as we lacked a clear strategy and the necessary resources to engage in multiple media markets. Slowly, we gained some momentum and even managed to land a few punches. In order to shine a light on the Kremlin's lies, we issued an irreverent State Department fact sheet entitled "President Putin's Fiction" that quoted Dostoevsky's famous line, "The formula 'two times two equals five' is not without its attractions," and presented a top ten list of Putin's most egregious false claims about Ukraine.[1] We also launched a Russian language Twitter platform to push back against the steady stream of lies being spewed out by the Kremlin-run troll factories. And we worked to provide our ambassadors and spokespersons in the field with real-time updates and points to refute Russia's claims and empowered them to engage full stop in their own media markets.

But fighting online disinformation, especially in the social media space, is like trying to subdue the mythic beast, the Hydra. If we chopped off one head, two immediately grew to take its place. It wears you down. People quickly get tired of trying to counter an endless stream of lies with fact-based content. In the hours following the downing of Malaysian Air Flight 17, for example, you could literally see Russia's false narratives spreading across the globe via social media like, as the Polish saying goes, mushrooms after the rain, quickly drowning out the facts. It was incredibly frustrating, but from a communicator's viewpoint, it was also impressive.

I have served on the front lines of the disinformation fight, not just as a Deputy Assistant Secretary, but also as the Deputy and Acting Spokesperson for three successive Secretaries of State. I have battled the bots and gone toe-to-toe with RT and Sputnik—both of which regularly covered State Department press briefings, often armed with "gotcha" questions—from the briefing room podium.

Now, as a Senior Advisor with the U.S. Helsinki Commission, a bipartisan, bicameral commission that promotes human rights and security in Europe and Eurasia, I have continued to evaluate how America's diplomats can best cut through the haze of disinformation and bypass the malicious calculus of social media algorithms to engage in real discussions with the people they are trying to reach. Here are a few of the lessons I have learned along the way.

Tell Your Own Story, Don't Simply Refute Theirs

The most common and reflexive response to disinformation is reactive – it is natural to want to expose and counter their lies with the plain truth. In cyberspace, however, that can be an exhausting and even futile, proposition. The smarter response is to not take the bait at all. Instead, U.S. diplomats must work to convince their audience of the rationale and rightness of our own policies and actions. We need to offer a narrative that positively asserts who we are and what we believe to be best for America, its allies, and its partners around the globe.

The best way to communicate is to tell a story. As a spokesperson, whenever I had to deal with a particularly thorny issue, I would ask myself, what is the core narrative here? Telling the story of how we got to a certain place and where we want to go is far more compelling than a barrage of facts, figures, and anodyne talking points. U.S. government communicators need to do a far better job humanizing our foreign policy. That is how we gain the authenticity that can win over a skeptical audience.

Call a Spade a Spade

We should not be afraid to claim the higher moral ground when we can. That was the long-game strategic vision that helped us win the Cold War. In the Ukraine conflict, it sometimes helped simply to plant a stake firmly on the right side of the story.

A good example was our response to the downing of Malaysia Airlines flight MH-17 over eastern Ukraine. In a furious burst of 111,486 tweets over a three-day period, Russian trolls spread competing false narratives in order to blur the truth surrounding the real culprits behind the tragic shootdown, including a false claim that it was Ukrainian fighter jets that shot down the airplane.

Rather than playing whack-a-mole, the U.S. conducted its own internal analysis and concluded that it was a Russian BUK missile fired from Russian-controlled eastern Ukraine that killed all of the 283 passengers on board. We supported the independent, Dutch-led investigation which eventually reached the same conclusion, but we never deviated from our own initial determination that it was a Russian missile that brought the plane down, one fired either by Russian troops or their surrogates in eastern Ukraine.

Rely on Surrogate Voices, especially on Social Media

America's diplomats must be empowered to engage on social media because when used well, it can be a powerful and effective way to connect to key audiences and demographics. But we should also realize the inherent limitations of that "official" U.S. voice.

In eastern Ukraine, for example, the online debate over Russia's presence would devolve into a "he said, she said" exchange between the U.S. and Russia that would often play to the Kremlin's favor. Far more credible

were the courageous citizen journalists who used their phones and social media to debunk Russian claims of noninvolvement by showing Russian armor and tanks rolling through actual towns in eastern Ukraine. Their voices helped lend a needed credibility to our claims because these were actual citizens who were living on the front lines and could show firsthand what was happening.

More broadly, surrogate, non-governmental voices are a good way to cut through the haze of bureaucratic language and add a level of authenticity that can make an abstract issue or policy more tangible and compelling.

Don't Always Fight Fire with Fire

No matter how right you may be, the simple truth is that no one wants to hear about it all the time. In the early days of the Ukraine conflict, we urged our U.S. diplomatic posts and missions abroad to use their social media platforms on Twitter and Facebook to push back 24-7 under the mistaken belief that we had to respond to every Kremlin lie or false narrative. We offered them a daily stream content to post or push out to their followers.

However, a constant diatribe, no matter how urgent the issue or compelling the content, can ultimately alienate an audience. I learned this during a trip to Prague, when a few people on the embassy staff asked if they could mix up the content with some lighter stuff.

As one of them noted, "Much of our audience is students, and they don't want to be bludgeoned 24-7 with Ukraine, Ukraine, Ukraine."

Similarly, we had a Twitter campaign, called #UnitedforUkraine, and even a presence on Vkontakte, Russia's largest social network. What we learned over time, though, is that you will not win over any audience if you are always scolding. You need to find ways to engage with people in order to persuade them. One-issue campaigns, especially those full of righteous indignation, can get tiresome after a while.

Be Careful the Cure isn't Worse Than the Disease

Finally, we should remember the Internet was originally intended to be an organic place where free speech could thrive. While we should address how to control those malicious actors – both state and nonstate – who want to harness its power to influence people for political or financial gain, we must never keep our eyes off that noble ideal. Which is why, when I hear calls for regulating the content that social media companies disseminate, it gives me pause. As the OSCE Representative on Freedom of Media, Harlem Desir, said recently: "At a time when freedom of media and expression are increasingly exercised online, states must ensure that the internet remains a space for pluralistic debate and information rather than a tool for censorship and repression."

Governments and civil society must find a way to address the very real threat posed by disinformation. It is corrosive and, when used effectively, can harm or hinder the democratic process. But we must ensure that the cure is not worse than the disease. We must have the confidence that our ideals will ultimately carry the day. For that reason, I will always choose to err on the side of less restrictions than more.

Mark Toner

Mark Toner is a career member of the Senior Foreign Service, currently serving as the U.S. Department of State's Senior Advisor to the Helsinki Commission. He most recently served as a Senior Faculty Advisor at the Eisenhower School for National Security and Resource Strategy, a part of the National Defense University. Prior to that post, Mark was the Acting Spokesperson for the Department of State and has also served twice – under two different Secretaries of State – as the Department's Deputy Spokesperson. Mark was a Deputy Assistant Secretary in the Bureau of European Affairs, where he coordinated public diplomacy programs for Department's largest regional bureau, and in the Bureau of Public Affairs, where he oversaw all the Department's front-line media engagement operations. Mark has served overseas at the U.S. Mission to NATO in Brussels, Belgium; the U.S. Consulate General in Krakow, Poland; and the U.S. Embassy in Dakar, Senegal. He has also worked in the State Department's Operations Center as a Senior Watch Officer and served as a staff member on the Senate Foreign Relations Committee.

The Future of Digital Empowerment: Combating Online Hate

Actions that are taken in the non-physical realm of cyberspace can have serious and deadly consequences in the physical world. The Christchurch Mosque Shooting, El Paso Shooting and the Pittsburg Synagogue Shooting are just a few examples of tragedies that utilized the power of digital global communication for nefarious purposes. How can we stop this from happening again?

Christina Chilin

As of August 2019, 43% of the US population reported living in a gun household.[1] Because of growing gun violence, gun control is now frequently and fiercely debated in the news media. However, we must not neglect to address another important part of the mass shooting equation: social media.

The perpetrators of mass shootings and targeted violence incidents often use social media platforms to proliferate their hatred of specific individuals or groups. In return, they can receive encouragement from these online communities to execute their violent plans. This is why it is necessary to combat these malicious actors at the source.

A New Report Card

For the past 25 years, the Simon Wiesenthal Center based in The Museum of Tolerance (MOT), Los Angeles, has released a yearly report assessing the digital health of web platforms with respect to the proliferation of hate and terrorism.

In this year's 2019 Digital Terrorism and Hate Report Card, the Wiesenthal Center tracked the continued emergence of Alt.Tech, a term used to describe a new generation of social media platforms that serve the agendas of Alt-Right groups. The Report Card also assessed the emergence of bigotry, anti-Semitism, and the glorification of radical Islamic terror on popular gaming platforms.[2]

Combat Hate: Promoting Digital Health for Students

To address the concerns raised by the 2019 Digital Terrorism and Hate Report Card, MOT kickstarted a

program targeting those who that are most vulnerable to online radicalization and hate: youth.

MOT, which functions as a human rights laboratory and the educational arm of the Simon Wiesenthal Center, is a trusted educational resource that works primarily with students in Los Angeles. MOT's vision is to promote a culture of accountability that challenges people of all backgrounds to confront their most closely held assumptions in order to prevent the proliferation of hatred.

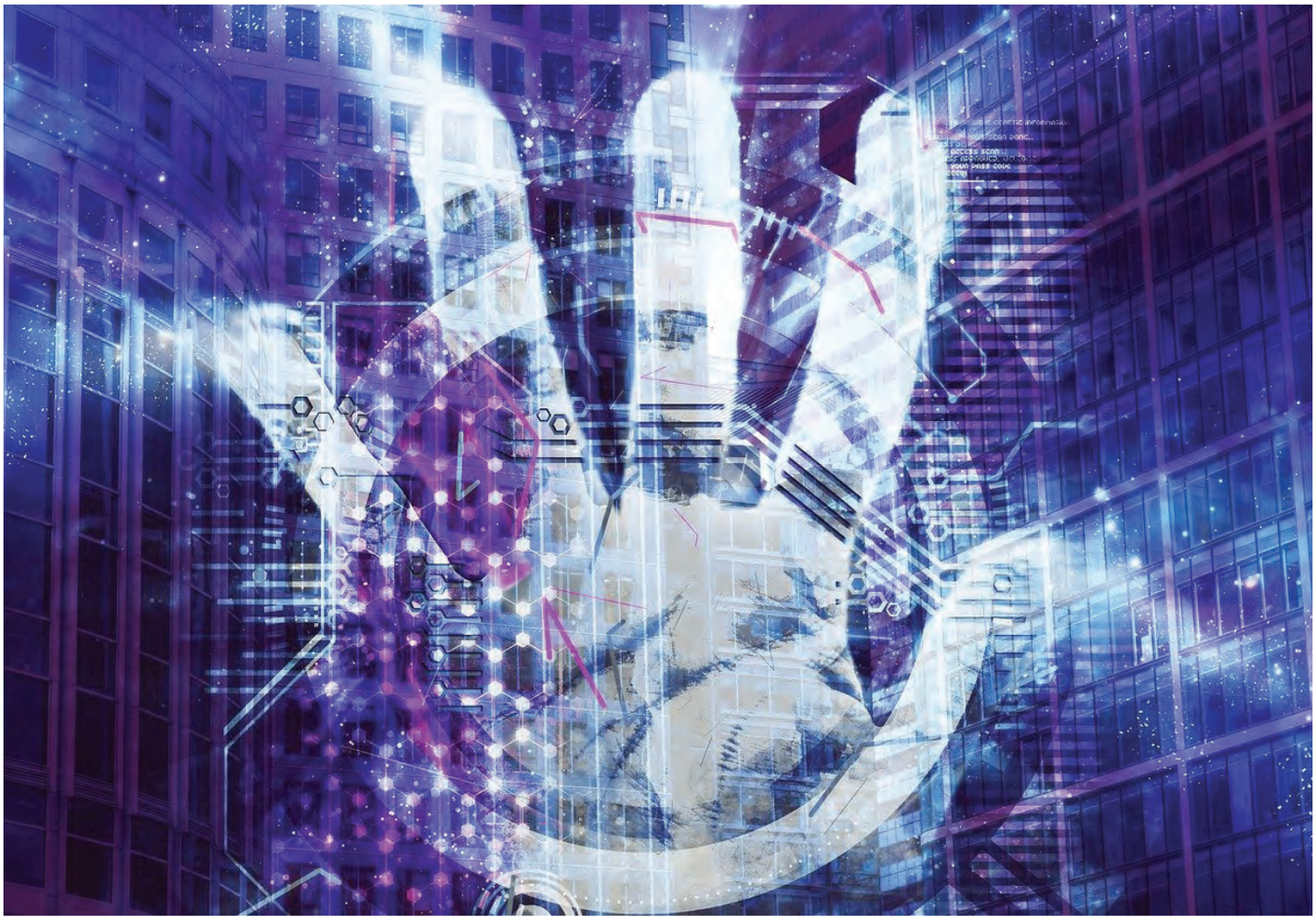
This led to the creation of the Combat Hate program. The Combat Hate program is a digital empowerment workshop targeting middle and high school students. It is designed to equip students to counter the perils of hate, prejudice, stereotyping and extremism in online social networking. The workshop is designed to take a whole community approach to tackling the potential threats young people encounter online, from extremists to extremist ideology.

Students are encouraged to think about:

- Who makes hateful posts online
- What is the intent behind hateful messaging
- Why do people post/share hateful content
- How to get help regarding suspicious online activity
- When is the right time to intervene in malicious online activity

MOT workshop facilitators pay visits to schools in Los Angeles and run hour-long workshops that foster much-needed dialogue among students, many of whom have seen or experienced cyber-attacks (most often in the form of cyber bullying and stereotyping). As a facilitator of the program, I was alarmed by how quickly young people can be exposed to extremist ideology. With just a few clicks, a young person could be connected to an extremist within minutes.

The urgent need for such educational programming earned Combat Hate a California Office of Emergency Services (CALOES) grant designed to give NGOs the opportunity to pilot new Prevent Violent Extremism (PVE) programs. This grant is an example of a growing joint-commitment by both the private and public sectors to address critical cyber threats. Efforts to integrate law



enforcement officers into Combat Hate's programming as workshop facilitators are now also underway.

MOT's vision is to establish better repertoire between students and law enforcement since the police force is ultimately responsible for intercepting the physical consequences of online hate. With local and state governments working together with community partners like MOT, Combat Hate is a prime example of the kinds of collaboration needed to address national challenges.

There is potential for this program to be replicated in cities beyond Los Angeles since its flexible structure allows for its evolution and modification for a broad range of audiences. Rick Eaton, senior researcher at the Simon Wiesenthal Center, hopes to see the program expand to other communities that are interested in PVE education for their students. With MOT offices in Chicago and New York, that vision is already on the horizon.

Educators as 'Digital Doctors'

As we move towards a future of advanced technological use, our education and law enforcement efforts must evolve with it. It is important to note that as we begin to prioritize preventing violent extremism as opposed to merely combatting it, the best agents of digital health are educators. Well-trained educators can teach the next generation about a cyber world that has the potential for both negative and positive impact. In order to promote the latter, educators can guide students towards empathy, media literacy, and digital empowerment.

Just as children are taught to look both ways before crossing a street, educators should see themselves as 'digital doctors' who can teach young people to pay close attention to the who, what, when, how and whys of social media messaging. The Combat Hate program at the Museum of Tolerance is a step in the right direction and has the potential to foster a generation of positive and healthy digital citizens.

With local and state governments working together with community partners like MOT, Combat Hate is a prime example of the kinds of collaboration needed to address national challenges.

Christina Chilin

Christina Chilin is a Master of Public Diplomacy candidate at the University of Southern California and the current president of the USC Society of Public Diplomats. Before beginning her graduate studies, she worked as a Designated School Official for the Office of International Students and Scholars at the University of California, Santa Barbara. In July 2019 she directed a cultural diplomacy program in Mexico that utilized cultural heritage as a gateway for professional collaboration. She is a trained facilitator for the Combat Hate program at the Museum of Tolerance in Los Angeles, California. Her current research interests are diaspora diplomacy and indigenous diplomacy.

Inquire. Innovate. Lead.

USC Annenberg
School for Communication and Journalism

MASTER OF PUBLIC DIPLOMACY

We prepare you to advance a more secure and vibrant globally connected landscape in one of the world's hubs for public diplomacy: Los Angeles.

A premier center for the arts, entertainment, media and technology, L.A. is home to more than 100 foreign consulates and a diverse array of diaspora populations. Here, you will work with our expert faculty to explore how governments and non-state actors can use media and communication to shape public opinion, international relations and public diplomacy for domestic and foreign audiences. You will learn how to further dialogue and understanding among individuals, cities, regions, nations and institutions.

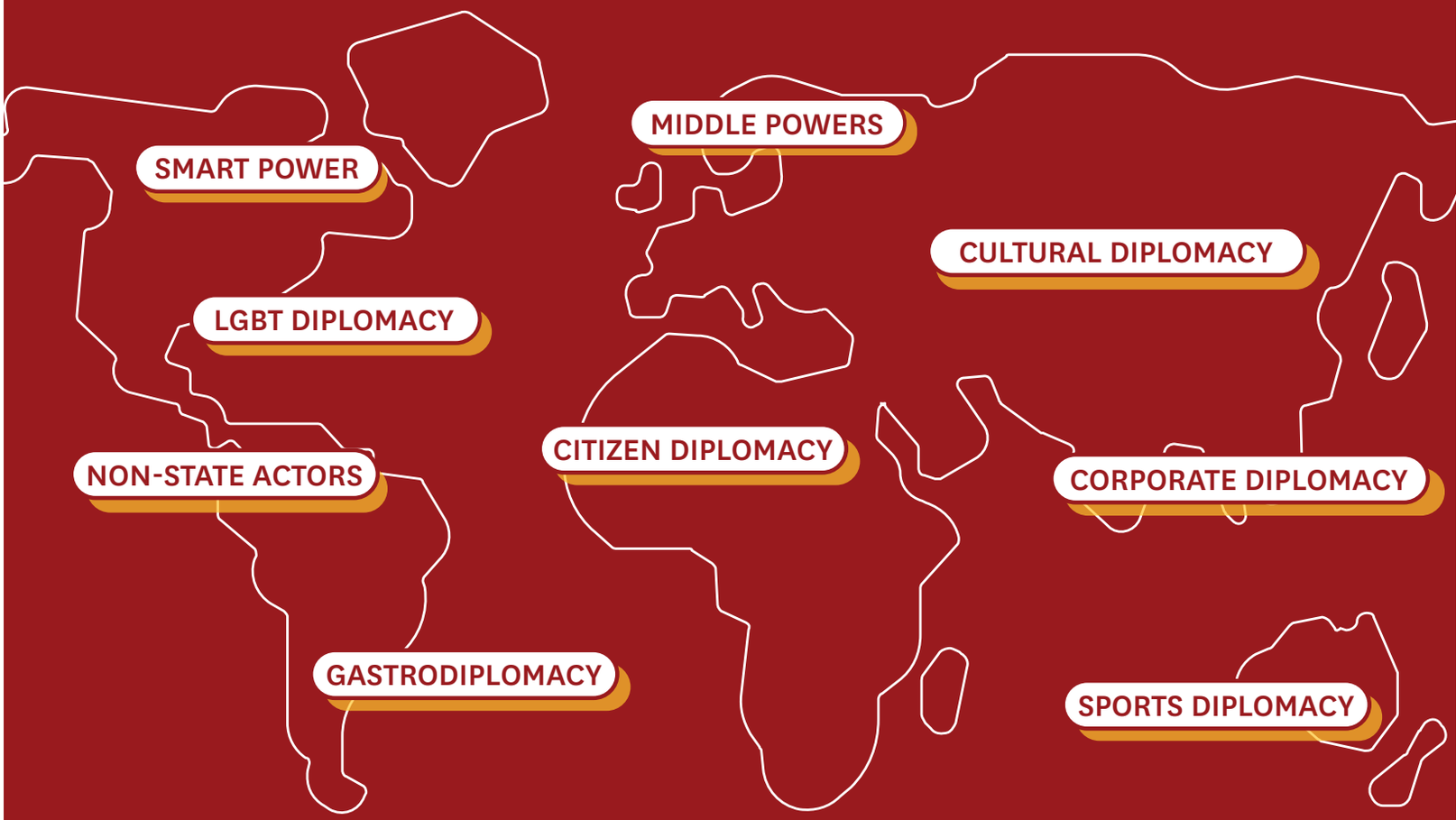
Learn more at annenberg.usc.edu

Member of the Association of Professional Schools of International Affairs

USC University of Southern California

USC Annenberg

USC University of Southern California



LEADING CHANGE ON A GLOBAL SCALE.

MASTER OF **PUBLIC DIPLOMACY**

annenberg.usc.edu

SOCIAL MEDIA: A POWERFUL CYBER ALLY

The Diplomatic Tower of Babel

Franklin T. Burroughs, Ed.D.

It is a strange, confusing season in diplomacy. Cyber, digital, net, and e-diplomacy have greatly expanded the possibilities and means for managing a country's international relations; they represent a century of change. They also raise concerns about cybersecurity breaches such as hacking, malware attacks, loss of data and cloud abuse. Differences in approach to cybersecurity, digital policy, and what might be considered normal diplomatic processes can sometimes create oppressive friction; this can result in misunderstanding and even conflict among nations.

In an article titled "China's Cyber Diplomacy: a Taste of Law to Come," which appeared in the online publication "The Diplomat" on January 14, 2015, Sonya Sceats talked about China's interest in and attempts at having the Internet regulated by states and the resulting protests from Western delegates at a conference dubbed the First World Internet Conference held near Shanghai. Despite the protests, "China's Internet Czar," Lu Wei, vowed to persist in promoting "Internet sovereignty," barriers built and maintained by a particular country and independent of international control. Such a vow inevitably leads to consternation by opponents and possible conflict.

But at least one traditional phenomenon challenges the ultimate effectiveness of "digital diplomacy:" the tendency of governments to push messages out rather than listening and creating dialogues.

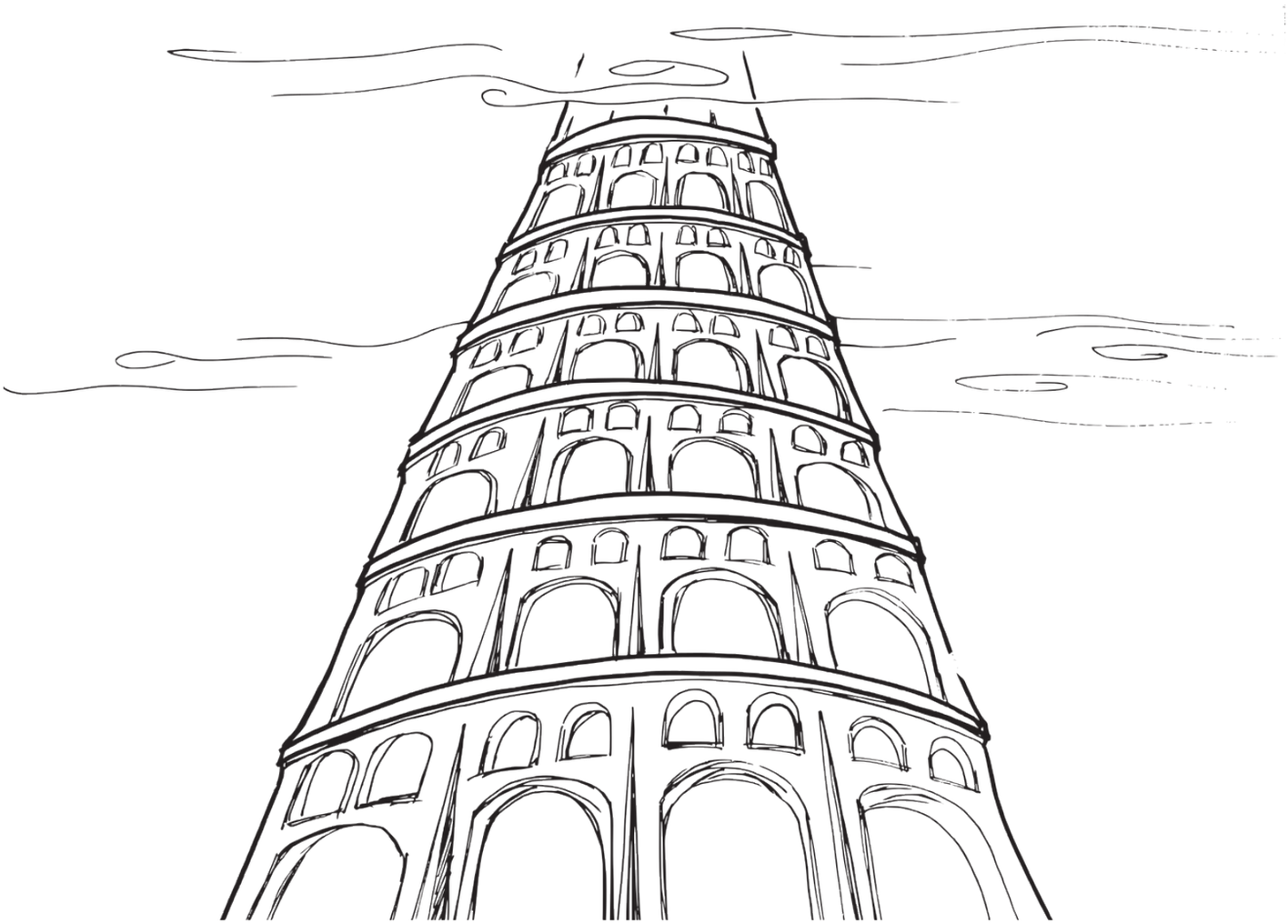
The United States and Russia seem to be developing different policies regarding and means for carrying out cyber-warfare based on their interpretations of international events and the availability of their resources. Mutual misunderstanding and divergent goals could result in a U.S.-Russia cyber war.

To avoid being viewed as diplomatic vermin, both professional diplomats and other actors on the international stage are using digital technology to transform the diplomatic process into what is often referred to as "digital diplomacy." This concept demands the replication of existing processes in digital form while transforming them into much more useful and better services. It focuses on the personal and individual use of information and communication technology (ICT) like Twitter, Facebook and YouTube to communicate with other individuals.

But at least one traditional phenomenon challenges the ultimate effectiveness of "digital diplomacy": the tendency of governments to push messages out rather than listening and creating dialogues. This more aggressive approach to communication requires the integration of ICT. This tendency has birthed "cyber diplomacy."

World powers often focus on such global issues as migration, peace and security, human rights, international law and justice, and ending poverty; the powers tend to adopt broad strategies for addressing the issues and use wide networks of ICT to express their current views and ideas of the future. They incorporate virtual reality into their foreign policies and use "cyber diplomacy" to promote their concept of an international society.

The current diplomatic season remains somewhat confusing. The overlapping use of the terms public, digital, and cyber diplomacy can create confusion about their meanings and relationships. Social media platforms like Twitter, Facebook, and Instagram can be used to communicate with foreign publics but can also bring about uncertainty and mistrust if employed by



individuals or groups not familiar with or opposed to the message being conveyed.

For many years, the conduct of diplomacy was viewed as a secretive process carried out between and among officials and politicians. The focus remained on nation-states and government bureaucracies. Elitism characterized much of the diplomatic activity, and, to the extent possible, the diplomatic activities were shielded from public view.

As early as the 1960s, however, both the public and media became increasingly involved in digital diplomacy, creating the sometimes unpredictable diplomatic season that has persisted until today. It is hoped that the strange and confusing season soon gives way to a universally known and acceptable season in which a single system that uses integrated data for multiple purposes will simplify diplomacy, improve the management of diplomatic data, and encourage international dialogic communication. Perhaps such a system can affect positive changes in the world order.

Franklin T. Burroughs

Franklin T. Burroughs, Ed.D. is a USC Center on Public Diplomacy Blog Contributor and Contractor and Teacher at the U.S. Department of State and John F. Kennedy University.

The U.S. Embassy's Microblog Diplomacy on Sina Weibo

Yuqi Ning

First proposed in 2001, digital diplomacy has entered the arena of public diplomacy naturally with technological advancements leading to innovations in information and communication.[1] By 2008, the term "Public Diplomacy 2.0" had been proposed by scholars, referring to the tendency that public diplomacy intertwines with online media.[2] Microblog diplomacy thus emerged in this context.

The actors in microblog diplomacy are evolving from traditional entities like government organizations, NGOs and the media to now include the mass of online social media accounts used to engage users with diverse issues through the functions of reposting, commenting and liking.

Among all the actors of public diplomacy, China and the United States are the most studied in this field, as China-U.S. relations greatly affect the world. Since the establishment of the People's Republic of China in 1949, China and the United States have experienced a variety of phases in their relationship, including tense standoffs, conflict mitigation and even cooperation with one another. In the digital era, both countries have switched their tactics of traditional communication activities into indirect digital diplomatic methods like microblog diplomacy to exert influence and facilitate interaction. Therefore, research on microblog diplomacy between China and the United States is of great significance.

U.S. Public Diplomacy on China's Sina Weibo Platform

Sina Weibo (or simply Weibo), the most influential microblogging website in China, resembles Twitter's role in American digital diplomacy. A number of governmental organizations have launched authenticated accounts on Weibo in order to reach China's public. Among all the embassies' Weibo accounts in China, the U.S. Embassy is the most dynamic with more than 2.4 million followers.

Regarding the significance of China-U.S. relations and the vigor of microblog diplomacy, this essay examines the contents and the online engagement of the U.S. Embassy's microblog, summarizes its features and seeks to answer the following two questions:

1. What are the factors influencing the interactions between the U.S. Embassy and Weibo users in China?

2. What are the key features of the U.S. Embassy's microblog diplomacy?

Upon analysis of the data collected, some solutions and tactics will be proposed to promote the efficiency of communication and mutual understanding between China and the United States.

Case Study: Methodology

We will be observing the U.S. Embassy's Weibo account as the subject for this study. The chosen samples are the Embassy's Weibo posts from January 1, 2019 to October 1, 2019. Using the latest samples guarantees a rather accurate result. The sample data is collected from two dimensions, namely the sample contents and degree of engagement. Based on the contents, the posts are classified into eight categories: politics, economy, culture, sports, health, security, environment, and science and education. The degree of engagement is measured by the average number of likes, reposts and comments.

The findings of the case study will be evaluated under the framework of the Four "E's" Strategy in order to explore the key features of America's microblog diplomacy. The Four "E's" Strategy was proposed by Karen Hughes, the

former Under Secretary of State for Public Diplomacy, and stands for Engagement, Exchange, Education and Empowerment.[3]

Case Study: Findings

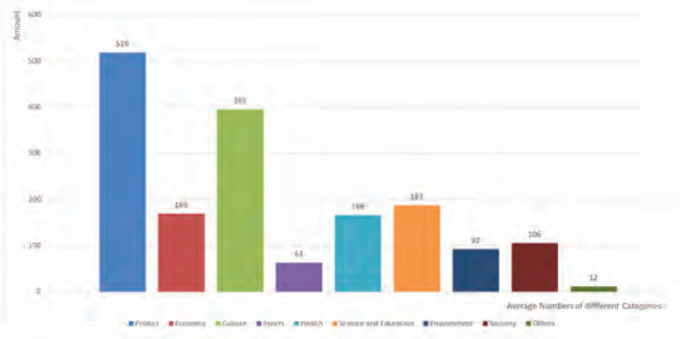
The posts on the U.S. Embassy's Weibo account from January 1, 2019 to October 1, 2019 are computed and classified into eight categories, with the statistics shown in the table below.

Figure 1. U.S. Embassy's Weibo Account Posts

Categories	Number of Entries	Total number of Likes	Total number of Comments	Total number of Reposts
1. Politics	519	413090	191797	59369
2. Economy	169	149022	76736	28501
3. Culture	395	344078	110668	38639
4. Sports	63	59026	11528	4725
5. Health	166	109992	34826	10382
6. Science and Education	187	137951	41484	16528
7. Environment	92	55656	21819	5757
8. Security	106	133203	45536	10390
9. Others	12	4231	2993	1225
Total	1709	1406249	537387	175516

From January 2019 to October 2019, the U.S. Embassy's Weibo account account posted more than 1,700 times, addressing a number of different issues. According to Table 1, more than 30% of the entries were related to politics, followed by culture, science and education, economy and health, with sports coming in last. On average, the U.S. Embassy's Weibo account posts more than five entries in one day through the forms of plain text, pictures and videos.

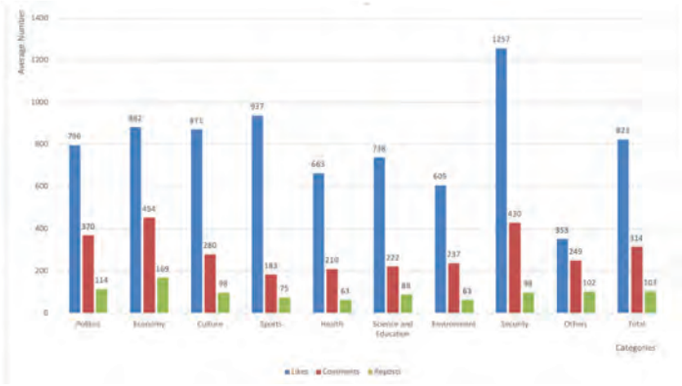
Figure 2. The 8 Major Types of Content Produced By the U.S. Embassy's Weibo Account (1 Jan 2019 - 1 Oct 2019)



What type of content is most popular on U.S. Embassy's Weibo Account?

The interactions or degree of engagement on the U.S. Embassy's Weibo account is embodied in three dimensions: likes, comments and reposts. The average number of likes, comments and reposts are calculated in the following chart.

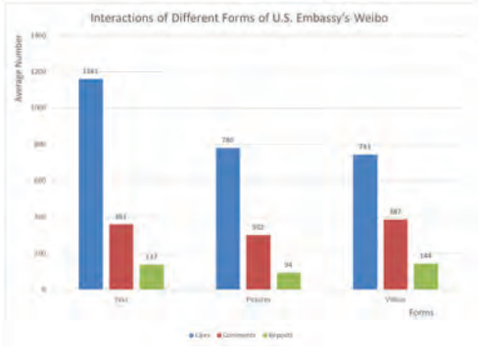
Figure 3. Engagement on U.S. Embassy's Weibo Account



Microblogs relating to different topics evoke different responses, demonstrated in the varying number of likes, comments and reposts. Figure 3 demonstrates that Chinese Weibo users are especially concerned with issues of security, including terrorism, the refugee crisis, human trafficking and cyber security. Microblogs related to the economy, sports, and culture provoke more likes than average, with those relating to the economy enjoying the most comments and reposts. The interaction with microblogs on environmental issues like global warming and pollution are relatively low in China at present.

In addition, the varying forms of microblogs – text, pictures and videos – provoke different kinds of engagement. Microblogs in the form of text gain the most likes, 1,161 on average, while videos provoke more comments and reposts.

Figure 4. Engagement with Different Forms of Microblogs on U.S. Embassy's Weibo Account



Case Study: Discussion

Based on the analysis of the 1,709 microblogs, it is evident that microblog content related to security, economic, and sports issues outweighed those of political, educational, and environmental issues in the degree of engagement.

The average number of likes received on political posts is below the average level; thus, it can be inferred that Chinese Weibo users are reluctant to be involved in political discussions. The high level of engagement with global issues like security and the economy are most likely a product of the recent trade frictions between China and the United States.

Among the 1,709 entries in 2019, only 63 of them were about sports. However, its amount of 'likes' ranks the second highest after security, which is due to the popularity of athletic leagues like the NBA in China.

Based on the data, it seems that the common perception regarding multimedia forms like images and video as being more 'attractive' to users than information-rendering forms like text is not true. Text-based microblogs still enjoy the most likes while videos receive the most comments and reposts. There may be less engagement on the U.S. Embassy's video and image content because its multimedia content is rigid to some extent. Most of the pictures posted are of formal conferences, portraits, and press meetings, and some videos lack a clear narrative and fail to showcase memorable highlights. The Chinese audience seems to be gradually losing interest in the ordinary enumeration of facts, even if its packaged in a variety of multimedia forms.

The Key Features of the U.S. Embassy's Microblog Diplomacy

Zhou Qingan from Tsinghua University proposed five modes of public diplomacy: repairing mode, constructing mode, influencing mode, infiltrating mode and subversion mode. The modes are listed according to the intensity of motive from negative and defensive to positive and aggressive.[4]

The direct participation of the United States government in promoting government policies and exporting ideology is rare in Weibo. Instead, the U.S. Embassy is actively introducing the social condition, activities, history and culture of the United States to a Chinese audience, explaining America's positioning on global issues. Considering the high frequency of the U.S. Embassy's microblog posts, it can be classified under "influencing mode."

The features of the U.S. Embassy's microblog diplomacy can also be examined under the framework of the previously mentioned Four "E's" Strategy. The first layer is "Engagement," which the data shows to be stable. The U.S. Embassy's frequency of posting on Weibo and the degree of interactions are stable, despite the relative differences in the distribution of posts among the eight content categories.

The second layer is "Exchange," with bilateral exchange as its key. "Bilateral" here means embracing Chinese elements in its microblog subject-matter. It is evident that U.S. Embassy's microblogs attempt to establish common ground with Chinese Weibo users by creating posts such as, "40 Years Between America and China." One microblog about America's National Football League (NFL) mentioned Chinese idol Kris Wu and gained 210,000 likes, around 1,000 comments, and more than 2,300 reposts. The inclusion of Chinese elements in microblogs enhance the efficiency of communication between the two countries.

The third layer is "Education," which comes in the form of short lessons in English grammar, American history, U.S. ideology in its Weibo posts. However, these lessons are often conveyed in a way that is prosaic and can come off as indoctrinating, which produces lowers levels of engagement among Chinese audiences. Hence, there is room for improvement in this area.

The fourth and final layer is "Empowerment." The U.S. Embassy chose to take the initiative to set up an account on the Chinese platform, Sina Weibo, giving Chinese netizens a platform to share their opinions, whether positive or negative, and question the U.S. directly. This platform empowers Chinese Weibo users, laying the foundation of building mutual understanding and trust.

Yuqi Ning

Yuqi Ning is a Master's degree candidate at Tsinghua University, China in Journalism and Communications. Her research interests are in public diplomacy and international communications. She obtained her Bachelor's degree in English Literature from Tianjin University, and in Finance from Nankai University. She was previously an intern Editor at Xinhua News Agency in Beijing and an intern Journalist at the European Bureau of China Daily in Brussels. The experience of being part of the Student Press Program of the US Embassy has encouraged her interest in American communication studies.

China: Winning Hearts on the Web

While China is trying to fight the China-U.S. trade war, it is also quickly gaining new territory in the cyber-realm, thanks to its great social media presence and foreign investments.

Lindsay Cai

The Cultural Revolution from 1968-1978 and the Tiananmen Square Protests of 1989 reflect censorship's long history in China. Today, the People's Republic of China (PRC) employs the most extensive censorship systems in the world. According to The Washington Post, Xi Jingping's appointment to the General Secretary of the Communist Party of China (CCP) has "significantly stepped up" censorship since 2012.[1] Right now, there are over 2,000,000 censors employed by the CCP; they screen content of all forms, including literature, television, news, film, text messages, and the Internet.

While censorship of the Internet is nothing new, the Chinese government has begun to implement unprecedented controls over the cyber realm as the Chinese public spends more time online. In 2018, 829 million netizens in China (that's more than two-and-a-half times the population of the U.S.) spent an average of one hour on social media sites per day.[2] Under this stricter censorship system, the Chinese government has developed unique ways of utilizing the digital realm to influence users on Chinese social media platforms, especially amidst the current China-U.S. trade war.

According to Kaiser Kuo, the internet in China is largely used for entertainment purposes and thus is referred to as the "entertainment superhighway."

Since 2018, the China-U.S. trade war has been an ongoing economic battle between the world's two largest national economies. The conflict, initiated by U.S. President Donald Trump, has an end-goal of forcing China to reverse what the U.S. deems "unfair trade practices."[3] The U.S. has also accused China of intellectual property theft along with the forced transfer of American technology to China.

In the meantime, China has successfully branded itself on state-run social media platforms as a victim of the U.S.'s insolence, helping China's policies gain the unconditional support of many Chinese nationals. Even young children in China are now conditioned to this messaging and have been filmed speaking out against the U.S.

Partnerships with Entertainment Platforms

According to Kaiser Kuo, the internet in China is largely used for entertainment purposes and thus is referred to as the "entertainment superhighway."[4] Therefore, the Chinese government has strategically partnered with entertainment platforms to deliver its policy messages. For example, XINWEN LIANBO, China's most famous daily news program produced by China Central Television (CCTV), began posting political commentary videos on the video sharing platform Douyin (known as Tik Tok in the US) this year. Douyin/Tik Tok, a platform with over 330 million active users under the age of 30, attracts users eager to consume stimulating, short, and amusing video content.[5] While news outlets are not yet popular on the platform, CCTV hosts Kang Hui and Hai Xia have successfully utilized Tik Tok to created viral short, humorous videos poking fun at U.S. policies. They have since attracted a large Chinese following.

On February 3, 2018, the Chinese government also instituted a "makeover" of Weibo, a popular Chinese social media app comparable to Twitter. With the "makeover," the app's signature 'Hot 50 List' feature

was required to save the number one spot for Chinese government news. In addition, Weibo added a new list on its homepage featured next to the 'Hot 50 List' titled "New Era" (新时代). Under this category, Chinese audiences can view detailed political activities and updates in real time. Weibo has became one of the main platforms for the promulgation of the Chinese perspective of the trade war with over 4,000 related-articles now available to users on the app. Weibo's function as a tool for mostly entertainment purposes has now evolved into an arm of Chinese domestic propaganda. Consequently, many Chinese netizens are only exposed to the CCP's stance on the conflict. Some even believe that the U.S. has already lost the trade war.

Even now, pro-CCP articles teem on the Internet in defense of President Xi's policies. Major Chinese media outlets such as Xinhua News, People's Daily, The Beijing News, and Guangming Daily harness their influence on the cyberworld to promote their skepticism and disapproval of the Trump administration's actions. When the highly-anticipated trade war debate between China Global Television Network (CGTV) host Liu Xin and Fox Business Network host Trish Regan aired in May 2019, many people in the West were unaware of the debate. However, the opposite was true in China as Chinese media encouraged netizens to live-stream the event. Following the debate, Chinese commentators online characterized Liu's speech as "confident, fluent, and successful" while diminishing Regan's performance as "terrible and inexperienced."[6] This prompted many Chinese media influencers from across different industries—culture, entertainment, business, and even food and travel—to simultaneously share and forward their comments.

China's Cyber-Diplomacy Initiatives

While the digital age has ushered in an era of more innovative methods of leading public opinion since Mao, one thing has not changed: China is preventing democratic processes in order to maintain a firm grip of power. China has eliminated Twitter, Facebook, and Google in its effort to build a Great Firewall around its cyber-realm, further distancing itself from the threats of Western liberalism.

In addition, there are signs that China is extending this firewall across its borders into other countries. After the US-China trade war commenced, the Chinese government began to meet with trading-partners such as Ethiopia, Sudan, Egypt, and Tanzania more frequently in order to conduct "cyber-diplomacy" initiatives, namely providing those countries with advanced AI and facial recognition technology at a low rate or even free of charge.

According to Freedom House, Zimbabwe reached an agreement with a Guangzhou-based software company, CloudWalk Technology Co., Ltd. to build a national facial recognition system for Zimbabwe's cities and public transport stations.[7] In exchange, China wishes to export its Great Firewall system into Zimbabwe and gain their support in the China-U.S. trade war. At least 38 countries have also installed Chinese-made telecommunications systems, including Nigeria: in 2018, a Chinese company won the contract for the construction of telecommunications networks in all of Nigeria's airports.[8]

Helping other countries to bolster their content control mechanisms are a sign that aside from winning the trade war, China hopes to export its values to other countries at the expense of freedom.

Lindsay Cai

Lindsay Cai is a staff writer for the Public Diplomacy Magazine and a journalist for USC US-China Today. She was born in mainland China and moved to Los Angeles with her family at 14. She is the author of two books; her first book was published when she was still in high school and her second book in 2019. In her books, she writes from a riveting first-person account about the major cultural, educational, and political differences between East Asia and the United States. In the future, she hopes to use her observations to craft powerful messages that will help reduce miscommunication between China and the U.S.

YouTubers as Digital Ambassadors: A Case Study of Ychina

Sometimes the best public diplomacy is when a country has someone else tell their story for them.

Jingzhen Yang

Ychina, a popular YouTube channel based in China, was launched in 2016 by Raz Gal Or, an Israeli student who graduated from Peking University's School of International Studies. Gal Or, more commonly known by his Mandarin name Gao Yousi, launched this platform after drawing public attention for his participation in the Chinese television talk show *A Bright World*. Capitalizing on this media momentum, the 23-year-old began starring in his own online videos that captured the perspectives of foreigners studying or working in China.

Ychina: A Window into the "Real China"

Initially, Gao's objective was to cultivate mutual understanding between foreigners living in China and the Chinese public. However, as Gao spent more time living in China, he embarked on a new goal: showcasing to the world his perspective of the "real China." In 2017, Gao started a YouTube documentary-series titled "Experience China," and in each episode, Gao is filmed spending one day employed in one of China's emerging occupations, i.e. as a cyber-café host, food-delivery boy, and subway worker. What is more, several of these episodes are filmed in China's countryside, showcasing the realities of Chinese life outside of its glimmering metropolises.

Ychina's content, which is often humorous and heartfelt, surged in popularity both domestically and internationally. Today, Gao has 126,000 followers on YouTube and 510,000 fans on Facebook, and over 50 million followers and an average of 250 million views per month via Chinese social media platforms.

Gao's ability to tell "China's story" eventually caught the attention of official Chinese state-run media *Xinhua News Agency*, the largest and most influential media organization in China. *Xinhua News Agency* transmitted several of *Ychina's* videos on its Facebook account, marking a turning-point for *Ychina*: its content had been recognized for its potential to be incorporated into China's public diplomacy outreach online.

Aspiring digital ambassadors who would like to similarly yield influence in the cyber realm can learn from Gao's approach in both storytelling and collaborations with state and non-state actors.

3 key factors in Gao's success as a digital ambassador are:

1. He produces videos in cooperation with a variety of other social media influencers

2. He establishes and maintains close relationships with fans i.e. through video collaborations with *Ychina* followers

3. His platform's objectives are in harmony with the public diplomacy objectives of the Chinese government

In short, by creating a channel to spread "China's story," *Ychina* is an example of how content creators are successfully building their own niche corners in the cyber realm and have unintentionally become powerful "digital ambassadors" who serve to inform, understand and influence the foreign public. As non-state actors, they are more readily received by public audiences and can traverse new territories considered "inaccessible" to traditional state actors. Gao's added edge is that he is a foreigner telling "China's story," giving him greater credibility among international audiences.

The cyberworld has created new opportunities for grassroots public diplomacy, giving YouTubers like Gao a platform to be rising stars in an age of cyber-diplomacy.

Gao's added edge is that he is a foreigner telling "China's story," giving him greater credibility among international audiences.

Jingzhen Yang

Jingzhen Yang is pursuing a Master of Communication Studies at Renmin University of China. Prior to that, she received her Bachelor's degree in Publishing and Editing at Wuhan University in 2018. Jingzhen is passionate about new media and youth political socialization in the current digital age.

Defeats and Defects of Spanish Cyber-diplomacy in the Arab World

This case study aims to reveal the linguistic deficiencies in the Facebook messaging of Spanish Embassies in the Arab world.

Samer Alnasir

Geographically situated as the nearest European-occidental nation to the Arab world, with physical involvement within two cities in the African Nordic Coast and within the Canaries Archipelago, Spain's involvement in this area of the world begets both nostalgia and resentment for Arab people. It brings to mind the United States and its involvement with the Hispanic world through Puerto Rico, though the Spanish example is only one instance in the country's history dating back to the 16th century. This socio-political involvement brings the demographic makeup of Spain to mind. Spain has a large number of Arabic citizens who originate from these cities and who are originally Spanish citizens under full Spanish sovereignty.[1] Therefore, Spain has access to a large reserve of Arabic human resources; however, they are not fully integrated in the public political sphere or in Spain's diplomatic missions in the Arab world.

The Spanish Strategic Vision for Asia 2018-2023 sets as one of its aims: "studying the form of use of the commercial and economic potential of the second generation Asiatic immigrants in Spain" (Object. 16, Vision of Asia Strategic plan, p. 27). The country is studying how to best include the second generation of Asiatic immigrants in the commercial and economic potential of its foreign affairs strategy, yet herein lies a problem. The second generation of Asiatic immigrants they refer to are not "second generation" at all; they have been living under Spanish sovereignty since the 16th century. Despite this fact, they are considered second generation "administrative citizens," meaning that although some may now have Spanish identification, they are seen as immigrants and not given any effective rights in Spain. Spain is still avoiding the involvement of their Arabic citizens' potential as a whole by considering them as immigrants, though many of them come from Spanish territories dating back five centuries.

Spanish Public Diplomacy via Facebook

The current situation regarding Spanish Embassies' messaging in the Arab world is still missing an effective standardized public cyber-diplomacy strategy. In Tunisia, for example, while the Tunisian constitution establishes the Arabic language as an official language of the Republic of Tunisia, and while the Spanish constitution establishes Spanish as the official language of the Kingdom of Spain, the Spanish Embassy in Tunisia's Facebook account is exclusively delivered in French and English, not in Arabic or Spanish. In Morocco, where the situation is similar, the Spanish Mission uses bilingual messaging in Arabic and French. These are clear examples of the significant language defects in Spain's cyber messaging strategy that are worth noting.

On October 25, 2018, the Spanish Embassy in Qatar published a message on its Facebook in the Arabic language announcing the «forfeiture by Spain of the European film festival by beating a Spanish movie...» (Figure 1).[2] Apparently, they used a direct translation of the word "close" translated literally by a standard

dictionary to the Arabic "forfeiture." Similarly, by translating the word "projection" in the same way, they produced a wrong translation for "beating." Therefore, the whole message became a denigrated message.

Figure 1. The Spanish embassy in Qatar incorrectly announces the forfeiture of the European film festival by beating the Spanish film...etc.

In another post by the Spanish Embassy in Morocco, the Embassy attempted to announce the visit of His Majesty the King of Spain Don Philip and Her Majesty the Queen of Spain Doña Letizia to Morocco.[3] The Arabic text, however, showed a significant defect. The Embassy failed to translate the titles «His Majesty», «Mister» or «Miss» in the Arabic language, so they settled for a transliteration of the Spanish pronunciation in Arabic letters, as shown in Figure 3.

Figure 2. The Spanish Embassy Facebook account in Morocco failed to properly announce the visit of Don Philippe and Doña Letizia to Morocco in Arabic.

That text resulted in derision of the Spanish Embassy by internauts, but it appears that the derisive messages issued in Arabic were not even understood by the page manager as something to be corrected (Figure 3).

Figure 3. An Arab internaut's derision of the Spanish Embassy's attempt to "create" the Arabic expressions for the Spanish terms «don» and «doña», which are unprecedented in the Arabic language.

Moreover, this post (Fig. 2) has been repeatedly used by the local media in Morocco without any changes. They incorrectly understood the Arabic transliterations of «don» and «doña» to be part of the Spanish King and Queen's names themselves, adding the title His Majesty to the transliterations of the embassy text «نوض». Only one media outlet understood the error in the post, placing quotation marks around the Arabic transliterations of «don» and «doña» to avoid perpetuating further misunderstandings while keeping the rest of the text in its original format (Figure 4):[4]

Figure 4. One local Moroccan media replicated the Spanish Embassy's press release (see Fig. 3) and placed the word «نوض» in quotations because it has no meaning in the Arabic language.

Spanish public diplomacy is also carried out by the Cervantes Institute which serves as the cultural arm of diplomatic missions. Cervantes Institutes are committed by law to promote Spanish language and culture around the world. Theoretically, these Institutes have better access to linguistic resources and instruments, yet their Facebook messaging in the Arab world also seems to experience the same issues as the Spanish Embassies.

Most of the posts published on the Institute's Morocco Facebook account are in French, which is neither the Moroccan local language nor the language of Spain. Overall, their Facebook posts are a melánge of French, Arabic and Spanish messages, lacking overall cohesion. Figure 5 below provides an example of this. The disparity begs the question, "Is the Cervantes Institute a Spanish or a French cultural center?"

Figure 5. A post from the Cervantes Institute of Marrakesh - Morocco Facebook site. It is an invitation to a Spanish music concert chaotically published in Spanish and French.[5]

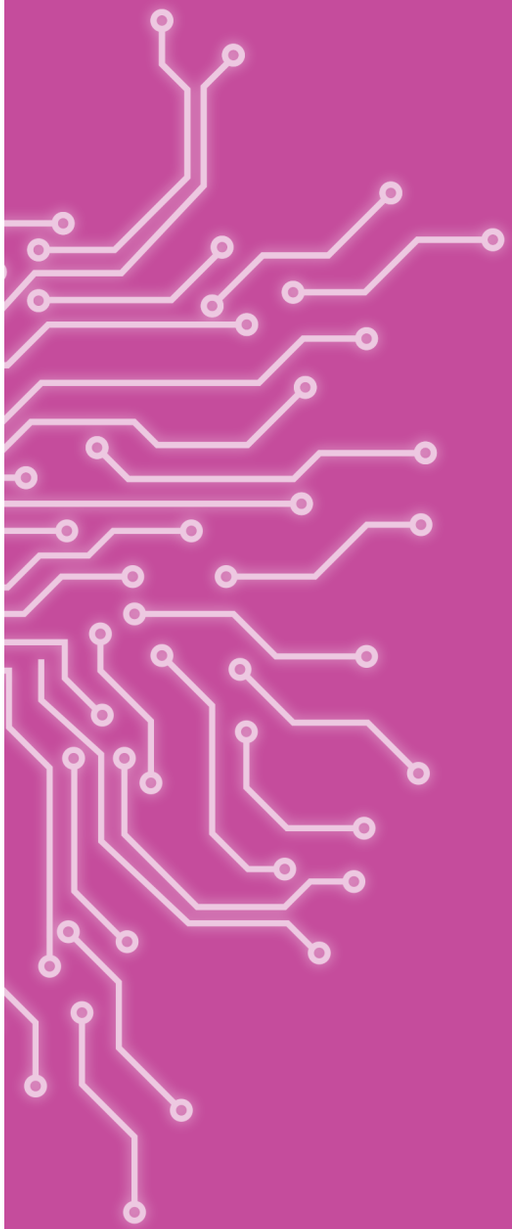
Conclusion

The exhibited language defeats and defects made by Spanish Embassies in the Arab world can be easily committed by any other administration that forgets the significance of cyber-diplomacy as it is an emerging, new form of diplomacy, not simply part of another type of diplomacy (Manfredi, 2014, p.6). Further,

the aim of cyber-diplomacy is to generate mutual understanding, not confusion (Gershenson, 2013, p.14). Unfortunately, the case study of Spain's social media outreach in Arab countries like Morocco, Qatar, and Tunisia demonstrate that cyber-diplomacy still remains unmastered in practice. This is occurring despite having ample human resources available to Spain through the Arab "administrative citizens" under their sovereignty whom Spain has yet to treat as full Spanish citizens and effectively integrate into Spanish society.

Samer Alnasir

Samer Alnasir is an Associate Professor of Legal History at the University of Carlos III of Madrid.



PREPARING FOR THE CYBER FUTURE

Bottom Lines and Data Dossiers: How Big Tech Commodifies Your Privacy

Devin Villacis

By many accounts, the world in which we currently live in is characterized by political division, wealth inequality, tenuous security protections, and the evasive corporations lacking in fundamental transparency who seem to benefit from it all. The corrosive relationship between greed and democracy is one that has plagued the United States since its inception, take for example the legacy of slavery or, to a lesser extreme, the imbalance of wealth and interests following the Industrial Revolution.[1] Who then serves to gain from the imbalance of 2019? The answer seems obvious, the technology companies that have become at once invaluable resources and not-so-hidden 'surveillors,' manipulators, and data auctioneers.

Network Effects

Both legal scholars, Jack Balkin refers to the time in which we currently live as the 'digital revolution' meanwhile, Julie Cohen calls this the shift from 'industrialism to informationalism.'[2;3] No matter what we call it, we can all agree we are living in the Information Age. Current political economy theorists have centered their arguments about the proliferation of information networks on governance over the last few decades. Fundamentally, with the rise of cyberspace, power has shifted away from sovereign states and toward their citizenry. Political scientist David Lake describes this new public power stating, "No longer are groups merely struggling against domestic policy rivals, and taking the rest of the world as fixed, but they are pursuing their aims in combination with other similarly strategic actors at home and abroad."[4] Online, the public is capable of finding like-minded individuals all over the world, form networks, and change policy. It would stand to reason then, that in a world dominated by information networks, whoever has the largest network holds the most cards. Though we can also apply the principles of "network effects, whereby, according to Metcalfe's law, the value of a network increases in proportion to the square of connections."[5] In recent years the organizations with the largest networks have been gigantic companies that connect to communities all over the world.

Those companies, like the telecommunications companies that came before them and exist among them, understand this concept well. In order to grow their businesses globally, they go to great lengths to shut out market competitors who threaten network dominance. Political economy theorist Jonathan Hardy writes, "In the ensuing 'winner-takes-all' markets, the gap between the number one and number two players is typically large and growing, generating new concentrations."[6] Facebook in particular has acquired over 70 companies since the company was founded in 2004.[7] Professors Robert McChesney and Dan Schiller expand on the two-fold result of this strategy as it applies to largely offline media companies. The first is that companies perceive themselves to be "supranational entities," not bound to any nation; the second, is "the rise of a global corporate media oligopoly."[8] The same of course can be said for the online tech companies that have grown out of the digital revolution.

As these companies grow worldwide, most no longer consider themselves to be fixed to the shores on which

they were built for good reason. Ultimately, though they are in fact subject to the laws of the countries in which they exist (and are capable of funding massive lobbying efforts to influence those laws), the platforms produced by these organizations can also be the ones on which, for example, political movements begin. As we now well know, they can also be home to quiet state-run campaigns against rival nations from within. Furthermore, when the same few companies are eating up competitors, there is in fact incredibly limited competition. For the purposes of this paper I will seek to outline a third outcome that is a result of the first two: lawless companies with so much network power they can and do override government and public interests for the sake of profit.

Balkin's 'Grand Bargain'

In 2018, Facebook made $55.838 billion in revenue, Alphabet (parent company of Google) made $136.819 billion in revenue, and Apple had $107.147 billion in total shareholders' equity.[9;10;11] Facebook was only 14-years-old at the time, and Google only 20. These margins are very much in line with telecommunications giants, like Comcast (owners of a significant portion of the telecommunications infrastructure in the U.S., as well as, of content creators like NBC Universal) which made $94.507 billion in revenue over that same period.[12;13] With the exception of Apple, the services provided by these technology companies come on a seemingly free basis. Armed with only your email address, you can have nearly unlimited access to YouTube, Instagram, Facebook, Google, Twitter, Snapchat, the list goes on and on.

How then do these companies, who frequently ask for no monetary compensation, amass such incredible amounts of wealth in such short periods of time? Balkin refers us to the "grand bargain of twenty-first-century media." He explains, "Privately-owned infrastructure companies will provide you with many different valuable services. … End-users get all of these services, all of this stuff – and they get it all for free. And in return, media owners get to collect their data, analyze it, and use it to predict, control, and nudge what end-users do."[14] Meaning, the product, the profit, the price of those services, if you will, comes from you, the consumer – suddenly a traceable, tangible set of data that follows you around through cyberspace. Why is this data of such incredible value? Because with that data advertisers can target consumers personally to boost sales. Why would you waste valuable resources advertising chic new Nikes to the masses, when you could target 18 to 22-year-old women in college with disposable incomes. From there you would want to know which ones like to follow trends, which ones like the Nike brand, which might be interested in pairing a newly bought maxi dress with a pair of new sneakers. These are all easily acquired pieces of information once you have their transaction history, their history with 'likes' on different social media platforms, and so on. Retired Harvard Business School professor Shoshana Zuboff calls this, "surveillance capitalism," defined by her as a "new form of information capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control."[15] Companies like Facebook and Google earn revenue by selling to advertisers looking to use their "digital dossiers

about individuals," as well as their platforms, to target consumers and boost performance.[16]

Collecting and utilizing data for profit is not in and of itself a wicked act. It would appear this is just capitalism at work in the Information Age, where resources, in this case data, are used effectively and efficiently. Many countries pride themselves on 'innovation' allegedly best served by the free flow of information. Innovation is thus an oft-cited reason for why protections on data could ultimately stunt growth. Many argue that without looser regulations the U.S. could be outpaced in fields like artificial intelligence, and lose out to countries like China, whose lack of restrictions allow them to create larger data pools.[17]

Similarly, Apple in some cases uses data to meet the end-user's needs, for instance to make iPhones better with every generation. This practice though, has met scrutiny. In one publicized example, the company used contract workers to analyze snippets of sound collected by iPhone's virtual assistant, Siri, to determine the quality of her responses. Per the company, the data was intended to improve future iterations of the virtual assistant.[18] Of course, however, a higher quality Siri would ultimately also improve the company's bottom line. Siri users, meanwhile, were likely alarmed when, in late July 2019, Guardian journalist Alex Hern reported that Siri recorded user audio, even when users did not intend for the system to be active, and sent that sound back for analysis. A whistleblower told the newspaper that oftentimes the pieces of information workers listened into were quite sensitive and could, if one wanted to, be traced back to a specific person in a specific location. What was more, the contract work reportedly had a high turnover rate and workers were untrained in, or not told to "even consider," consumers' privacy.[19]

Information Fiduciaries

Inevitably, if we have no oversight of data usage, there will be cases of mishandling or misuse. In countries where privacy is considered a right that constituents can fight for at the polls and in courtrooms, companies may actually end up paying the price of mishandling data in legal fees.[20] The most prolific example of this kind is of course the Cambridge Analytica-Facebook scandal. This case has thrown into question the results of the 2016 U.S. Presidential election and has done significant damage to Facebook's reputation, as well as that of its CEO Mark Zuckerberg.[21] Legal scholar Lindsey Barrett expands on the vulnerable position of consumers in this system stating, "Like traditional fiduciaries, companies that collect enormous amounts of data on individuals have a strategic advantage over their clients due to the fact that they are trusted with the user's sensitive information, in addition to superior and specialized knowledge, lack of transparency, and the reliance of their users on the specialized services provided."[22] Barrett's succinct analysis includes one incredibly important word, "fiduciary."

Fiduciary duties hold businesses to the charges of care, confidentiality, and loyalty, preventing them from compromising the end-user in exchange for some kind of corporate gain.[23;24] Several professional industries owe clients fiduciary duties, including the doctors, lawyers, and accountants singled out by Google's Chief Economist Hal Varian in an attempt to abate the fears of consumers worried about sharing their data with tech companies.[25;26;27] "Because of the economic logic that underpins the digital public sphere,

capitalism has created a new system of relationships between us and digital media companies," Balkin writes, "These relationships have created new forms of digital vulnerability, and therefore these relationships should be fiduciary relationships, relationships of trust."[28] In other words, imposing fiduciary duties on technology companies would provide both them and the public a level of economic security. Lindsey Barrett's analysis reminds us that the concept was borne of balancing commercial and individual interests. Per Barrett, an information fiduciary framework would likewise not go as far in locking up data as the newly imposed EU General Data Protection Regulation.[29] This solution may work best for the American system and could also set an important precedent around the world. However, the asymmetry of information in the digital age goes beyond the relationships between corporations and individuals, seeping into democracy in unexpected ways via the targeted "surveillance capitalism" that seems to run the entire system.[30]

Data Privacy, Democracy, & Diplomacy

That concept also extends beyond sovereignty. Julie Cohen highlights the effects targeted information streams are likely having on citizenry, who are now receiving information in homogenous bubbles that not only support the biases of the companies who direct that information to them, but also fail to expose those same individuals to uncomfortable ideas and therefore new ways of thinking. Per Cohen, the effects are logically corrosive. She writes, "Ideological and cultural homogeneity produces complacency, reinforces existing biases, and inculcates resistance to contradictory facts, leading to polarization of wider debates on issues of public importance."[31] People may not always do what they are told, but if the same messaging is directed at them over and over again, soon enough they will begin to do so. Inequality is also cultivated from this system, where homogenous thinking lends itself to biases against minority populations, ones that are also largely not represented in the tech world. These biases are especially persistent online.[32] Privacy, she argues, is an important facet of democracy.

Ultimately, these problems are global ones that need to be taken head on in order to protect our political systems and, if Cohen's somewhat apocalyptic narrative is correct, also our free will. Information fiduciaries are a solid first step in the U.S.; the GDPR is as well for the EU. Elsewhere, like India, the data fiduciary framework is also being considered as a possible solution to a growing problem. There, a federal bill entitled the Personal Data Protection Bill using said language was drafted in 2018, and Parliament is set to discuss the bill in the upcoming 2019 winter session.[33;34]

Diplomats, especially of countries where wealth has accumulated at the expense of citizens around the world, should consider including data privacy in their campaigns. This could include a 'Best Practices' campaign that explains how to adjust the privacy settings on different social media platforms, for example. These sorts of initiatives could get the ball rolling on a global conversation about data privacy, as well as improve the soft power of countries willing to admit they have been affected by tech greed. However, these should only be the first steps in comprehensive cyberspace regulation. The companies will adjust, the wealth will continue to grow. As a citizenry we cannot continue to put our heads down while oligopolies lobby their way out of important protections for our privacy. The Internet gave us a space in which to connect globally, and as such we need to come together globally to make the appropriate changes for our future.

Devin Villacis

Devin Villacis is a Master of Public Diplomacy candidate at the University of Southern California expected to graduate in 2020. In 2014 she received her Bachelor's Degree in History with a minor in Photography from Duke University. There she was also inducted into Phi Alpha Theta, the History Honor Society. She spent the four years after her graduation at the ABC National News headquarters in New York, before moving to Los Angeles where she continues to freelance for the west coast bureau. Her interests in Public Diplomacy range from program evaluation to the effects of cyber power in the international space. Devin hopes to be able to continue learning after USC while working in the corporate social responsibility sector.

Replacement or Displacement: Preparing for the Fourth Industrial Revolution

Jessica Chan-Ugalde

Steam engineering. Mass production. Digital technology. These three advents mark radical points in history that irrevocably changed how humans interact and organize — the First, Second, and Third Industrial Revolution. In less than three centuries, the potential of individual and corporate output skyrocketed. However, not all countries (or even parts of countries) industrialized at the same rate. Often, government-enforced policies and regulations trailed far behind.

We are arguably in the midst of the beginning of the Fourth Industrial Revolution with defining technologies like the Internet of Things (IoT), artificial intelligence (AI), and machine learning (ML) leading us into a new age of automation.[1] You might wonder how automation brought on by AI or ML is any different than automation resulting from previous revolutions. After all, Eli Whitney introduced parts standardization, marking a shift toward replacing craftsmen with factory workers. Social networks like Facebook virtually eliminated the need to manually search for contacts in phone books or through personal contacts. Why can the Fourth Industrial Revolution lay special claim to being an age of automation? I argue that while previous revolutions did advance automated practices, their advents generally *extended* human thought and action; however, the Fourth Industrial Revolution is *replacing* human input altogether. To understand how labor may be affected, I will analyze the dichotomy between *extension* and *replacement*, the potential repercussions of replacement, and discuss whether replacement is a benign euphemism for something much more insidious — displacement.

Tools that Extend vs. Tools that Replace

With extension, tools and technologies supplement human thought and action, augmenting the amount of work humans are able to do i.e. instead of pulling horse-drawn carriages, we conducted steam-powered vehicles; instead of lighting a room with oil-lamps, we lit a room with a flip of a switch; instead of looking through an encyclopedia for a specific entry, we query search engines for the answers.

Meanwhile, the Fourth Industrial Revolution's advances in AI and robotics may entirely replace (and possibly, *displace*) human labor. Earlier I noted that parts-standardization replaced craftsmen with factory workers. Although factory workers were often subject to harsh conditions, they were still receiving extrinsic and arguably intrinsic rewards for their work. In contrast, the replacement of human workers with AI-augmented robots means that in certain instances, human labor is removed almost entirely. For example, in China, there has been a rise in "dark warehouses'' since October 2017 when JD.com, an e-commerce company and top competitor of Alibaba, announced the opening of a new factory in Shanghai which required no light. All work is done autonomously by robots.[2]

But maybe this distinction between extension and replacement is arbitrary: a matter of socio-economic intuition, influenced by whether a country is experiencing labor shortages or unemployment. In China, we are

beginning to see the ramifications of the one-child policy take form as labor shortages. At the same time, manufacturers in China are finding it increasingly difficult to maintain margins relative to competitors in Southeast Asia because of the increase in labor costs, prompting some executives to turn to robotics as the solution.[3] In response, the Chinese government is institutionalizing support for automation efforts (often AI-augmented) with their "Made in China 2025" policy, a 10-year plan leveraging government subsidies and bureaucratic support to rapidly develop high-tech sectors and decrease dependency on foreign technology.[4]

This isn't the first time China has experienced a labor shortage; their rocketing rise to becoming an industrial power is astounding in speed and effectiveness. While industrialization unfolded over centuries in the United States and Europe, China went from an agrarian society to a manufacturing superpower in under four decades — in fewer years than the age of the United State's youngest sitting president, J.F.K.[5] Mobilizing China's labor force to transition into a technical or service role might just be a natural next step.[6]

In countries whose economies are spotted with high unemployment rates in the past decades, however, support for automation is not as enthusiastic. To understand this, let's narrow our scope to a single, major player in the United States economy — Amazon. Amazon's acquisition of Kiva Systems, a robotics company, in 2014 underscored the company's keen interest in automation.[7] However, Amazon's position on could not be more different from China's. While China publicly welcomes and lauds a "dark age" of manufacturing, Amazon insists that human-free warehouses are decades down the line (which is becoming increasingly difficult to believe given China's progress). Martin Ford, who authored *Rise of the Robots*, contends that we may see only a gradual slowdown of job creation from companies investing heavily in automation.[8] Yet Amazon still emphasizes that their robot workforce isn't resulting in any lay-offs and Dave Clark, a top operations executive at Amazon, says that the idea that automation destroys net job growth is a myth.[9] The picture they paint is clear — people aren't going anywhere.

Unemployment rates and labor shortages can influence how governments and corporations approach, execute, and publicize advances in automation and their effect on labor. Where does this leave us? Is China right in assuming that we can efficiently retrain a workforce while simultaneously implementing automation? Are Amazon's assurances that joblessness isn't on the horizon for its workers persuasive? Is it possible to preserve job security and continue to advance automation technologies that enhance the work humans do?

I argue that perception of technological advances as either an extension or replacement of human action is a matter of scale. The advents of the Fourth Industrial Revolution simply encompass an unprecedented proportion of labor functions, replacing some job roles all together, but not precluding *other* job roles from being extended. However, replacement does not entail displacement. I believe the fear of replacement is a misguided and thinly veiled fear of displacement, fueled by a hesitation to believe that there will be sufficient recourse for retraining. The Fourth Industrial Revolution is different because it is replacing human input altogether *in some roles* — but elimination does not have to mean displacement if we invest in stimulating emerging markets so that the demand for non-automated jobs increases. Then, we will find ourselves in a position where we *need* and *welcome* automation.

AI and International Trade

As increasingly sophisticated AI penetrates a wider breadth of industries, the impact of the predicted shift toward service economies will extend past domestic labor policy and influence international trade. While increased production and excess supply may encourage foreign trade, a streamlined supply chain may involve decreased dependency on tools and technology acquired through the foreign market. For example, one of the specific goals outlined in China 2025 is to achieve 70% self-sufficiency in high-tech industries, a goal they plan on achieving through direct government subsidies, foreign investment and acquisitions, and stringent joint venture rules.

While AI-powered applications in fields like data analytics or recommendation engines may lower barriers to entry for small companies seeking to participate in a foreign market, AI itself is still considered an emerging market. Emerging markets are disruptive and AI is uniquely poised to penetrate a wide breadth of markets. China has invested heavily in foreign technology companies the past decade in an effort to acquire a larger market share of high-technology markets (e.g., CPUs) and advanced technological intellectual property (e.g., source code). This may be an indicator that industrialized countries seeking to capitalize on AI technology will be initially participating heavily in foreign markets. Sophisticated trade regulations developed in conjunction with AI experts and applied ethicists should be implemented to stimulate the AI market without compromising end-user privacy or protection for proprietary AI source code.

Jessica Chan-Ugalde

Jessica Chan-Ugalde is a graduate from the University of Puget Sound having studied Computer Science and Philosophy. She currently resides in Seattle, WA and is working as a technical consultant in the cloud-computing industry.

America Unplugged? The Effects of Net Neutrality on Cyber-diplomacy

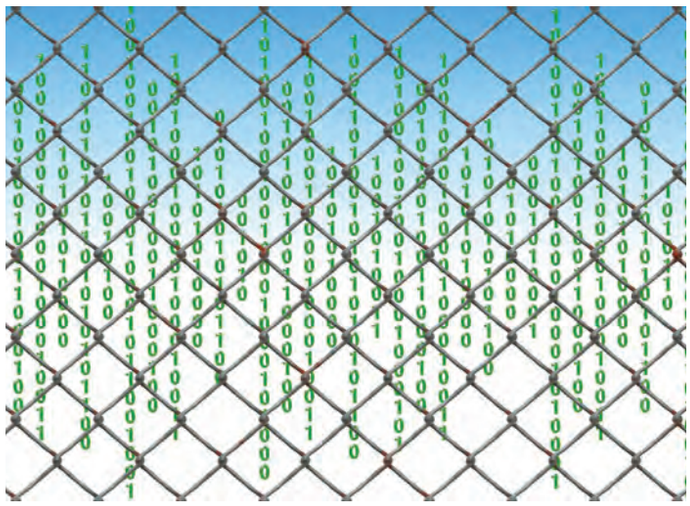
Joshua Morris

Twenty-nine years after the invention of the World Wide Web, the technology, infrastructure, policies, and dynamics that define the internet are still rapidly emerging, changing the landscape in which cyber diplomacy is performed.[1] The culture, the access, and the players are constantly shifting, and right now something seismic is underway in the U.S. For those of you who missed it, behind the scandals and intrigue that dominates today's headlines, a battle has been raging for the very soul of the internet in the U.S - net neutrality. So what exactly is net neutrality, how does it affect cyber diplomacy, why is there a fight in the U.S over it now, and what has happened thus far?

The seemingly innocuous phrase "net neutrality" refers to the principle that internet service providers cannot discriminate against websites or users by slowing down or blocking their connections.[2] Net neutrality has historically been protected in the U.S., but since 2017, the Federal Communication Commission (FCC) has been slowly unraveling these protections;[3] should net neutrality protections be completely compromised, an internet service provider like Spectrum would have the power to charge a company like Netflix a premium so that its customers receive a faster and more reliable connection, a premium that a competitor or startup might not afford.[4] Without net neutrality, private companies, NGOs, non-profits, and the government itself could all be competing for the supply of bandwidth that internet service providers control. In addition to forcing organizations to compete, the eradication of net neutrality could also force its customers to compete amongst one another.[5] People who pay more will have their service speed accelerated while those who cannot afford premium prices will have their speeds cut. Some will have their connections enhanced while others might barely be able to connect at all.

For cyber diplomacy, this means that digital communication to and from the U.S. becomes a lot more complicated. The first change to be considered is the strength of the audience's service plans. Does the audience pay for enough bandwidth to stream high-data-services like 3D videos or live events? 2D videos? Images? Do they even have enough bandwidth to regularly use the internet? With net neutrality, all customers are guaranteed an equitable distribution of bandwidth. Without it, we may need to reconsider how, when, and if to use the internet as a public diplomacy medium.

Cyber diplomats will also need to begin thinking about the internet service providers' relationships with the platforms they rely on. Perhaps in the future, internet service provider Xfinity will partner with Twitter to give their customers faster connections to the site. In turn, they may slow down connection speeds to Twitter's competitor, Facebook. In this case, cyber diplomats should start investing more time and resources into



Twitter (assuming the audience is primarily Xfinity customers). That scenario is simple enough, however, the deals between the internet service providers and media platforms may not be as straightforward. Internet companies might provide varying access to platforms for their customers based on which subscription the customer pays for. They may also create different subscriptions for different regions. For example, Xfinity might provide a fast connection to Twitter in California, but not to Facebook in Alabama. Right now, websites are guaranteed equal connectivity from service providers, but with the dismantling of net neutrality it will become important to track how internet service providers distribute connectivity across the map, in much the same way they create different cable packages across the U.S.

The erosion of net neutrality also has political ramifications. Without net neutrality, internet service providers will likely start taking a more active position in global affairs. These are some of the largest and wealthiest companies in the world and their interests are highly diverse. If they can protect these interests, their fiduciary responsibilities require them to do so. AT&T, for example, has holdings in health, manufacturing, retail, finance, and construction. If AT&T feels that any of these interests are threatened by a cyber diplomacy campaign, there may be little to keep them from slowing down or cutting off public access to campaign materials.

Those who oppose net neutrality argue that rolling back protections will allow internet providers to put in a "fast lane" for customers willing to pay for it and provide greater incentive to invest in infrastructure.[6] However, detractors point to the slower internet speeds that have already been experienced since 2017. Comcast placed "service speed limits" for customers that do not pay a premium in some areas.[7] Furthermore, AT&T and Verizon have both slowed down customers' service speeds to video services in order to allow others to access new unlimited data plans.[8]

So why is net neutrality being rolled back now? Internet service providers have been fighting to roll back non-discrimination policies since the dial-up era, with little success. That is until now. Internet service providers have found an ally in this administration's commissioner of the FCC, Ajit Pai. In 2017, Pai changed commission policy and overturned net neutrality protections.[9] This decision was promptly challenged in court. In October 2019, a federal judge ruled that the FCC does have the authority to take such action; however, the states are free to implement their own net neutrality protections if they so choose. Now, the states are rushing to implement their own policies. Another flurry of court cases to determine their constitutionality will inevitably ensue.[10]

Depending on who you ask, a U.S. without net neutrality will either open the doors for a dystopian age of internet access or one in which it is relegated to the wealthiest among us. Either way, as cyber diplomats, it is important to follow this story and pay attention to how it is shifting the digital landscape beneath our feet.

Joshua Morris

Joshua Morris is a master's student in USC's Master of Public Diplomacy program, Class of '21. He earned his BA from the University of Kentucky in Communication and International Studies, with a focus on comparative politics and societies of the Middle East and North Africa. He is currently a staff writer for the Public Diplomacy Magazine and is an assistant researcher in the USC Marshall Behavioral Research Lab. He has worked as a storyteller at Lexington Brewing and Distilling Co., doing public relations and marketing work at this charter member of the famed Kentucky Bourbon Trail. He has also worked as an Audience Research Intern at the Smithsonian Institution.

Decentralizing Diplomacy: Convening in the Digital Age

Brett Solomon and Nikki Gladstone

In 2011, social media platforms were being leveraged[1] in the Arab Spring, a series of protests against authoritarian governments in Bahrain, Egypt, Libya, Tunisia, and Yemen; WikiLeaks released the Spy Files, thousands of pages exposing the global mass surveillance industry[2]; IBM's Watson computer had defeated reigning champions of the television game show, Jeopardy![3]; and Apple had just launched Siri, it's brand new, virtual digital assistant.[4]

It was two years before leaked NSA documents by Edward Snowden would catapult issues of privacy and surveillance into public consciousness and seven years before the Cambridge Analytica scandal would threaten the integrity of democratic systems, but the world was already grappling with the impact of technology – both negative and positive – on our lives and our rights.

In the same year, Access Now hosted its first ever RightsCon (then the Silicon Valley Human Rights Conference), with the recognition that protecting and extending the digital rights of users at risk would require bringing all stakeholders – from tech companies to government representatives to human rights defenders – to the table. The outcome was a tangible set of rights-based standards for a rapidly expanding technology sector and the start of a summit series that has now taken place on five continents and attracts more than 2,500 participants annually.

The conversations we hosted in 2011 with a few hundred participants across a handful of workshops have expanded and shifted into the ones we have today. The last decade has seen near ubiquitous integration of technology into our everyday lives. Governments are rapidly responding to protests online and off by increasingly shutting down access to the internet;[5] the exporting of surveillance technology[6] and advances in facial recognition software are facilitating targeted and mass surveillance at an intractable scale; artificial Intelligence underpins many industrial and human processes;[7] and our homes and devices play host to increasingly sophisticated virtual assistants.[8]

Following the RightsCon program over time aptly illustrates the growing complexity of building a rights-respecting future, as well as the convergence of issues once classified as outside the digital rights or "cyber" domain.[9] Yet even as the program and participation expands, the core idea of our summit remains: in-person, multi-stakeholder convening is a powerful tool for change.

Getting the Right People in the Room

"Multi-stakeholderism" can feel like a tired and outdated term, but so many challenges stem from a disconnect between different perspectives. Getting the right people in the room can be difficult – it requires trust and at times is uncomfortable – but the challenges ahead are complex and interconnected. This means that multi-stakeholder approaches to convening aren't a buzzword or a nice-to-have; they're a necessity to move from problem identification to problem solving.

We also see this approach as a necessary step to redistribute power. Current challenges can't be solved by traditional tools of diplomacy alone. Too often, the communities that are most affected by rapid changes in technology aren't represented in the rooms where decisions are made. For this reason, we prefer intimate strategic roundtables over highly-produced keynotes. When done wrong, events can perpetuate existing power asymmetries by elevating certain voices over others. When done right, they can bring decision-makers in policy and industry face-to-face with those affected, and strengthen accountability mechanisms.

Building an Adaptive Program

Being responsive to change requires agility. Our program remains relevant because we don't do it alone. Every year, in our Call for Proposals, we turn to a global community of experts and ask: what are you working on now and what is needed to move it forward? Once we close our Call, building the program can't be formulaic. We work alongside session organizers to curate a program and create an environment that facilitates impact, even when it can be difficult to identify what that looks like ahead of time.

Over the last nine years, that network has expanded, highlighting an important shift in focus from digital rights to human rights in the digital age. This flexibility in the agenda has meant our program hosts the enduring themes present at our very first convening – business and human rights, freedom of expression, and privacy – while expanding to include unforeseen emerging concepts and trends. In Brussels,[10] it was artificial intelligence, in Toronto,[11] humanitarian response, in

Tunis,[12] election integrity, and in Costa Rica,[13] it will likely be the climate crisis.

Including new transformative collisions across the human rights sector is not an attempt to duplicate hard work already being done in those spaces. Rather, it's an opportunity to dismantle traditional silos for a "merging of rivers" that can result in shared learnings and unexpected collaborations.

Creating a Movement

Movements that drive transformational change "respond holistically and flexibly to seize strategic opportunities to act."[14] Our collaborative, community-driven model is what makes RightsCon effective and unique as a convening space, especially when what qualifies a community "member" is fluid and individually-defined by each participant.

Since 2011, RightsCon has cultivated a "core community" of activists, technologists, public servants, researchers, and issue area experts who return to our summit year after year, and meaningfully contribute to its structure and content. The key to these long-standing relationships is trust. As conveners, we are accountable to our community, and our community, in turn, invests energy, time, and resources into designing a space that drives human connections and furthers social change.

We think of RightsCon as a movement because of the cyclical, nonhierarchical nature of our work. Change is incremental, and our program is a living record of our community's growth and transformation over time. Every convening adds another layer of complexity and ushers in a fresh cohort of innovators and thought leaders. At this year's summit, we published the Tunis Learnings, a statement considering each major track and outlining a starting point for centering human rights in each industry and body of work.[15]

Focusing on Impact

Informal conversations and planned discussions are important tactics for building networks, but alone they're not enough to drive action. Since the beginning, we've emphasized the importance of sessions that translate into concrete outcomes and strategies that carry momentum forward and often build the foundation for the next cycle of our program.

Convening is important because we've seen what happens when it works. Coordination between civil society organizations to protect the rights to equality and non-discrimination in machine learning led to a first of its kind declaration.[16] A meeting between Global South advocates and Facebook representatives launched a coalition to uphold platform accountability for traditionally underserved users.[17] An official statement from UN Special Rapporteurs calling for the protection of human rights defenders in digital spaces set a standard for other multilateral bodies.[18] In the midst of the 2019 summit, as the Sudan uprising unfolded, the #KeepItOn coalition – itself an outcome of the summit – mobilized the RightsCon community to demand an end to internet shutdowns in the country.[19]

At our next summit, we'll explore how we can build on what has been done to shape what's to come.

In 2020, RightsCon will take place in San Jose, Costa Rica from June 9-12. RightsCon Call for Proposals closes on January 14, 2020.

Brett Solomon

Brett Solomon is the Executive Director of Access Now, an international NGO which combines direct technical support, comprehensive policy engagement, global advocacy, grassroots grant-making, and convenings to fight for human rights in the digital age.

Nikki Gladstone

Nikki Gladstone directs RightsCon, Access Now's annual, globally-rotating convening. She is excited about creating inclusive and accessible spaces for the digital rights community to drive change.

The Old Fundamentals Will Not Change in This New Digital Age

Interview by Jasmine Kolano

Nicholas J. Cull, a pioneer of public diplomacy studies and a leading expert in the field, shares about his new book, *Public Diplomacy: Foundations for Global Engagement in the Digital Age* (Polity 2019). Recommended by Joseph Nye, author of *The Future of Power*, Cull captures the timeless wisdom of succeeding as a diplomat in the digital age and in the ages to come.

His book will be translated into Italian December 2019.

Jasmine Kolano (JK): Your book is rich with so many public diplomacy case studies. How many years was it in the making?

Nicholas Cull (NC): The book began as a series of lectures, each of which has been evolved over a long time. The first chapter of the book is actually based on one of the first public diplomacy talks that I gave just before 9/11. These lectures have changed and developed thanks to audiences I've worked with around the world these past twenty years. I wanted to push these lectures into a final form and this book is the result.

JK: It sounds like it was a collaborative process from the beginning! Why else did you write *Public Diplomacy: Foundations for Global Engagement in the Digital Age*?

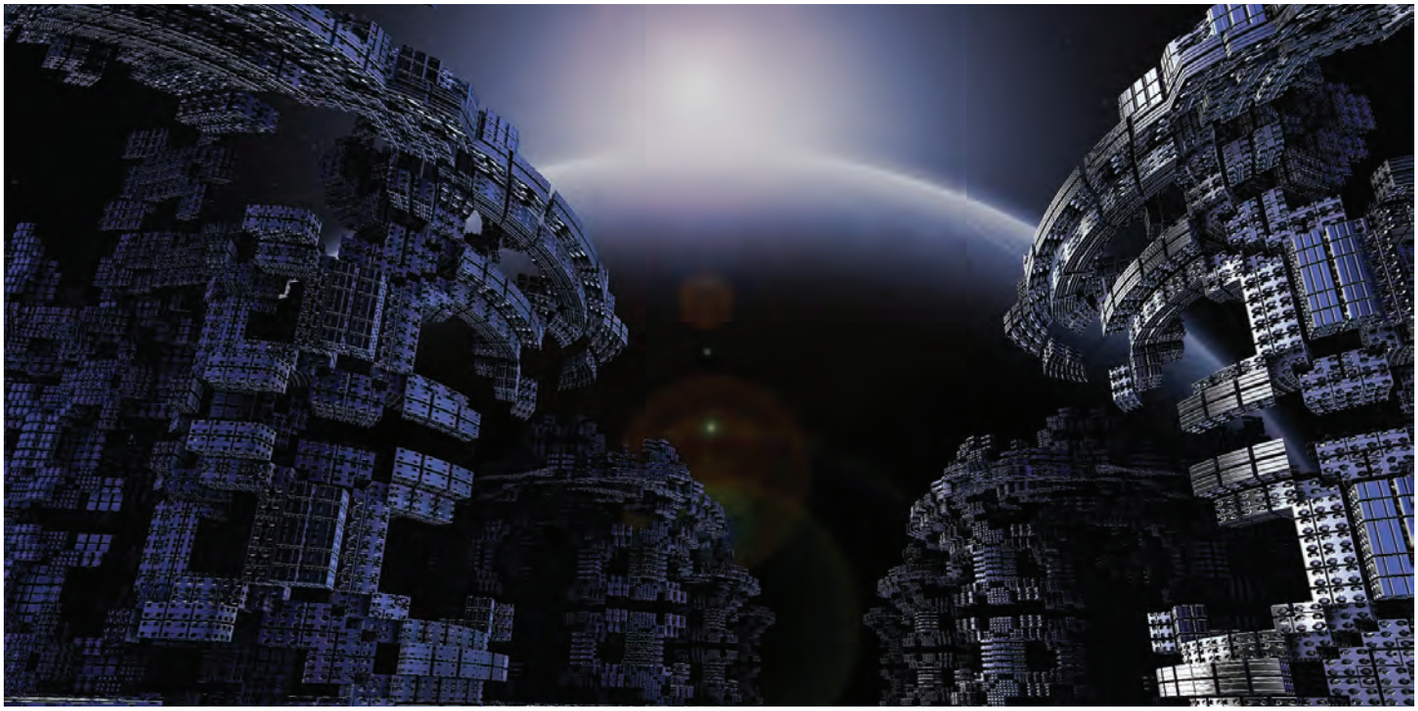
NC: I believe that in this generation, everyone is going to be judged on how good of a team player they are. One point of this book is that sometimes, nation-branding gets in the way of international collaboration. For a nation to be truly useful, it needs to be truly collaborative. When problems are big, solutions have to be big too, and in order to provide them nations need to be collaborative.

JK: What do you think happens to public diplomacy in a world of "cyber terror" where individuals can hack others and remain faceless?

NC: The danger is that it the threat becomes personified and we start cyber-place branding. This could be a real danger for Russia. People already identify Russia with hacking, the same way Nigeria became associated with phishing emails. When Nigeria realized it did not want to be called the "phishing letter country," the government of Nigeria started to crack down on those letters because it was a form of negative place branding.

JK: Instead of "branding" other nations, how can a country be successful in its collaborations in the current cyber age?

NC: The best public diplomacy in the world can never compensate for a bad policy, and the best thing you can do to get good policy is to listen. I was struck that in my book, I spent a lot more time writing about peoples'



biases when it comes to listening than I did about the superficial big stories of the digital age like Mark Zuckerberg!

JK: How can the U.S. overcome these "biases" in listening, especially amidst ongoing cyber conflicts with other state actors?

NC: The U.S. government should be trying to listen to everybody and asking other international actors who they're listening to and what they hear when they do so. Great listeners are eclectic in their listening. The best listening is both collaborative and active; it doesn't mean listening and just assuming you understand. The skilled listener repeats back what they've heard to clarify: What I think you're saying is X, is that the case? In the process the listener and the subject create shared meaning. It's hard work.

JK: You write that "right-sizing" a problem is important so that public diplomats do not overextend themselves. The cyberworld is a growing universe and zero-ing in on a problem can be incredibly daunting. How do you suggest nations begin to identify smaller-sized problems that are easier to address?

NC: The first thing to do is to talk about it because these problems are shared. A lot of places are experiencing the same problems simultaneously. One of the things I say when talking to governments and officials is that we live in an age where information is an armament, but we haven't begun a process of information disarmament. Of course there are great examples of countries working together, and good models for collaboration too.

JK: Are initiatives like Denmark's Tech Ambassador effective in helping nations negotiate with big tech and producing good outcomes for its citizens back home?

NC: There have always been consuls in the West Coast that have been keeping in tight with high tech as a big part of their role, so in a way, I see it as an example of branding as opposed to a completely innovative approach. I see the Tech Ambassador as a public relations initiative for Denmark and its achievement has been to advance the idea that Denmark is a tech savvy country. It's also been significant for Silicon Valley as now it gets to say, "We're so significant that people are now sending ambassadors to us." But it shows how central that is now to the way people understand the West Coast.

JK: How can the U.S. take advantage of cyber crises in order to gain back lost territory in terms of soft and sharp power?

NC: A weakness of American public diplomacy is the assumption: "The answer is 'America,' now what is the question?" The U.S. should not present itself as the "answer country" but be honest about the problems it faces. There are some American problems that it should ask the rest of the world about. People like people who are honest about their flaws. It should be a strength to talk about your weakness, and to be honest about the problems you face. Remember, Superman would be unbearable without Kryptonite.

JK: Are foundations still important in the current

digital age?

NC: You're not going to get very far with the digital technology if you don't remember the basics. Foundations put a "brake" on the enthusiasm for the digital: Sure, we live in a digital age, but what's really fundamental doesn't change from year to year. Sometimes, in the digital world, people feel "un-empowered" because they do not understand newer technologies. They need to be affirmed in the fundamentals they already know.

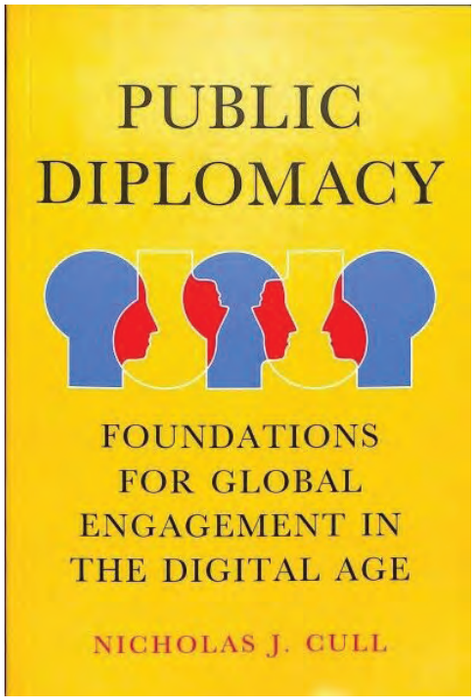
JK: At the end of your book, you speak about hope. Do you think there is hope for superpowers like China and the U.S. - countries with vastly different values when it comes to how the cyberworld should be managed - to ever engage in effective cyber-diplomacy?

NC: If you look at the history of international relations it goes in cycles. You see cycles where people look inwards and backwards. You see moments where people look forward and pull together. The problem is that what usually prompts people to move forward together is something cataclysmic.

With my book, I'd like for countries to work together and think together without suffering the cataclysmic part. I see the thinking of 1910 and 1938 and I want to get to 1919 and 1947 without going through the processes that produced the kind of insight that we saw at the end of the World Wars and in the 1980s, when people realized they are going to have to work together.

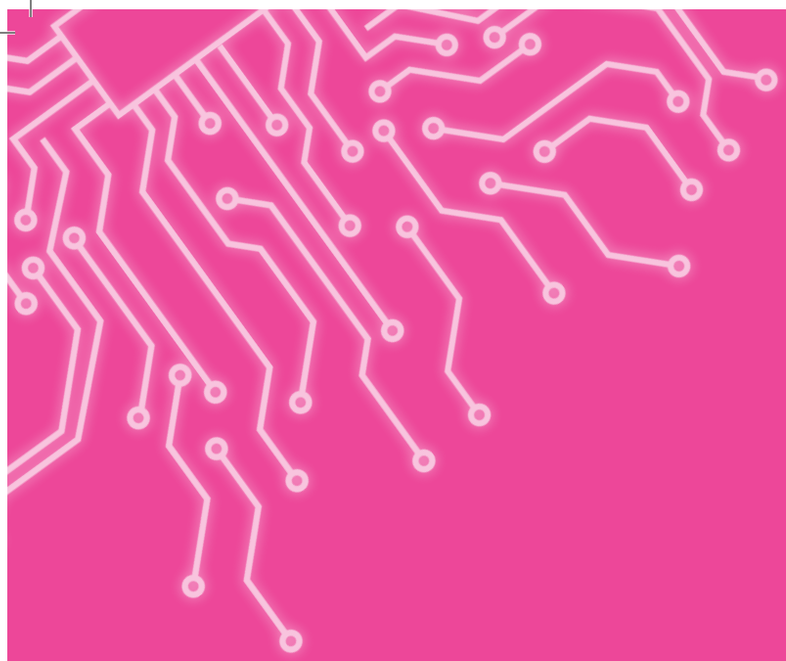
Maybe some governments are so stubborn that they can't learn other than the hard way. But, I believe in these cycles. I believe that at some point the ideas of the collective and working together and a vision of the future will be sought, and people will ask, "Who was thinking about this stuff?" and when they do, I want them to have something to read, so they won't have to reinvent the wheel.

Public Diplomacy: Foundations for Global Engagement in the Digital Age is available online and can be found at: bit.ly/pdfoundations



Nicholas J. Cull

Nicholas J. Cull is a Professor of Public Diplomacy and is the founding director of the Master of Public Diplomacy program at USC. His research and teaching interests are inter-disciplinary, and focus on public diplomacy and – more broadly – the role of media, culture and propaganda in international history. He is the author of two volumes on the history of US public diplomacy: *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989* (Cambridge 2008), named by Choice Magazine as one of the Outstanding Academic Texts of 2009 and *The Decline and Fall of the United States Information Agency: American Public Diplomacy, 1989-2001* (Palgrave, New York, 2012). His first book, *Selling War*, published by OUP New York in 1995, was a study of British information work in the United States before Pearl Harbor.



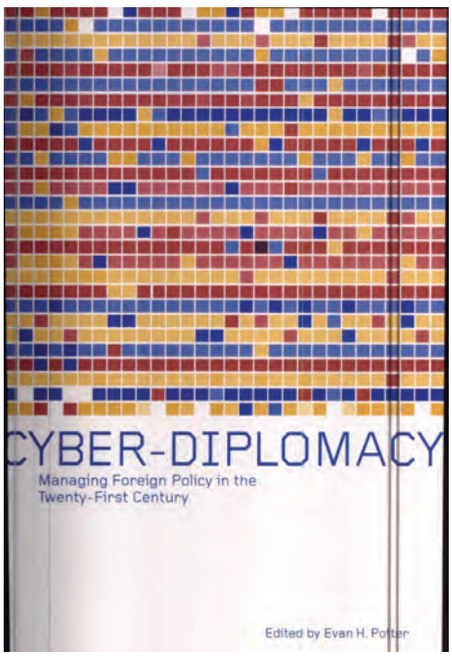
“CYBER HACKS:” GETTING AHEAD

Special Features

Fatime Uruci

Recommended Readings, From Past to Present

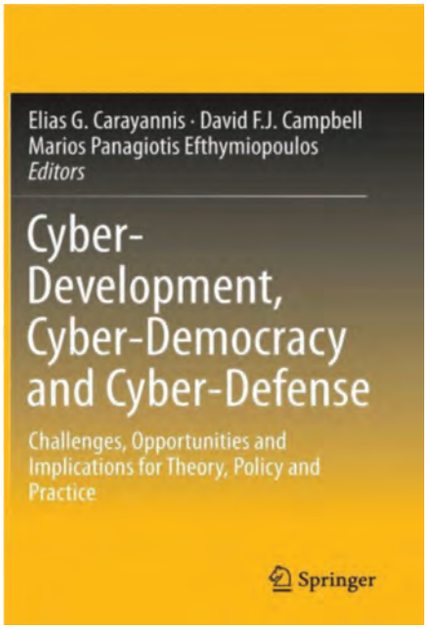
These three readings showcase the growth of the field of cyber diplomacy between 2002 and 2019 across multiple perspectives and in interdisciplinary ways.



Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century

By Evan H. Potter

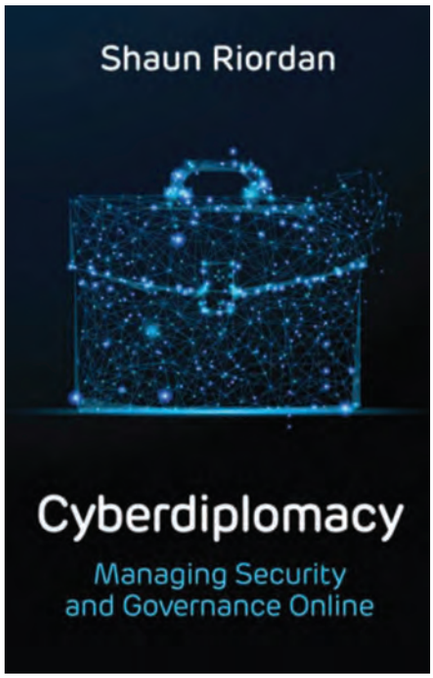
Published September 12, 2002



Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice

By Elias G. Carayannis, David F. J. Campbell (Editor), Marios Panagiotis Efthymiopoulos (Editor)

Published August 15, 2014



Cyberdiplomacy: Managing Security and Governance Online

By Shaun Riordan

Published April 22, 2019

Resources for Research on Cyber Diplomacy & Possible Career Pathways

The following list details resources for research and careers in cyber diplomacy across traditional government agencies and NGOs active in the field.

CyberPeace Foundation

https://www.cyberpeace.org/career/

UNIDIR's Cyber Policy Portal

https://cyberpolicyportal.org/en/

Digital & Cyber-diplomacy Courses, Web Discussions, Seminars, & Conferences

A number of institutions have begun to create courses, web discussions, seminars, and conferences around cyber-diplomacy and related themes.

The DiploFoundation is in the midst of hosting a cyber-diplomacy web series in partnership with Microsoft. Summaries of the different web series are available on their website. The date for the final talk in the series has yet to be announced, but past series have focused on cyber-armament, international law, and cyber-attacks.

https://www.diplomacy.edu/calendar/cyber-diplomacy-web-discussion%C2%A0applicability-international-law-cyberspace

The ICT4Peace Foundation has hosted a number of workshops around international law, norms and CBMs, CERT-Building, strategy building and legislation around promoting openness, prosperity, trust and security in cyberspace. Links to their workshops and publications can be found online.

https://ict4peace.org/wp-content/uploads/2019/09/Cybersecurity-Policy-and-Diplomacy-Capacity-Building-15-August-2019-1-1.pdf

The UNIDIR Annual Cyber Stability Conference last took place on Thursday, June 6, 2019, in CR-4, United Nations HQ, New York. Key issues addressed by the speakers included the impact of the global digital technology development on States, economies, industries and security ecosystems, the risks of mounting cyber threats and the potential costs of failure to agree on effective international cybersecurity cooperation mechanisms – and the incentives for States to engage with the multilateral processes on cybersecurity policy norms, including UN GGE and OEWG on cybersecurity. All conference sessions are viewable online.

https://www.unidir.org/conferences/2019-cyber-stability-conference

UNODA Course on Cyber Diplomacy, supported by the Government of Singapore: Based on the assessments and recommendations of the GGE reports, the United Nations Office for Disarmament Affairs has developed, with the support of the Government of Singapore and in collaboration with other key partners, this online training course to encourage greater understanding of the use of ICTs and its implications for international security.

https://cyberdiplomacy.disarmamenteducation.org/home/

Popular Podcasts on CyberDiplomacy

The CyberWire Daily Podcast (979 episodes and counting)

https://thecyberwire.com/podcasts/daily-podcast.html

***Government Information Security Podcast*, The Rapid Evolution of Cyber Diplomacy**

https://podbay.fm/podcast/504642939/e/1430863560

Sound Discussion, Timo Koster: Cyber Diplomacy

https://podcasts.apple.com/us/podcast/timo-koster-cyber-diplomacy/id1324072644?i=1000451345537

Fatime Uruci

Fatime Uruci is from Queens, New York and is a first-year Master of Public Diplomacy student in the Annenberg School. She completed her B.A. English and Philosophy, with a concentration in Literature and Law in the former, at the City University of New York's John Jay College of Criminal Justice, where she also minored in Theatre Arts and Interdisciplinary Studies. Her past academic work has explored justice in its many dimensions, such as race, gender, the environment, technology and new media, and more, within both domestic and international contexts.

Footnotes

EQUIPPING DIPLOMATS FOR THE CYBER AGE

If You Can't Beat Them, Join Them: The Story of Hackers as Non-State Actors Affecting Geo-politics

By SANYA BUDHIRAJA

1. Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, [online] 4(1), pp.1-37. Available at: https://content.sciendo.com/view/journals/jms/4/1/article-p1.xml [Accessed 17 Apr. 2019].
2. Nye, J. (2010). CyberPower. [online] Belfercenter.org. Available at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [Accessed 29 Mar. 2019].
3. Tennat, D. (2009). The fog of (cyber) war. *Computerworld*. [online] Available at: https://www.computerworld.com/article/2523545/the-fog-of--cyber--war.html?page=3 [Accessed 19 Apr. 2019].
4. Barrett, B. (2018). DOJ CHARGES NORTH KOREAN HACKER FOR SONY, WANNACRY, AND MORE. *Wired*. [online] Available at: https://www.wired.com/story/doj-north-korea-hacker-sony-wannacry-complaint/ [Accessed 16 Apr. 2019].
5. Bergal, J. (2018). White-Hat Hackers to the Rescue. *PEW*. [online] Available at: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/05/14/white-hat-hackers-to-the-rescue [Accessed 21 Apr. 2019].
6. Whittaker, Z. (2019). Hackers publish personal data on thousands of US policy officers and federal agents. *Techcrunch*. [online] Available at: https://techcrunch.com/2019/04/12/police-data-hack/ [Accessed 18 Apr. 2019].
7. Awad, O. (2018). How Israel is becoming the world's top cyber superpower. *Vice News*. [online] Available at: https://news.vice.com/en_us/article/evmyda/how-israel-is-becoming-the-worlds-top-cyber-superpower [Accessed 20 Apr. 2019].
8. Vincent, A. (2017). State-sponsored hackers: the new normal for business. *Network Security*, [online] 2017(9), pp.10-12.
9. Sheldon, J. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, [online] 5(2), pp.95-112. Available at: https://www.jstor.org/stable/26270559?seq=1#metadata_info_tab_contents [Accessed 17 Apr. 2019].
10. Yang, Y. (2018). China discourages its hackers from foreign competitions so they don't help others. *South China Morning Post*. [online] Available at: https://www.scmp.com/tech/article/2138114/china-discourages-its-cybersecurity-experts-global-hacking-competitions [Accessed 30 Apr. 2019].

Training Diplomats For An AI-Driven Future

By NIKKI BURNETT

1. Dutton, Tim. "An Overview of National AI Strategies." Medium.com. Last modified July 25, 2018. https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd
2. Digital Diplomacy Camp - Brussels. DiploFoundation. Last modified March 8, 2019. https://www.diplomacycamp.org/
3. Hone, Katharina and Maciel, Marília. "Lessons learned: Offering our course on AI for the first time." DiploFoundation. Last modified September 5, 2019. https://www.diplomacy.edu/blog/lessons-learned-offering-our-course-ai-first-time
4. Ibid.
5. *Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy*. 2019. DiploFoundation. https://www.diplomacy.edu/sites/default/files/AI-diplo-report.pdf
6. Artificial Intelligence: Technology, Governance, and Policy Frameworks. DiploFoundation. Last modified September 20, 2019. https://www.diplomacy.edu/courses/AI
7. *Malta: The Ultimate AI Launchpad: A Strategy and Vision for Artificial Intelligence in Malta 2030*. 2019. Malta.AI. https://malta.ai/wp-content/uploads/2019/11/Malta_The_Ultimate_AI_Launchpad_vFinal.pdf

When High-Tech is Not Enough

By JASMINE KOLANO

1. Furedi, F. and Furedi, A. (2019). Fear Today | Frank Furedi. [magazine] First Things, p.11. Available at: https://www.firstthings.com/article/2019/01/fear-today [Accessed 20 Mar. 2019].
2. Ibid.
3. McClory, J. (2018). The Soft Power 30: A Global Ranking of Soft Power. [ebook] Portland, Facebook, and USC Center for Public Diplomacy, p.32. Available at: https://softpower30.com/wp-content/uploads/2018/07/The-Soft-Power-30-Report-2018.pdf [Accessed 10 Apr. 2019].
4. The Soft Power 30: A Global Ranking of Soft Power. [ebook] Portland, Facebook, and USC Center for Public Diplomacy, p.50.
5. Vargas, J. (2019). The Face of Facebook. [online] The New Yorker. Available at: https://www.newyorker.com/magazine/2010/09/20/the-face-of-facebook [Accessed 5 Mar. 2019].
6. Kang, C. (2019). Facebook Fine Could Total Billions if F.T.C. Talks Lead to a Deal. [online] NYTimes.com. Available at: https://www.nytimes.com/2019/02/14/technology/facebook-ftc-settlement.html?
7. Brant, R. (2019). Who will challenge China's 'open' internet?. [online] BBC News.
8. Fear Today | Frank Furedi. [magazine] First Things, p.10.
9. Hone, K. (2019). Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy. [ebook] diplomacy.edu, p.29. Available at: https://www.diplomacy.edu/sites/default/files/AI-diplo-report.pdf [Accessed 1 Apr. 2019].
10. Ibid.
11. Ibid., p.231.
12. Hickey, J. (2018). Advancement of artificial intelligence opens health data privacy to attack. [online] Berkeley News. Available at: https://news.berkeley.edu/2018/12/21/advancement-of-artificial-intelligence-opens-health-data-privacy-to-attack/ [Accessed 29 Apr. 2019].

13. Consumer.ftc.gov. (2019). About the FTC. [online] Available at: https:// www.consumer.ftc.gov/sites/default/files/games/off-site/youarehere/pages/about_the_ftc.html

14. WashingtonPost.com (2018). Transcript of Mark Zuckerberg's Senate Hearing. [online] Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.104b9c91e937 [Accessed 30 Apr. 2019].

15. ChooseToEncrypt.com. (2019). All US States Need Privacy Laws Like California Consumer Privacy Act. [online] Available at: https://choosetoencrypt.com/privacy/california-privacy-laws/ [Accessed 29 Apr. 2019].

16. Eugdpr.org. (2019). EUGDPR – Information Portal. [online] Available at: https://eugdpr.org [Accessed 29 Apr. 2019].

17. Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy. [ebook] diplomacy.edu, p.34.

18. Ibid.

19. Investopedia. (2019). De-Anonymization. [online] Available at: https://www.investopedia.com/terms/d/deanonymization.asp [Accessed 30 Apr. 2019].

20. Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy. [ebook] diplomacy.edu, p.34.

21. Pew Research Center. (2016). The state of privacy in America. [online] Available at: https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [Accessed 29 Apr. 2019].

22. Freedomhouse.org. (2018). China. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/china [Accessed 20 Apr. 2019].

23. Freedomhouse.org. (2018). China. [online] Available at: https://freedomhouse.org/report/freedom-net/2018/china [Accessed 20 Apr. 2019].

24. Ibid.

25. Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy. [ebook] diplomacy.edu, p.99

26. Ibid., p.30.

27. Brant, R. (2019). Who will challenge China's 'open' internet?. [online] BBC News.

28. Freedomhouse.org. (2018). Freedom on the Net 2018 Report. [online] Available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism [Accessed 20 Apr. 2019].

29. Javelinstrategy.com. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity | Javelin. [online] Available at: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity [Accessed 29 Apr. 2019].

30. Ibid.

31. ChooseToEncrypt.com. (2019). All US States Need Privacy Laws Like California Consumer Privacy Act. [online] Available at: https://choosetoencrypt.com/privacy/california-privacy-laws/ [Accessed 29 Apr. 2019].

32. Ibid.

33. Ibid.

34. Linder, E. (2018). The Soft Power 30: A Global Ranking of Soft Power. [ebook] Portland, Facebook, and USC Center for Public Diplomacy, p.108. Available at: https://softpower30.com/wp-content/uploads/2018/07/The-Soft-Power-30-Report-2018.pdf

35. Linder, E. (2018). The Soft Power 30: A Global Ranking of Soft Power. [ebook] Portland, Facebook, and USC Center for Public Diplomacy, p.110.

36. Ibid., p.111.

37. Ibid.

38. Ibid.

39. Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy. [ebook] diplomacy.edu, p.35.

CYBER-DIPLOMACY'S RISING STARS

Cyber-diplomacy in Qatar: A Virtue of Necessity?

By KRHISTO AYAD and ABED SHIRZAI

1. S. Riordan, "Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction" CPD Blog, USC Center on Public Diplomacy, 12 May 2016, www.uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction.

2. A. Krieg, "The Gulf Crisis and Qatari blockade – A Feud Maintained by an Information War. Interview with researcher Andreas Krieg", Opinion Internationale, 28 March 2018, https://www.opinion-internationale.com/2018/03/28/the-gulf-crisis-and-qatari-blockade-a-feud-maintained-by-an-information-war-interview-with-the-researcher-andreas-krieg_53442.html.

3. "About," Global Security Forum, October 2019, https://globalsecurityforum.com/about/.

4. "Qatar National Vision 2030," Planning and Statistics Authority, General Secretariat For Development Planning, July 2008, www.mdps.gov.qa/en/qnv1/Pages/default.aspx.

5. "Qatar National Cyber Security Strategy," Ministry of Transport and Telecommunications, Government of Qatar, May 2014, www.motc.gov.qa/en/cyber-security/national-cyber-security-strategy.

6. "Qatar International Cybersecurity Contest," Hamad Bin Khalifa University, October 2019, www.hbku.edu.qa/en/qicc.

7. "The New Battlefront: Cyber Security Across the GCC," Gulf International Forum, 28 Oct. 2018, https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/.

Estonian Leadership in the Cyber Realm

By DANIEL E. WHITE

1. Damien McGuinness, "How a cyber attack transformed Estonia," *BBC News*, 27 April 2017. https://www.bbc.com/news/39655415

Footnotes (cont.)

2. Aaron Metha, "Estonian Defense Minister Juri Luik on Russian threats and defending the Baltics," *Defense News*, 17 September 2018. https://www.defensenews.com/interviews/2018/09/17/estonias-defense-minister-on-russian-threats-and-defending-the-baltics/

3. E-Estonia, June 2017. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

4. Republic of Estonia, "Estonian E-Residency," *Ministry of Foreign Affairs*, 12 June 2019. https://vm.ee/en/estonian-e-residency-how-apply

5. Shannon Vavra, "Estonia debuts first-ever diplomacy training," *Cyber Scoop*, 29 July 2019. https://www.cyberscoop.com/cyber-diplomacy-estonia-summer-school/

6. Stephan Faris and Matthew Kaminski, "Politico 28–Who to Watch in 2019," *Politico*, 4 December 2018. https://www.politico.eu/list/politico-28-class-of-2019-the-ranking/heli-tiirmaa-klaar/

7. United Nations Security Council. "Countries Elected Members," *United Nations* https://www.un.org/securitycouncil/content/countries-elected-members

Georgia's Cybersecurity Stand and March Toward Progress

By MARIAMI KHATIASHVILI

1. Ministry of Defense of Georgia (2018). "2019 – Cyber Security Year in the Georgian Armed Forces." Retrieved from www.mod.gov.ge/en/news/read/6908/2019-%E2%80%93-cyber-security-year-in-the-georgian-armed-forces

2. Ministry of Defense of Georgia (2019). "Intermarium Cyber Security Forum 2019." Retrieved from www.mod.gov.ge/en/news/read/7555/intermarium-cyber-security-forum-2019

3. Ministry of Foreign Affairs of Georgia. "National Security Concept of Georgia" (2011). Retrieved from www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx

4. International Telecommunication Union (2019). "Global Cybersecurity Index 2018." Retrieved from www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

5. "National Security Concept of Georgia" (2005). Retrieved from www.parliament.ge/files/292_880_927746_concept_en.pdf

6. Ibid.

7. Ibid.

8. "Law of Georgia on Information Security" (2012). Retrieved from www.matsne.gov.ge/en/document/view/1679424?publication=3

9. Ibid.

10. Ministry of Defense of Georgia. "Cyber Security Bureau." Retrieved from https://mod.gov.ge/en/page/59/cyber-security-bureau

11. "Cyber Security Strategy of Georgia: 2013-2015." (In Georgian). Retrieved from www.matsne.gov.ge/ka/document/download/1923932/0/ge/pdf

12. Ibid.

13. North Atlantic Treaty Organization (2016). "Substantial NATO-Georgia Package (SNGP)." Retrieved from www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_02/160209-factsheet-sngp-en.pdf

14. Davis, Susan (2019). "NATO in the Cyber Age: Strengthening Security and Defense, Stabilising Deterrence." Draft General Report. Retrieved from www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf

15. North Atlantic Treaty Organization (2017). "NATO-Georgia Relations." Retrieved from www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/20171201_171201_Media_Backgrounder_Georgia_en.pdf

OVERCOMING DISINFORMATION

Are Digital Rights Human Rights?

By ILAN MANOR, Ph.D.

1. BBC News. (2016). LinkedIn blocked by Russian authorities. Available at https://www.bbc.com/news/technology-38014501

2. Bradshaw, S. & PHoward, P.N (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper 2019.3. Oxford, UK: Project on Computational Propaganda.

3. Cowhey, P. F., & Aronson, J. D. (2017). Digital DNA: disruption and the challenges for global governance. Oxford University Press. Ditchley Foundation (2016). Will we still have a single global internet in 2025? Available at https://www.ditchley.com/events/past-events/2010-2019/2016/will-we-still-have-single-globalinternet-2025

4. Manor, I. (2019). The Digitalization of Public Diplomacy. Springer International Publishing. NATO StratCom Centre of Excellence. (2015). Analysis of Russia's information campaign against Ukraine: Examining non-military aspects of the crisis in Ukraine from a strategic communications perspectives. Riga: NATO StratCom Centre of Excellence. Available at https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine-1.

5. Teracin. (2019). Facebook removes dozens of anti-Israel fake accounts from Iran. The Jerusalem Post. Available at https://www.jpost.com/International/Facebook-suspends-Russian-Instagramaccounts-targeting-US-voters-605332

6. United Nations .(2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

You Can't Solve Lying: Adapting to the Disinformation Age

By DEAN JACKSON

1. "Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,'" Dean Jackson, International Forum for Democratic Studies, October 17, 2017. https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

2. "Cambridge Analytica's Kenya election role 'must be investigated,'" *BBC*, March 20 2018. https://www.bbc.com/news/world-africa-43471707.

3. "Facebook Admits It Was Used to Incite Violence in Myanmar," Alexandra Stevenson, *The New York Times*, November 6, 2018. https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

4. "The Crackdown: How the United States looked the other way while Bahrain crushed the Arab Spring's most ill-fated uprising," Kelly McEvers, *Washington Monthly*, March/April 2012. https://washingtonmonthly.com/magazine/marchapril-2012/the-crackdown/.

5. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," Fletcher Schoen and Christopher J. Lamb, *Strategic Perspectives*, Center for Strategic Research, Institute for National Strategic Studies, National Defense University, June 2012. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

6. "Did Media Literacy Backfire?" danay boyd, Data & Society, January 5, 2017. https://points.datasociety.net/did-media-literacy-backfire-7418c084d88d.

7. "Fact checking doesn't work (the way you think it does)," Africa Check, Chequeado, and Full Fact, June 2019. https://fullfact.org/blog/2019/jun/how-fact-checking-works/.

8. "The 'Demand Side' of the Disinformation Crisis," Dean Jackson, International Forum for Democratic Studies, August 2, 2018. https://www.ned.org/issue-brief-the-demand-side-of-the-disinformation-crisis/.

9. "Katarina Klingova: How we involved Youtubers in Media literacy campaign," Digital Communication Network, Youtube, January 4, 2019. https://www.youtube.com/watch?v=TF0gF1tAfWM.

10. "The Lie is Not the Story: Practicing Journalism in the Disinformation Age," Dean Jackson, Power 3.0 Blog, April 5, 2018. https://www.power3point0.org/2018/04/05/the-lie-is-not-the-story-practicing-journalism-in-the-disinformation-age/.

Effectively Pushing Back against Disinformation in Cyberspace: What I've Learned in the Trenches

By MARK TONER

1. President Putin's Fiction: 10 False Claims About Ukraine. U.S. Department of State. Last modified March 5, 2014. https://2009-2017.state.gov/r/pa/prs/ps/2014/03/222988.htm#.XXZ1TOfkXNA.email

The Future of Digital Empowerment: Combating Online Hate

By CHRISTINA CHILIN

1. Saad, Lydia. "What Percentage of Americans Own Guns." Gallup. Last modified August 14, 2019. https://news.gallup.com/poll/264932/percentage-americans-own-guns.aspx.

2. Simon Wisenthal Center Releases 2019 Digital Terrorism and Hate Report Card, March 14, http://www.wiesenthal.com/about/news/2019-digital-report-card.html

SOCIAL MEDIA: A POWERFUL CYBER ALLY

The U.S. Embassy's Microblog Diplomacy on Sina Weibo

By YUQI NING

1. Evan Potter (2018. The evolving complementarity of nation-branding and

2. Public diplomacy: projecting the Canada brand through "weibo diplomacy" in China, Canadian Foreign Policy Journal, 24:2, 223-237, DOI: 10.1080/11926422.2018.1469523

3. Nicholas J. Cull (2013). The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy, International Studies Review, 15:1, 123–139, DOI: https://doi.org/10.1111/misr.12026

4. Karen Hughes (2005). "Nominee For Under Secretary For Public Diplomacy and Public Affairs Testifies at confirmation Hearing before Senate Foreign Relations Committee", US Fed News Service, Including US State News, Washington, D. C.

5. Zhou, Q. A. (2011). From the Evolution of Modes in the Transformation of Public Diplomacy after the Cold War. *European Study*, 29(04),19-31.

China: Winning Hearts on the Web

By LINDSAY CAI

1. Denyer, Simon (25 October 2017). "China's Xi Jinping unveils his top party leaders, with no successor in sight". *The Washington Post*. Retrieved 25 October 2017.

2. CircleID Reporter (28, Feb. 2019). "Number of Chinese Internet Users Reaches 829 Million, More Than Double the Population of the US." *CircleID.com*

3. Swanson, Ana (5 July, 2018). "Trump's Trade War With China Is Officially Underway." *The New York Times*. (online)

4. Kuo, Kaiser. TEDxHonolulu Technology, Entertainment and Design Conference, 5 November 2009.

5. Stevens, T. & Mazuca, P. *Relevance Report 2020*. "Tiktok Isn't Just For Teens Anymore." Los Angeles: USC Center for Public Relations, 2020.

6. 中国网推荐. May 29, 2019. CGTN主持人应战福克斯主播 中美贸易战隔空辩论即将上演. https://baijiahao.baidu.com/s?id=1634829722060953601&wfr=spider&for=pc

7. Woodhams, Samuel. *TheDiplomat.com* (23, Feb. 2019) "How China Exports Repression to Africa." https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/

8. China Power Team. "How is China bolstering its military diplomatic relations?" China Power. October 27, 2017. Updated December 18, 2017. Accessed November 29, 2019. https://chinapower.csis.org/china-military-diplomacy/

YouTubers as Digital Ambassadors: A Case Study of Ychina

By JINZHEN YANG

1. Cull, N. J. (2011). WikiLeaks, public diplomacy 2.0 and the state of digital public diplomacy. Place Branding and Public Diplomacy,

Footnotes (cont.)

7(1), 1-8.

2. Payne, G., Sevin, E., & Bruya, S. (2011). Grassroots 2.0: Public diplomacy in the digital age. Comunicação Pública, 6(n10), 45-70.

Defeats and Defects of Spanish CyberDiplomacy Toward the Arab World

By SAMER ALNASIR

1. Pay attention that the Spanish civil code, art. 17 distinguishes between original Spanish citizens and "acquired" Spanish citizenship, where the latter has to pass an additional 10 years to be considered as a consolidated Spanish citizen, as stated in art. 18. Meanwhile article 11.2 of the Spanish constitution establishes that an original Spanish citizen cannot be stripped of his nationality, so Arabic citizens originally from these cities in North Africa are original Spanish citizens within all effects. Meanwhile they still, due to their original race and religion, are considered as an exceptional category of citizens, their identity aligned to Morocco more so than their citizenship to Spain, just as a simple administrative status.

2. The Spanish Embassy in Qatar website [consulted at 16 October 2019] at: https://www.facebook.com/SpainEmbassyQatar/posts/2156251067752593.

3. The Spanish Embassy in Morocco website [consulted on 16 October 2019] at: https://www.facebook.com/EmbEspMarruecos/posts/1962957347345409

4. Moroccan local daily news media available on 16 October 2019 at: https://lakome2.com/politique/104111.

5. Cervantes Institute of Marrakesh - Morocco Facebook, available on October 16 2019, at: https://www.facebook.com/Instituto.Cervantes.Marrakech/posts/1185679811582602

Sources:

Gershenson, Carlos. ¿Cómo hablar de complejidad?. Lengua Sociedad y Comunicación, nº 11 (2013), DOI: https://doi.org/10.1344/LSC-2013.11.3.

Manfredi, Juan Luis. El desafío de la diplomacia digital, Elcano, available online on October 16, 2019 at: http://www.realinstitutoelcano.org/wps/wcm/connect/83e13f004340cd358e95fe788bd2636c/ARI15-2014-Manfredi-desafio-diplomacia-digital.

PWC. Spain in the World 2033, a report managed by Javier Solana in cooperation with the Spanish Minister of Foreign Affairs, 2014. Available online on October 16, 2019 at: https://www.pwc.es/es/publicaciones/economia/assets/espana-en-el-mundo-2033.pdf

Una Visión Estratégica Para España En Asia 2018 – 2022, Spanish Minister of Foreign Affairs, available on October 16, 2019 at: http://www.exteriores.gob.es/Portal/es/SalaDePrensa/Multimedia/Publicaciones/Documents/ESTRATEGIA%20DE%20ACCION%20EXTERIOR%20castellano.pdf.

PREPARING FOR THE CYBER FUTURE

Bottom Lines and Data Dossiers: How Big Tech Commodifies Your Privacy

By DEVIN VILLACIS

1. Balkin, Jack, "The First Amendment in the Gilded Age," *Buffalo Law Review*, 66, no. 5 (December 2018): 980.

2. Ibid.

3. Cohen, Julie E., "Surveillance vs. Privacy: Effects and Implications," *Cambridge Handbook of Surveillance Law*, eds. David Gray & Stephen E. Henderson, (August 2017): 455.

4. Lake, David A, "International Political Economy: A Maturing Interdiscipline," in *The Oxford Handbook of Political Economy*, eds. Donald A. Wittman and Barry R. Weingast (Oxford: Oxford University Press, 2008), 768.

5. Hardy, Jonathan, "Critical political economy of communications: A mid-term review," *International Journal of Media & Cultural Politics*, 10, no. 2 (2014): 192.

6. Ibid.

7. Lohr, Steve, "New Google and Facebook Inquiries Show Big Tech Scrutiny Is Rare Bipartisan Act," *The New York Times*, September 6, 2019, accessed September 7, 2019, https://www.nytimes.com/2019/09/06/technology/attorney-generals-tech-antitrust-investigation.html.

8. McChesney, Robert W. and Dan Schiller, "The Political Economy of International Communications: Foundations for the Emerging Global Debate about Media Ownership and Regulation," *Information Technologies and Social Development*, Geneva: United Nations Research Institute for Social Development, 2003: 8.

9. Facebook, Inc., *Facebook Reports Fourth Quarter and Full Year 2018 Results*, Menlo Park, CA: Facebook, Inc., p.1, accessed October 10, 2019, https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx.

10. Alphabet Inc., *Alphabet Announces Fourth Quarter and Fiscal Year 2018 Results*, Mountain View, CA: Alphabet Inc., p. 5, accessed October 10, 2019, https://abc.xyz/investor/static/pdf/2018Q4_alphabet_earnings_release.pdf?cache=adc3b38.

11. Apple Inc., *Apple Reports Fourth Quarter Results*, Cupertino, CA: Apple Inc., p. 2, accessed October 10, 2019 https://www.apple.com/newsroom/pdfs/Q4-FY18-Consolidated-Financial-Statements.pdf.

12. Crawford, Susan, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*, New Haven: Yale University Press (2013): 3.

13. Comcast Corporation, *Comcast Reports 4th Quarter and Full Year 2018 Results*, Philadelphia, PA: Comcast Corporation, p. 1, accessed October 10, 2019, https://www.cmcsa.com/node/32411/pdf.

14. Balkin, Jack, "The First Amendment in the Gilded Age": 994.

15. Zuboff, Shoshana, "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology*, 30, no. 1 (March 2015): 75.

16. Balkin, Jack, "The First Amendment in the Gilded Age": 991.

17. Lee, Kai-Fu, *AI Superpowers: China, Silicon Valley, and the New*

World Order, New York: Houghton Mifflin Harcourt Publishing Company (2018): 16.

18. Apple Inc., "Improving Siri's privacy protections," in *Apple Newsroom,* August 28, 2019, accessed November 15, 2019, https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/.

19. Hern, Alex, "Apple contractors 'regularly hear confidential details' on Siri recordings," *The Guardian*, July 26, 2019, accessed October 10, 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

20. Balkin, Jack and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy," *The Atlantic*, October 3, 2016, accessed November 15, 2019, https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

21. Granville, Kevin, "Facebook and Cambridge Analytica," *The New York Times*, March 19, 2018, accessed October 23, 2019, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

22. Barrett, Lindsey, "Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries," *Seattle University Law Review*, 42, no. 3 (March 2019): 1087.

23. Ibid, 1084.

24. Balkin, "The First Amendment in the Gilded Age": 1007.

25. Ibid, 1007 and 1010.

26. Varian, Hal R, "Beyond Big Data," *Business Economics*, 49, no. 1 (January 2014): 28.

27. Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization": 83.

28. Balkin, "The First Amendment in the Gilded Age": 1007.

29. Barrett, "Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries": 1062-1063.

30. Cohen, "Surveillance vs. Privacy: Effects and Implications": 457 and 462.

31. Ibid, 464.

32. Ibid, 466.

33. Mahajan, Rohit, Shree Parthasarathy and Manish Sehgal, 2019, "India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation: A comparative view," Risk Advisory, Deloitte Touche Tohmatsu India LLP, accessed November 23, 2019, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf.

34. Sharma, Aditya, "India's Data Bill Sets New Precedent on Privacy and Protection. But Whose Data Is It Anyway?" *News18*, November 22, 2019, accessed November 24, 2019, https://www.news18.com/news/india/indias-data-bill-sets-new-precedent-on-privacy-and-protection-but-whose-data-is-it-anyway-2396195.html.

Replacement or Displacement: Preparing for the Fourth Industrial Revolution

By JESSICA CHAN-UGALDE

1. Marr, Bernard. "The 4th Industrial Revolution Is Here - Are You Ready?" *Forbes*, Forbes Magazine, 14 Aug. 2018, www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/#4831e609628b.

2. Xiao, Eva. "From Dark Warehouses to Delivery Robots, Chinese Ecommerce Figures out Models of Automation." *Tech in Asia - Connecting Asia's Startup Ecosystem*, 8 Nov. 2017, www.techinasia.com/jd-x-logistics-unmanned-warehouses.

3. Khalid, Asma. "A Dirty Word In The U.S., 'Automation' Is A Buzzword In China." *A Dirty Word In The U.S., 'Automation' Is A Buzzword In China | Bostonomix*, WBUR, 20 Nov. 2017, www.wbur.org/bostonomix/2017/11/20/china-automation.

4. McBride, James, and Andrew Chatzky. "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, Council on Foreign Relations, 13 May 2019, www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

5. Wen, Yi. "China's Rapid Rise: From Backward Agrarian Society to Industrial Powerhouse in Just 35 Years." *Federal Reserve Bank of St. Louis*, The Regional Economist, Apr. 2016, www.stlouisfed.org/~/media/publications/regional-economist/2016/april/lead.pdf.

6. Allen, Gregory, and Kania, Elsa B. "China Is Using America's Own Plan to Dominate the Future of Artificial Intelligence." *Foreign Policy*, 8 Sept. 2017, foreignpolicy.com/2017/09/08/china-is-using-americas-own-plan-to-dominate-the-future-of-artificial-intelligence/.

7. Rusli, Evelyn M. "Amazon.com to Acquire Manufacturer of Robotics." *The New York Times*, The New York Times, 19 Mar. 2012, dealbook.nytimes.com/2012/03/19/amazon-com-buys-kiva-systems-for-775-million/.

8. Wingfield, Nick. "As Amazon Pushes Forward With Robots, Workers Find New Roles." *The New York Times*, The New York Times, 10 Sept. 2017, www.nytimes.com/2017/09/10/technology/amazon-robots-workers.html.

9. Ibid.

America Unplugged? The Effects of Net Neutrality on Cyber-diplomacy

By JOSHUA MORRIS

1. Ivushkina, Elena B., Natalia Z. Alieva, Irina B. Kushnir, and Olga M. Kalmykova. "The Internet of Things as a Precondition of Development of the ICT Global Infrastructure." In *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*, pp. 1003-1009. Springer, Cham, 2019.

2. Cheng, Hsing Kenneth, Subhajyoti Bandyopadhyay, and Hong Guo. "The debate on net neutrality: A policy perspective." *Information systems research* 22, no. 1 (2011): 60-82.

3. Kendall, Brent, and McKinnon, John D. "Net Neutrality Rollback Faces Legal Challenges Testing Trump Agenda." *The Wall Street Journal Eastern Edition*. Dow Jones & Company, Inc., February 1, 2019.

Footnotes (cont.)

4. Crookes, David. "Our Guide to Net Neutrality." *Web User*, no. 427 (July 12, 2017): 36–37. http://search.proquest.com/docview/2010639652/.

5. Stern, Lendsay. "Broadband Providers Are Quietly Taking Advantage of an Internet Without Net Neutrality." *Public Knowledge*, January 29, 2019. https://www.publicknowledge.org/blog/broadband-providers-are-quietly-taking-advantage-of-an-internet-without-net-neutrality-protections/

6. "Save the Internet: What You Need To Know." *Free Press Net* https://www.freepress.net/issues/free-open-internet/net-neutrality/net-neutrality-what-you-need-know-now

7. Finley Clint, "A $60 Million Fine Won't Stop AT&T From Throttling 'Unlimited' Data Plans." *Wired*, May 11, 2019. https://www.wired.com/story/ftc-att-unlimited-data-throttling-fine/

8. Molla, Rani. "Verizon and AT&T Customers are Getting Slower Speeds because of Unlimited Data Plans." *Vox*, August 2, 2017. https://www.vox.com/2017/8/2/16069642/verizon-att-tmobile-sprint-mobile-customers-slow-speeds-unlimited-data-plan

9. Fung, Brian. "The F.C.C. Just Voted to Repeal its Net Neutrality Rules, In A Sweeping Act Of Deregulation." *The Washington Post*, December 14, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/12/14/the-fcc-is-expected-to-repeal-its-net-neutrality-rules-today-in-a-sweeping-act-of-deregulation/

10. Kendall, Brent, and McKinnon, John D. "FCC Rollback of Net Neutrality Rules Is Partly Upheld by Appeals Court.(Tech)." *The Wall Street Journal Eastern Edition*. Dow Jones & Company, Inc., October 2, 2019.

Decentralizing Diplomacy: Convening in the Digital Age

By BRETT SOLOMON and NIKKI GLADSTONE

1. David Batty, "Arab spring leads surge in events captured on cameraphones", 2011, https://www.theguardian.com/world/2011/dec/29/arab-spring-captured-on-cameraphones (accessed on October 12, 2019).

2. WikiLeaks, "Spy files Releases", 2011, https://wikileaks.org/the-spyfiles.html (accessed on October 12, 2019).

3. Jo Best, "IBM Watson: The inside story of how the Jeapardy-winning supercomputer was bron, and what it wants to do next", 2013, https://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/ (accessed on October 12, 2019).

4. Wired, "Tech 2011: Biggest news stories of the year", 2011, https://www.wired.com/2011/12/tech-2011-biggest-news-stories-of-the-year/ (accessed on October 12, 2019).

5. Berhan Taye and Sage Cheng, "The state of internet shutdowns", 2019, https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/ (accessed on October 14, 2019)

6. Lucie Krahulcova, "New report: FinFisher changes tactics to hook critics," 2018, https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/ (accessed on October 14, 2019)

7. Lindsey Andersen, "Human rights in the age of artificial intelligence," 2018, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf (accessed on October 14, 2019).

8. James Vlahos, "Smart talking: are our devices threatening our privacy?", 2019, https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy (accessed on October 14, 2019).

9. Sarah Harper, "Getting ready for 2020: The RightsCon program past, present, and future", 2019, https://www.rightscon.org/the-rightscon-program-past-present-and-future/, (accessed on October 16, 2019).

10. RightsCon, "RightsCon Brussels 2017 programme", 2017, https://www.rightscon.org/cms/assets/uploads/2017/03/RightsCon-Brussels-2017-Official-Program.pdf (accessed on October 16, 2019).

11. RightsCon, "RightsCon Toronto 2018 program", 2018, https://rightscon2018.sched.com/, (accessed on October 16, 2019).

12. RightsCon, "RightsCon Tunis 2019 program," 2019, https://rightscon2019.sched.com, (accessed on October 16, 2019).

13. Nikki Gladstone and Sarah Harper, "On the RightsCon agenda: Technology in the time of climate crisis", 2019, https://www.rightscon.org/technology-in-the-time-of-climate-crisis/, (accessed on October 16, 2019).

14. Michael Silberman, "What advocacy organisations need to win today", 2019, https://mobilisationlab.org/stories/what-advocacy-organisations-need-to-win-today/, (accessed on October 16, 2019).

15. RightsCon, "RightsCon Tunis 2019 Community Learnings," 2019, https://www.rightscon.org/cms/assets/uploads/2019/06/RC19-RightsCon-Tunis-2019_-Community-Learnings-draft-2.pdf, (accessed on October 16, 2019).

16. Access Now, "Access Now and Amnesty International launch Toronto Decaration on human rights and artificial intelligence", 2018, https://www.accessnow.org/access-now-amnesty-international-launch-toronto-declaration/, (accessed on October 16, 2019).

17. "Civil society groups form coalition to demand parity, transparency, and accountability from Facebook in the Global South", 2018, https://drive.google.com/file/d/1hawh_RIedi0z5VcciHMD7DLPiqPK6kBp/view, (accessed on October 16, 2019).

18. OHCHR, "UN experts stress links between digital space and human rights at RightsCon, Tunis", 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24696&LangID=E, (accessed on October 16, 2019).

19. Berhan Taye, "#IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan!" 2019, https://www.accessnow.org/iamthesudanrevolution-theres-a-direct-link-between-internet-shutdowns-and-human-rights-violations-in-sudan/, (accessed on October 16, 2019).

SIGNATURE PUBLIC DIPLOMACY TRAINING

TWO WEEKS OF MULTI-DISCIPLINARY, SOLUTION-DRIVEN LEARNING IN LOS ANGELES

Now in its 15th year, CPD's flagship training program is an opportune time and place to reflect and build your public diplomacy toolkit, while drawing on the latest social science research, critical thinking, storytelling tools and network-building opportunities.

MODULES

- Smart Power, Soft Power & Fundamentals of PD
- Integrating Data & Storytelling in PD Strategy
- Stakeholder & Influencer Analysis
- Influence & Advocacy
- Case Studies in Crisis Communication
- Data-Driven PD: Theory of Change, Research Methods, Performance & Measurement
- Digital Analytics & Algorithms
- Cultural Diplomacy: Cases & Impact
- Movement as Information: Cross-Cultural Communication
- Digital Insights and AI for PD Campaigns
- National Security Concepts & Communications
- Media & Public Opinion Framework
- Nation/Place Branding
- Framing Public Diplomacy
- AI & Bots for Public Diplomacy
- Digital Storytelling
- Creating Visual Content for PD
- Virtual Reality & Immersive Storytelling for PD
- Countering Disinformation: Beyond "Fake News"
- Designing & Planning PD Strategies

Summer Institute 2020 will run from **July 12–24** and will take place at the University of Southern California.

For more information, please contact us:
cpdevent@usc.edu

APPLY now at USCPublicDiplomacy.org | Deadline April 17, 2020

Society of Public Diplomats

USC Annenberg
School for Communication and Journalism

CPD

WINTER 2019
www.publicdiplomacymagazine.com