

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/331073991>

Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation

Technical Report · November 2017

DOI: 10.13140/RG.2.2.29664.33283

CITATIONS

2

READS

652

1 author:



Hamid Akin Ünver
Özyeğin University

70 PUBLICATIONS 462 CITATIONS

SEE PROFILE

November 2017

Computational Diplomacy

H. Akin Ünver, Kadir Has University & EDAM

This paper was supported by
Robert Bosch **Stiftung**

Computational Diplomacy

H. Akin Ünver

“If one is to be able to handle, successfully, such drastic uncertainty which The (Machiavellian) Prince meets in those political situations where conflicts are a life and death issue and in which no rules apply, one needs to be flexible. One needs to be a fox and foxes flex the language.”¹

Foreign Policy Communication in the Age of Algorithms and Automation

Uncertainty is a foundational aspect of politics and diplomacy. Critical elections, armed conflicts, ally/adversary behavior, explicit/implicit threats are fundamentally uncertain, yet core processes of statecraft, diplomacy and politics. That's why over centuries, diplomacy has grown into an art form of managing high-risk uncertainties between nations and institutions. Uncertainty isn't trivial, or secondary, since it has direct impact on policy and fortunes of nations through costly miscalculations. Cognitive processes, misperception and elite psychology have thus grown into central themes of inquiry in international relations research through the Cold War and continued to define foreign policy research after the fall of the Berlin Wall. War onset, results of diplomatic negotiations or how people behave during emergencies or crises, are all variables in a three-dimensional equation, determining power relations at the global level.

Uncertainty is also a communicative process. How we understand, contextualize and navigate through uncertainty depends on verbal and nonverbal cues. That's why historically, articulation, tact and acumen grew into key qualities of good emissaries and ambassadors, as they communicated power relations between nations. This is also the main reason why states always sought to narrow down their key communications into a small audience of highly qualified individuals, specifically trained in the art of uncertainty management. As more people got involved in political processes, leaks became more likely, but perhaps more importantly, sides lost their common political language to navigate through periods

of uncertainty. As communication technology progressed, diplomatic processes had to adapt in order to protect both secrets and also common language. Take for example how the invention of writing led to the development of seals of authentication, printing press to mechanical cipher, telegram to morse code and radio to modern encryption.

From this perspective, digital diplomacy sounds like an unnatural progression in the long history of technology and diplomatic communication. Politics online is anything but hierarchical, unidirectional or secret. From Ministers of Foreign Affairs to notetakers, all parties to a political or diplomatic process have equal access to social media platforms, or can build a website. Quality of content determines follower count and diplomatic language is replaced by a new type of tech language, where emojis, directness and snark have a higher value than elaborate, long explanations. 'It is rather complicated' is the motto of diplomacy, yet the craft itself is moving into the domain of 140-word explanations and emojis. In November 2016, Guardian reported that Whatsapp was becoming the primary medium of communication among diplomatic circles, even during some of the key voting and negotiating processes in the UN and the EU headquarters.² The spread of Whatsapp among diplomatic circles was alarming as the UK Foreign Office reported that its diplomats were using the platform instead of the specially designed encrypted messaging application. User-friendly platforms always win over clunky, elaborate interfaces and design is always often popular than security; especially for

¹ Airaksinen, T. 'Against all the odds: Machiavelli on Fortune in Politics' in Donskis, L. (Ed.). (2011). Niccolò Machiavelli: history, power, and virtue (Vol. 226). Rodopi.

² Julian Borger Jennifer Rankin in Brussels and Kate Lyons, "The Rise and Rise of International Diplomacy by WhatsApp," The Guardian, November 4, 2016, sec. Technology, <https://www.theguardian.com/technology/2016/nov/04/why-do-diplomats-use-this-alien-whatsapp-emoji-for-vladimir-putin>.

Social media space is increasingly more vulnerable to ‘digital spoilers’, such as trolls and bots, that amplify messages (including leaks) by the millions.

younger diplomats. Furthermore, as evidenced by a succession of high-profile leaks by Edward Snowden, Julian Assange, Chelsea Manning and many others, even the best-kept state secrets can be leaked. In the past, such leaks would involve intelligence agencies, or media companies. Now all leaks are public and governed by the same attention economy metrics as advertisements. Furthermore, social media space is increasingly more vulnerable to ‘digital spoilers’, such as trolls and bots, that amplify messages (including leaks) by the millions.

States now have to craft more ingenuous policy positions and elaborate national strategies as some of the deepest secrets of their nation are distributed online, shared in the millions, all while their governments are paralyzed without a clear agenda on how to tackle such processes. Before diplomacy could adapt to ‘digital’, it is now faced with problems from more advanced computational aspects of technology. From this perspective, MFAs have to adapt to three layers of computational challenges. The first of these is size (volume). Digital interconnectedness has increased the number of actors and parties in key political processes, reducing the level of influence in diplomacy to the random online citizen. Unprecedented volumes of information and opinion flows in digital space, weakening states’ control over their nation’s image, policy and branding. Government-led PR campaigns tend to be more boring, less imaginative and ‘gray’, inevitably losing against more creative and vibrant offerings of non-state actors. Second, digital communication is instantaneous. Communicative processes of high-priority and high-risk political issues rapidly proliferate online, far exceeding states’ ability to respond through traditional modes and policy processes. States’ adaptation to digital platforms not only requires an upgrade in tools, but also in the way of thinking and responding to emergencies. Finally, not all information that travels online is true. Often, in the heat of the moment, misleading information or doctored images spread rapidly, bringing in the necessity for states to verify and correct mis-

takes to prevent escalation. Recently however, states themselves have begun flirting with these misleading content types to gain the upper hand against their diplomatic rivals, which is blurring the lines between states and non-state actors in legitimate digital political communication.

Digital diplomacy (or Internet, cyber, e-, Diplomacy) emerged as a state reaction to its growing irrelevance in digital space. process. States were forced to discover and seize the potential of these capabilities, only after a succession of three high-profile international crises, that demonstrated the extent to which they were left behind in the digital communication revolution. The emergence of ‘digital diplomacy’ as a global concept coincides with the onset of the 2010 Arab Spring and Occupy movements that emerged in 2011. When fuelled with enough grievances and social organizational power, digital technologies allowed masses to mobilize against, and threaten state power, sometimes fundamentally changing power relations in their country, such as in the cases of government toppling in Egypt and Tunisia. These technologies were also challenging state narratives and framing of social and political events, bypassing traditional modes of state propaganda, as well as existing governmental controls on mass media outlets. As a result, states began to strategize to establish digital representation and communication practices, gradually evolving into digital diplomacy practices that we know of today.

The emergence of ‘digital diplomacy’ as a global concept coincides with the onset of the 2010 Arab Spring and Occupy movements that emerged in 2011.

A second evolutionary trigger of digital diplomacy was the rise of ‘citizen journalism’ phenomenon. The emergence of a global caste of citizen reporters that established digital and real-time news dissemination networks online, was perhaps the greatest challenge to states’ control over information. Marginalized in the business model of state - mass media relationship, the neglected practice of local reporting received an unprecedented boost with digital technologies, allowing any individual to be able to gather news at the street level and share it with global audiences, bypass-

ing the hegemonic state-media power. Then came another trigger: the spread of extremist content online and digital recruitment. 'Digital radicalization' became popularized with the rise of the Islamic State in Iraq and Syria (ISIS) and the term then almost exclusively referred to jihadi extremist messaging online. Although equally large networks of radicalization and extremist messaging can be observed in European and American digital space, states' digital focus is still very much concentrated on online jihadi networks. Yet, growing range of threats from other tints of global radicalization will inevitably awaken states to the need to think about the phenomenon as a trans-cultural topic. The need to counter all ranges of radical messages and frames online will eventually add another layer of responsibility to digital diplomacy: formulating and disseminating alternative religious, political and social messages and preventing the spread of radical content online.

The pace with which communication technologies evolve, will render the concept of 'digital diplomacy' obsolete, before it even became mainstream. The evolutionary impulses of political communication are being increasingly driven by automation and computation, and seek to overload, overwhelm and distract collective attention on a global scale. Websites and social media actors are no longer necessarily 'human' and 'bots' - that are operated by a single programmer - can mass-produce digital content at a theoretically infinite scale. Such digital content can be factually false, misleading or anachronistic and can easily flood social media systems during emergencies and crises. They can impair diplomatic communication and escalate inter-state disagreements; worse, they can bypass governments and influence entire populations at key political junctures. By increasing the likelihood of misperception, they also render armed escalations more likely. To that end, automation sits at the heart of modern diplomatic evolution and requires a new framework and strategy that goes beyond 'digital'.

Online Diplomatic Behavior: Who Speaks on Behalf of the State?

Digital communication technologies have fundamentally altered the nature of diplomacy by changing the very environment diplomats function. In October 2012, during the

“
Digital communication technologies have fundamentally altered the nature of diplomacy by changing the very environment diplomats function.
”

U.S. Presidential election debate, Barack Obama and Mitt Romney were at loggerheads with each other over the behavior of American diplomatic representatives in Libya and Egypt. The debate was whether the members of US foreign mission in Tripoli and Cairo were right in issuing online support and tweets for the anti-government protests, without a clear government policy. Obama had to walk a fine line between his government's necessity to control US diplomats' online expression and not denouncing ongoing protests against Muammar Ghaddafi and Hosni Mubarak.³ The digital revolution and social media platforms reduced the costs of political engagement for all parties and strengthened the communicative agency of diplomats, but also created a new domain of political authority; one that doesn't necessarily play along with offline state interests. Should states restrict their diplomats' presence online and risk irrelevance, or should they allow individual expressions of opinion and dismiss them as 'not representative of the state'?

Fast forward to August 2014, when western world capitals were hotly debating Russian involvement in Ukraine (specifically, whether Russian soldiers were directly engaged in the clashes in Donbass region). Simultaneously, Russia was mounting one of its best-funded and highest profile diplomatic defenses against these 'allegations', insisting that armed men in Donbass were pro-Russian locals. Around the same time, a Russian signal corps sergeant - Alexander Sotkin - began posting geotagged selfies from within Ukrainian territory, soon joined by other Russian artillery, logistics and combat troops.⁴ These goofy and clueless social media posts on Russian media platforms VKontakte and Odnok, eventually proliferated in Twitter, Facebook through mass sharing, ultimately nullifying state-sponsored propaganda efforts of Moscow.

³ Brian Fung, "Digital Diplomacy: Why It's So Tough for Embassies to Get Social Media Right," The Atlantic, October 17, 2012, <https://www.theatlantic.com/international/archive/2012/10/digital-diplomacy-why-its-so-tough-for-embassies-to-get-social-media-right/263744/>.

⁴ Sean Gallagher, "The Sad, Strange Saga of Russia's 'Sergeant Selfie,'" Ars Technica, August 14, 2014, <https://arstechnica.com/information-technology/2014/08/the-sad-strange-saga-of-russias-sergeant-selfie/>.

MFAs, embassies and diplomats are online actors willingly or not, and their offline activities are getting influenced increasingly by issues that have a significant digital component.

Whether a nation, its diplomats, soldiers or ministers should formally exist in digital space is a trickier question than the mainstream debate suggests. MFAs, embassies and diplomats are online actors willingly or not, and their offline activities are getting influenced increasingly by issues that have a significant digital component. Arguments in favor of digital engagement include the ability to shift, mold and influence global public opinion with much lower costs compared to traditional forms of public diplomacy. Politicians, diplomats, ministries and international organizations already tap into this influencing capacity for positive (i.e. charm offensive, cultural engagement, awareness-building), as well as negative (heated online arguments, defensive comments, propaganda) reasons. For example following the coup attempt in Turkey in July 2016, Turkish MFA has launched one of the best-coordinated examples of digital diplomacy. A wide network of Turkish embassies, as well as members of mission, used their Twitter accounts to disseminate information, videos and photos to build awareness in foreign capitals. In the deep uncertainty of the immediate post-coup phase, MFA's sentiment-neutral messaging travelled farther and shared more across foreign media outlets, compared to the government-led combative and antagonistic messaging, that was mostly shared within Turkey. The country has since then become an instrumental part of global political engagement, from the Jerusalem protests to Rohingya crisis. In a previous piece, I discussed how Turkey got involved in the Jerusalem crisis through a combination of official and unofficial digital campaigning.⁵

Yet, mere presence of large numbers of government or institutional actors online doesn't qualify as a successful social

media or nation-branding campaign. One common mistake is to think of digital nation-branding as a one-way street, in which official government or institutional positions are simply uttered online, without any direct engagement with interested online parties. Such campaigns are viewed as dull, uninteresting and unimaginative, effectively yielding questionable multiplier effects on states' existing image. On the other end of the spectrum however, are the 'social media diplomats/ministers', that favor direct engagement with online actors, but share too much, effectively making statements that do not converge with government policy, ending up generating controversy rather than engagement. The balance isn't always straightforward and tends to be heavily subjective. One of the good examples of this balance has been Israeli MFA's culture-oriented nation-branding campaign, which steers clear of thorny political issues and follows direct engagement with questions on Twitter, Facebook and Youtube on Israeli cuisine, artists and daily life.⁶

How much should states commit to online representation, just like other forms of diplomacy, requires a strategy. Although there is increasingly more quality research on the topic, we are still very much in the dark over what makes a digital campaign successful and especially how do political and non-political media campaigns are consumed and distributed differently. This is because what constitutes as 'success' in digital space, is highly subjective and context-specific. This renders political social media campaigns hard to control and even harder to measure in terms of their impact and success. Often, well-led digital media efforts can suffocate among other well-led brand or event campaigns, generating far less engagement, or yielding unintended diplomatic outcomes than desired. One example was the Russian Airstrike Watch unit under the British Foreign Office, which tweeted real-time information on Russian bombing operations in Syria.⁷ Challenging Russia's narrative of targeting, frequency and strategy in Syria, this unit eventually generated a Russian backlash against the British Government itself. While the campaign itself was apparently successful from a digital media point of view, diplomatically it impaired Britain's ability to pressure and bargain against Russia in Syria. Furthermore, some of the best-led and best-distributed digital media campaigns failed to bring about the change they

⁵ Unver, Akin. 'What Twitter can tell us about the Jerusalem protests' The Washington Post. 28 August 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/08/26/what-twitter-can-tell-us-about-the-jerusalem-protests/?utm_term=.52f561258ead

⁶ Unver, Akin. 'What Twitter can tell us about the Jerusalem protests' The Washington Post. 28 August 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/08/26/what-twitter-can-tell-us-about-the-jerusalem-protests/?utm_term=.52f561258ead

⁷ Worley, Will, "Russians Stage 'Retaliation Protest' Outside British Embassy," The Independent, November 4, 2016, <http://www.independent.co.uk/news/world/europe/russia-british-embassy-moscow-retaliation-protest-demonstration-aleppo-syria-a7398441.html>.



Although there is increasingly more quality research on the topic, we are still very much in the dark over what makes a digital campaign successful and especially how do political and non-political media campaigns are consumed and distributed differently.



desired. One of the best examples of a highly professional digital media campaign was #bringbackourgirls - dedicated to 276 Nigerian students kidnapped by Boko Haram. Although the campaign was widely shared and received high-level of attention (including Presidential) it ended up having virtually no real effect on the outcome of the hostage situation. Some of the chibok girls were released, but long after the campaign and with no visible response to the popularity of the digital effort.⁸

These instances point to the necessity of a well-thought out strategy that connects a nation's offline interests to its online presence, in a way that reinforces both domains. Digital diplomacy doesn't exist in a vacuum and is a highly interactive process, where every tweet, like and share is a digital activity and are interpreted as state policy. A diplomat retweeting, or liking a particular foreign policy article will be interpreted by journalists as a formal government position and will be produced into a news article in that light. Denials or clarifications will usually arrive much later than the incident enters into news cycle and even then, clarifications will not be as popular as the made-up news. Especially in contested issues, there will always be a challenge or a backlash against MFA-led digital media campaigns. Not only rival embassies

or MFAs, but foreign government officials, celebrities and random citizens alike will join the conversation. But these essentially human-led accounts aren't the main problem. What happens when this challenge comes from thousands of anonymous accounts, posting irrelevant or simply wrong information by the thousands?

Computational Propaganda: Attention Economy in International Crises

Marketing and advertising have predominantly relied on attracting consumer attention as a form of currency. As advertising got digital, so did political advertising and propaganda. Digital advertising is structured upon the premise that our digital footprint can - and should - be monetized, at increasingly lower marginal costs. The content that we share online, along with people we follow, or personal information we post across our social networks returns back to us in the form of tailored advertisements. Political campaigns too, use similar tools. Companies, politicians, ministries, celebrities all compete for attention and produce content that has the best likelihood of getting shared and surviving online. Attention has always been a scarce resource, although digital media and communication increased its value substantially, as the production costs of digital content became far cheaper than consumption costs. This was foreseen by Herbert Simon, who has first coined the term 'attention economics'⁹ in 1971 in reference to the overabundance of information, with the likes of Thomas Davenport and John Beck¹⁰, Michael Goldhaber¹¹ and Georg Franck¹² expanding the term as it relates to information overload in business and marketing. The term took on its more relevant form in social media through Huberman (et. al.) 2008 piece, which asserted that the digital media has strengthened the agency of ordinary people for whose attention multi-million dollar companies, states, intelligence agencies and presidential candidates all competed.¹³

⁸ Maeve Shearlaw, "Did the #bringbackourgirls Campaign Make a Difference in Nigeria?," The Guardian, April 14, 2015, sec. World news, <https://www.theguardian.com/world/2015/apr/14/nigeria-bringbackourgirls-campaign-one-year-on>.

⁹ Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," The American Political Science Review 79, no. 2 (1985): 293-304, doi:10.2307/1956650.

¹⁰ Thomas H. Davenport and John C. Beck, The Attention Economy: Understanding the New Currency of Business (Harvard Business Press, 2002).

¹¹ Michael H. Goldhaber, "The Attention Economy and the Net," First Monday 2, no. 4 (April 7, 1997), <http://firstmonday.org/ojs/index.php/fm/article/view/519>.

¹² Georg Franck, "The Scientific Economy of Attention: A Novel Approach to the Collective Rationality of Science," Scientometrics 55, no. 1 (September 1, 2002): 3-26, doi:10.1023/A:1016059402618.

¹³ Bernardo Huberman, Daniel M. Romero, and Fang Wu, "Crowdsourcing, Attention and Productivity," Journal of Information Science 35 (October 17, 2008), doi:10.2139/ssrn.1266996.

“Emotion eliciting content, produced at increasingly larger quantities eventually became an arms race, following an escalation pattern that brought about computer programs called ‘bots’.”

This naturally changed how political messaging and propaganda works. Competing over attention means producing both higher quantities of and more striking (not necessarily higher quality) digital content. Visuals that trigger people’s extreme emotional response mechanisms of hate, outrage, fear or lust eventually dominate social media metrics and online behavior patterns, forcing the field to evolve into more darker corners of human nature. Automation sits at the heart of this debate. Emotion eliciting content, produced at increasingly larger quantities eventually became an arms race, following an escalation pattern that brought about computer programs called ‘bots’. These bots eventually took on tasks of spamming, posting and resharing content in digital space at a theoretically infinite magnitude. Bots gradually evolved from business and marketing related tasks to politics, heralding a new era of political communication: computational propaganda.

According to Oxford’s ‘Computational Propaganda Project’, the term refers to a vast network of automated agents, distributed across multiple media platforms in order to distract, flood and mislead public opinion.¹⁴ The primary currency of computational propaganda is a ‘bot’ (short for robot), which is a computer program that performs pre-defined automated tasks. Bots can simply utter pre-designated set of words on Twitter, like/dislike posts, or engage in more complicated assignments with the use of machine learning, such as learning how to respond to social media posts. Bots proliferate exogenous (and often unpopular) opinions, set dig-

ital agenda, generate engagement with online campaigns and beef up follower counts in digital space. When they are used in political processes, they significantly amplify fringe and radical positions, spam information providers (such as journalists) and flood the discussion by hijacking dedicated hashtags. States use bots to disrupt protests as well as each others’ digital media campaigns and non-state actors too, use bots to distract away from state-driven political agendas, or simply force participants into inaction, through mass confusion. Samuel Woolley for example, distinguishes between three types of political bots: paid ‘follower bots’ that increase politicians’ social media follower ranks, ‘roadblock bots’ that hijack popular hashtags to confuse, mislead and distract political opponents, and ‘propaganda bots’ that automatically attack online speech that is deemed ‘dangerous’ or unwanted - such as government criticism. How significant are bots in digital communication? A University of Southern California study predicts 48 million Twitter accounts (15% of all users as of 2015) are bots,¹⁵ although measuring bot activity is an inherently difficult task, due to their rapid proliferation and disappearance during key moments. Regardless of how many bot accounts there are, what renders bots troublesome is the fact that they can concentrate around a single issue, dominate and overwhelm its online debate, then disappear and reappear as necessary. As of 2016, the world’s largest number of bot infections (one bot for every 1139 users) was in Turkey, making up 18.5% of all bots in Europe.¹⁶ This renders the country in a special position with regard to computational propaganda, bot-driven political engagement and automated propaganda efforts. Other usual suspects are Russia, Italy and Germany, although lack of reliable measurement prevents us from judging the true place of China.

Bots and principles of automation that operate them are getting more advanced every day. While it was easier to recognize a bot from its monolithic and binary responses, machine learning advances allow bots to continuously improve and evolve their discursive options. Instead of disseminating previously coded word combinations, bots are now able to adapt to the language of a political movement,

¹⁴ Samuel C. Woolley and Philip N. Howard, “Automation, Algorithms, and Politics | Political Communication, Computational Propaganda, and Autonomous Agents — Introduction,” *International Journal of Communication* 10, no. 0 (October 12, 2016): 9.

¹⁵ Onur Varol et al., “Online Human-Bot Interactions: Detection, Estimation, and Characterization,” arXiv:1703.03107 [Cs], March 8, 2017, <http://arxiv.org/abs/1703.03107>.

¹⁶ Abel, Robert. ‘And the country with the most bot infections is.. Turkey’. SC Media. 5 October 2016. <https://www.scmagazine.com/turkey-tops-the-list-in-the-number-of-bot-infections/article/527590/>

reading increasingly more like a human account. It is not hard to see journalists, diplomats or politicians getting embroiled into a quarrel with a well-programmed bot during crisis situations. There are also some earlier examples of bots copying communicative structures and lexicon of key political figures, significantly adding to the high-level political confusion during emergencies. Following recent scholarly and policy emphasis on political bots on Twitter and Facebook, most of these bots moved to Tinder – where people would least expect them; in an online dating app. During the British election campaign of July 2017, a group of political programmers have developed a Tinder chatbot that would disseminate targeted political messaging to 18-25 year olds in battleground constituencies.



The volume of digital consensus is usually more important than the factual truth or the quality of the argument in getting those messages shared and this is specifically what bots are designed to do.



Factual truth in computational propaganda is often irrelevant to its success. In digital platforms, large numbers of accounts uttering the same political position creates a bandwagon effect (groupthink and availability cascade). The volume of digital consensus is usually more important than the factual truth or the quality of the argument in getting those messages shared and this is specifically what bots are designed to do. Although a number of fact-checking platforms exist globally, the time required to disseminate false information in large volumes is always shorter than verifying it conclusively. Even when a false message is quickly refuted, such messages still linger on due to confirmation bias - namely, by people who believe that the message is true because it fits their political preconceptions.

All of this incurs far greater weight over existing capacities of diplomatic communication and public engagement channels. Balance of power in computational propaganda - like cyber war - favors the offensive side as costs of defending

against such attacks require greater resources and better coordination. Even when the defender is successful (i.e. corrects disinformation quickly), psychological processes of digital information consumption still linger on. This significantly impairs individual embassies' ability to formulate responses and offer a counter-narratives in the heat of a crisis. Even when these efforts are led by a central MFA with enough resources to mount a real-time information verification crusade, content that will be posted online must go through regular channels of institutional checks and balances (bureaucracy), creating significant lags in official responses. Conversely, a faster and less controlled information campaign has the risk of sharing content that doesn't reflect government policy or MFA view on issues. Such content can unintentionally criticize government policy in another matter, sapping the campaign efforts of the MFA. Russian MFA has currently improved its use of digital communication technologies, specifically Twitter, to reconstruct its image as a dull and boring online actor. A recent example is an exchange between CIA and Russian Ministry of Foreign Affairs. As CIA tweeted a job call for Russian speaking new college graduates, Russian MFA responded with a tweet: 'We are ready to assist with experts & recommendations'.

A second issue relates to diplomatic use of automation itself. Should MFAs engage with bots in an endless battle for narrative, or should diplomatic missions create their own botnet and 'fight' with other bots? Engaging with bots is a futile task, but given increasing difficulties in recognizing well-programmed bot accounts, most people cannot tell the difference. An honest public diplomacy and digital engagement attempt can descend into an unending exchange, whereas refraining from engagement can impair digital diplomacy efforts if the account is actually human. One way around this is to respond only to verified accounts, or at least accounts that appear to have a real name. Another is to work with data scientists to create influence network maps of political processes and understand which accounts are the most influential and top-drivers of political debate in any given situation. Through engaging with central figures in an engagement network, MFAs can adjust to the changing contours of a political process and attain an efficient balance between engagement and caution. A good example of such influence network analysis is the work of Efe Sevin, whose work on MFA influence metrics in digital diplomatic networks has won the 2017 ISA ICOMM best paper award.¹⁷

¹⁷Sevin, Efe, 'Traditional Meets Digital: Diplomatic Processes on Social Media'. Paper presented at the International Studies Association 2017 Annual Conference. [https://isaicomm.wordpress.com/icomm-awards/best-paper-award/#2017 Winner](https://isaicomm.wordpress.com/icomm-awards/best-paper-award/#2017%20Winner)

Although current evidence points mainly to authoritarian governments as the primary users of bots as a form of political communication, democracies too, rely on bot-driven political engagement during key domestic events like elections or protests.

The last, and perhaps the greatest, challenge computational propaganda poses to diplomats is the fact that their own governments use them as well. Although current evidence points mainly to authoritarian governments as the primary users of bots as a form of political communication, democracies too, rely on bot-driven political engagement during key domestic events like elections or protests. In fact, Bradshaw and Howard report that 'the earliest reports of government involvement in nudging public opinion involve democracies'.¹⁸ This prevents any particular country to assume the moral high ground in computational propaganda, often offsetting image-building and PR work conducted by MFAs and diplomats. Given the multitude of interests in a crisis (government seeking to discredit a protest, intelligence services spreading false information, journalists disseminating information

"There has never been a better time to be a politician. But it's an even better time to be a machine learning engineer working for a politician."

from the ground, diplomats trying to sustain nation's image and brand), bots can quickly create mass chaos, where multiple government agencies are working against each other. The costs of uncertainty is greater for embassies in foreign soil that may not have immediate access to their ministers and either have to improvise to engage in real-time PR work in their host country, or remain silent in order not to conduct political work that may serve against home government. The scale of computational propaganda is just too big for individual embassies to make sense of and steer, significantly weakening their role during digital crises. The result reverses the diplomatic autonomy afforded by the digital media revolution and reverts back to MFA-centric missions, effectively weakening the effects of 'digital diplomacy'.

Artificial Intelligence and Complex Tasks in Foreign Affairs

Vyacheslav Polonksi wrote in his Independent column in August: 'There has never been a better time to be a politician. But it's an even better time to be a machine learning engineer working for a politician'.¹⁹ His view is supported by evidence on how different A.I. tools help politicians run campaigns, mine public opinion, predict voting patterns and engage voters to build support on key issues. A.I. research and political science are currently overlapping across a wide range of research agendas beyond elections and campaigning. The notorious case of Cambridge Analytica - the data science firm - which embarked on a micro-targeting campaign by emotion mining through voter data based on fear-based messaging,²⁰ is an important case. It is through this case that we today know that A.I. can profile people through social media data, create tailored political advertisements that cater to their emotional-psychological profile and successfully shift their political behavior as they interact with social media platforms like Facebook, Twitter or Instagram.

Digital media isn't the only place where A.I. is changing foreign policy. In June 2017, National Geospatial Intelligence Agency - the US agency in charge of drone, satellite and other aerial imagery network - decided to push for greater

¹⁸Bradshaw, Samantha and Philip N. Howard 'Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation'. Oxford Project on Computational Propaganda. Working Paper No. 2017.12. <http://comprop.oi.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>

¹⁹Polonksi, Vyacheslav, "How Artificial Intelligence Conquered Democracy," The Independent, August 9, 2017, http://www.independent.co.uk/news/long_reads/artificial-intelligence-democracy-elections-trump-brexite-clinton-a7883911.html.

²⁰Gillian Tett, "Trump, Cambridge Analytica and How Big Data Is Reshaping Politics," Financial Times, September 29, 2017, <https://www.ft.com/content/e66232e4-a30e-11e7-9e4f-7f5e6a7c98a2>.



One main consideration in the technology-diplomacy nexus is that if A.I. progress outpaces international legislative capacity, large number of countries will have to deal with the effects of technological processes that they haven't approved or even understood.



automation in visual data processing and collection.²¹ Police agencies in several developed countries are working on predictive models that collect and process real-time big data to prevent crimes before happening, or stop popular mobilization and protests before they grow in size and scope.²² All of this has implications on how threats are processed and intelligence is collected on a global scale, in addition to how states cooperate diplomatically to address the challenges of these new technologies. The challenge of A.I. on human conflict was so great that more than in 2015 a number of A.I. experts - including Stephen Hawking and Elon Musk - signed an open letter calling for deeper research into the nature of automation, along with its harmful effects.²³ One of the best-known examples of concerns in the letter related to 'machine ethics', exemplified by the question that 'who should a self-driving car choose to kill if accident is inevitable?' A similar debate brews in national security discussions on autonomous weapons systems. In August 2017, Elon Musk this time led a group of A.I. specialists with Alphabet's Mustafa Suleyman, in calling for the high contracting parties to the UN Convention on Certain Conventional Weapons (CCW) to ban on 'killer robots'.²⁴ CCW had recently initiated

a formal session of discussions on the use of autonomous weapons systems in conventional national militaries. Procedural and budget-related problems had prevented a resolution emerging from the meetings, pushing A.I. experts to greater set of worries over delays. Regulating a new arms race is a difficult task, just like regulating nuclear armament, but one that needs to be addressed, given the enormous destructive potential of such technologies. One main consideration in the technology-diplomacy nexus is that if A.I. progress outpaces international legislative capacity, large number of countries will have to deal with the effects of technological processes that they haven't approved or even understood.

While cybersecurity and cyberwar received the lion's share of diplomatic attention in the last decade, the trend is rapidly evolving into more complex issues such as A.I. governance, norm-building in automation and regulating machine learning in multinational political processes. The Economist brought the issue into mainstream policy debate in May 2017, by arguing that 'the world's most valuable resource is no longer oil, but data'.²⁵ The statement followed the current financial trends whereby big oil corporations are replaced by big data firms in terms of capital, wealth and political influence. Access to larger volumes of data is comparable to access of hydrocarbons, as companies compete with each other over the resource and state actors (at least try to) compete over control over the companies. Diplomacy has to bring in significant levels of technology know-how into negotiations as multilateral negotiations have to settle international norms on what Google can do with users' search history, Facebook with how they share personal information for sales data and how Amazon, with advertising companies.

There are also ongoing experiments in bringing data closer to the heart of diplomatic profession. Diplomatic reports and activities are performed increasingly in digital domain,

²¹ McLaughlin, Jenna, "Artificial Intelligence Will Put Spies Out of Work, Too," Foreign Policy, June 2017, <https://foreignpolicy.com/2017/06/09/artificial-intelligence-will-put-spies-out-of-work-too/>.

²² Bernard Marr, "How Robots, IoT And Artificial Intelligence Are Transforming The Police," Forbes, September 2017, <https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/>.

²³ Alex Hern, "Experts Including Elon Musk Call for Research to Avoid AI 'Pitfalls,'" The Guardian, January 12, 2015, sec. Technology, <https://www.theguardian.com/technology/2015/jan/12/elon-musk-ai-artificial-intelligence-pitfalls>.

²⁴ Samuel Gibbs, "Elon Musk Leads 116 Experts Calling for Outright Ban of Killer Robots," The Guardian, August 20, 2017, sec. Technology, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>.

²⁵ "The World's Most Valuable Resource Is No Longer Oil, but Data," The Economist, May 6, 2017, <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

Embassies will inevitably build large databases for their diasporas and engage with them in the most cost-efficient way, which will introduce multiple elements of automation into the picture.

rendering diplomacy a function of data - not the other way around. Large volumes of country data (i.e. in the UN, or EU) requires increasingly larger processing power, which in turn, will inevitably lead to the development of A.I. platforms in dealing with key country data. North Carolina government office for example, is building chatbots that are continuously improved to answer real-time constituency questions. Singaporean government too, is using Microsoft-based chatbots systems to assist their citizens in key government services such as registration, licensing and utility management. In the foreseeable future, automated legal counsel, document support, classifying and sorting diplomatic inquiries, translation and document drafting will become highly automated and will directly concern the conduct of diplomacy. Which company will handle that A.I. work and how to conceptualize that company in an international legal framework, or what the company will do with that processed data is another fu-

For example, a hypothetical A.I. diplomat negotiating a trade agreement would have real-time access to all available economic, social and political datasets, partnering with its rival A.I. diplomat to come up with a set of mutually agreeable offers, at the fraction of costs and time spent by real diplomats.

ture challenge - one that will certainly be a topic of intelligence agencies. Similar questions go to automating consular services, visa background checks, evaluations and decisions on visa outcomes. Embassies will inevitably build large databases for their diasporas and engage with them in the most cost-efficient way, which will introduce multiple elements of automation into the picture.

Further discussions need to be made on autonomous negotiation and the prospect of A.I.-based diplomacy in key bargaining processes. There are negotiation support systems that are currently in development that are applied to several legal processes, from job negotiation to bail terms. An infinite number of possibilities are calculated by A.I. platforms that continuously process key variables. For example, a hypothetical A.I. diplomat negotiating a trade agreement would have real-time access to all available economic, social and political datasets, partnering with its rival A.I. diplomat to come up with a set of mutually agreeable offers, at the fraction of costs and time spent by real diplomats. Diplomatic A.I. haggling would infinitely save time in multilateral negotiations like the Paris climate change agreement and push several deadlocked political processes into a set of solutions. This doesn't imply removing the human touch from diplomacy or politics, as personality and individual skill will still matter. Rather, AI-based negotiation imagines a diplomatic future where diplomatic bargaining is more streamlined, with redundant or time consuming tasks are outsourced to bots, whereas more important, 'high politics' processes are still managed by human diplomats. Proponents of AI diplomacy argue that human error and personal egos - primary causes of escalation - will be removed from the majority of negotiating topics, eventually leading to greater cooperation between nations. Critiques on the other hand question how objective AI diplomacy can be, since algorithms reflect biases and personality traits of another caste: programmers. Whether AI can truly be freed from human error and ego is a hotly contested topic within computer science itself and its answers aren't necessarily convincing to the critiques of AI diplomacy.

Future Trajectories in Computational Diplomacy

Contextualizing the rapid shift in communication technologies is a deeply confusing endeavor for diplomacy. The sheer size of data produced and transmitted globally everyday, prevents a proper framing of how MFAs can adapt to these rapid changes, as well as disagreements over what they exactly need to adapt to. Diplomacy has certainly more

tools available at its disposal compared to a decade ago, but also a larger, more diverse audience, less time and greater uncertainty over communication. The elaborate sets of communicative processes that emphasized trust and common language developed over the course of centuries are becoming increasingly obsolete, unnecessary and slow. States too, have new sets of interests online and in digital platforms that are built on automation. They all want to build online influence, get acknowledged and steer key political processes that go on every minute, at different layers of global interconnectedness. The information related to these processes no longer come solely from embassies, intelligence agencies, or conventional media corporations, but in platforms where such information is disseminated equally to everyone. While these information intermediaries are certainly not obsolete, they are also not as important as they used to be and will have to devise new capabilities and competencies in order not to end up irrelevant.

In August 2017, Facebook's A.I. negotiator project went sour as the chatbot started developing its own language that cannot be understood by outsiders and learned how to lie. This issue was a hotly debated topic at the Oxford Internet Institute when I was a visiting fellow there. A retired member of the British diplomatic service who was attending a meeting, upon hearing this news, calmly told me: 'Good. Machines have learned how to conduct diplomacy'.

In coming years, MFAs will have to adapt to computational diplomacy through a multitude of approaches:

- **Verification and Counter-Messaging:** Depending on financial and human resources, MFAs can employ a number of automation measures themselves. The primary use of automation will have to challenge and verify information flowing at enormous volumes during crises and emergencies. Such verification tools can also automatically get translated into multiple languages for the use of a country's embassies in foreign countries. Furthermore, MFAs can use automation to detect transient influence networks and misinformation sources in real-time, helping substantially with attribution and fact-checking.
- **Data/Sentiment Mining:** Real-time scanning of social media platforms through pre-determined set of word combinations may allow MFAs to mine opinion and sentiment, in issues related to foreign policy and political engagement. Whether a particular issue is de-

bated more within a certain age group, nationality or geographic area is an important policy variable for diplomatic missions. These engagement profiles usually vary between different policy agendas, so automated data mining is usually a better way of profiling engagement compared to snapshots.

- **Digital Content Creation:** Currently, several sports media companies are experimenting with automated content writing, that are growing more sophisticated in a way that will soon eclipse human-based reporting. Automated content curation is key for journalism and can also be adopted by MFAs in similar fashion for nation-branding, agenda-setting and awareness-building campaigns. When combined with data/sentiment mining, A.I.-based diplomacy efforts can also incorporate automated policy writing, which can communicate a pre-set policy preference across multiple language platforms.
- **Diaspora/Business Engagement:** Address, personal information, financial assets and investment data that belong to Diaspora groups abroad and business commitments all benefit from automation. Communication with both groups can be significantly streamlined through the use of chatbots that provide information on elections, registration, taxes or trade agreement terms to better mobilize and inform them with regard to both home country and host country requirements. Chatbots are also potentially lifesaving in natural disasters or other emergency situations to connect a large Diaspora group with necessary professional help.
- **Micro-negotiations:** Micro-negotiators - bots that run multiple rounds of negotiations based on vast sets of data - can be vital to multilateral negotiations and save significant time to reach agreements. When the issue that is negotiated is data-heavy (trade, infrastructure, financial and other numerical policy issues), micro-negotiators can do a far better and faster job than human negotiators. These micro-negotiators can either reach an agreement on their own, or assist senior negotiators in determining political aspects of a settlement. In multilateral and multinational summits, micro-negotiators can be even more valuable as sides can focus on more human-centric aspects of negotiations. For example, in discussing foreign aid sum and disaster relief, micro-negotiators can rapidly designate key aid areas through geospatial imagery analysis and real-time social media posts from the region, significantly easing and streamlining aid negotiations.



New power centers - in the form of technology companies and big data brokers - are changing the state-centric parameters of classical realism perhaps, but the inherent dynamics of power realignment still render diplomacy a crucial endeavor.



Automation doesn't change the fact that diplomats and embassies still matter. Foreign policy, like all politics, is a factor of human condition, including sense, gut feeling and cultural cues, along with its imperfections. However, there is a clear trajectory whereby states that can best adapt to automation - in war, foreign policy and economy - will develop more efficient ways of dealing with the challenges of an interconnected, data-centric world. Diplomacy too, can retain its relevance and influence over politics between nations, so long as it can properly designate areas where automation can help and where it can't. Although all states will come up

with their own answers to these questions, based on their own individual interests and needs, the common direction in which automation and foreign policy is headed is more or less similar for all countries. In the future, diplomacy has to build data processing and management capabilities, with dedicated departments and scientists supporting diplomats and negotiators on the ground. The structure of this new framework will also heavily depend on regime type, scope of foreign interests and alliance behavior.

The structural shadow of uncertainty over diplomacy is stronger than ever. Some communicative rituals and practices of diplomacy are growing more obsolete, as modern political communication slides increasingly to short and sharp rhetoric, coupled with automation tools that bombard audiences at unprecedented levels. Diplomacy itself is hardly obsolete however, as the task of mediating and negotiating power relations is perhaps as important as it was during the Cold War. New power centers - in the form of technology companies and big data brokers - are changing the state-centric parameters of classical realism perhaps, but the inherent dynamics of power realignment still render diplomacy a crucial endeavor. To rise to the challenge however, modern diplomacy has to develop a strong computational capacity, able to adapt to the changing nature of digital communication and advances in automation.



Cyber Governance and Digital Democracy 2017/3

November 2017

Computational Diplomacy

H. Akin Ünver, Kadir Has University & EDAM