Working Paper
For circulation at the 2017 Global Digital Futures Forum
May 5, 2017

COLUMBIA|SIPA
School of International and Public Affairs

Panel Discussion:

Cyber Conflict and Democratic Institutions

By Sean Kanuck

1. Introduction

This year's Global Digital Futures Policy Forum focuses on the tension between fragmentation of the Internet and globalization. While fragmentation, splintering, or "Balkanization" of the Internet has been a prominent topic of discussion for several years now, globalization has recently received a resurgence of attention in popular debate[i]. Globalization – long revered as a teleological objective of the Western liberal order – is increasingly being questioned by electorates in North America and Europe. Rising nationalist tendencies among certain political parties and candidates seek to re-assert domestic advantage and the self-interest of their constituents as their primary political goals. That trend, coupled with the legal debates about privacy and data localization in multiple jurisdictions, has reinvigorated interest in studying fragmented futures for the Internet.

This Panel will address cyber conflict as it pertains to the manipulation and/or compromise of democratic institutions – both directly and indirectly. Direct intervention in a democratic election could comprise either public efforts to personally obstruct voters or else clandestine alteration of actual vote tabulations; indirect intervention could consist of using proxy voices or inducing political, economic, or media events with secondary impacts on voter turnout and election results. Manipulative actions that do not directly alter the voting process or results are to be considered "influence operations", while actual changes to registered voters (including threats of violence or other means to physically deter eligible voters from attending the polls) or the ballots that are cast are typically deemed illegal "voter fraud", even when perpetrated by the state apparatus itself. (Figure 1 below reflects the fact that both direct intervention and indirect influence in democratic elections can be either overt or covert.)

Information communication technologies (ICT) present many new vectors for potentially interfering with democratic institutions. Foreign competitors, traditionally offset by geography, can now impose themselves on domestic political systems anywhere in the world. Social media platforms enable

individuals or special interest groups to broadcast their policy positions at little or no cost and even to strategically misrepresent broader support for those positions. Internet-connected ICT networks are highly susceptible to unauthorized access, thereby rendering sensitive data vulnerable to theft and public release. In essence, the digital future – and liberal democratic processes that will rely upon it – is susceptible to interference and disruption. This Panel will consider ways to safeguard democracies and the international order from corruptive influences (or at least to minimize their impacts) in the future.

Figure 1: Examples of Methodologies for Manipulation of Democratic Elections

	DIRECT INTERVENTION	**INDIRECT INFLUENCE**
OVERT	Intimidating or deliberately misinforming voters in order to deter turn out. For example, unofficial "robocalls" used during the 2011 Canadian federal election to falsely claim changes to polling station locations.[ii]	Public campaign donations and/or speeches by non-candidates in support of specific ballot choices. For example, President Obama's 2016 speech in London opposing "Brexit" before that referendum.[iii]
COVERT	Secretly altering the election results in order to favor a specific candidate. For example, the historical allegations regarding Lucien Bonaparte's inflation of voting results in the French constitutional plebiscite of 1800.[iv]	Clandestine, third-party activity intended to increase or decrease support for specific candidates. For example, reputed Russian espionage and publicization of materials during the 2016 U.S. presidential campaign.[v]

2. Historical Precedent

When evaluating the impact of cyber modalities (i.e. ICT) on democratic institutions, one must first consider what is genuinely new in either the objectives or possible impacts. Regardless of which quadrant of Figure 1 is of concern, there is ample historical precedent from geo-politics. Thucydides recounted Athenian efforts to lobby the magistrates of Melos to capitulate without battle (i.e. indirect and overt influence). Similarly, Radio Free Europe and Voice of America were designed to provide the electorates of foreign polities with information that was otherwise unavailable and/or forbidden. Nor is history want for allegations of ballot-box stuffing (i.e. direct and covert intervention) or voter intimidation (i.e. direct and overt intervention). Digital manifestations of those forms of fraud are certainly illegal and deserving of policy attention, but they are not the focus of recent debate. What seems to capture the current imagination – and concern – is the heightened opportunity for indirect, covert influence through

cyber means. Careful analysis is required, however, to properly assess the nature and foundation of that concern.

Framing Question 1: What is so new and inherently objectionable about digital influence campaigns?

If one reasonably acknowledges that foreign efforts to influence elections are as old as elections themselves, then one is left with either (i) a theoretical objection that is so counterfactual to historical practice that it is relegated to pure academic consideration, or (ii) a practical objection that employing a new technological means to an old political end is somehow unacceptable. It is worth recalling that public international law does not outlaw espionage – which is merely accepted as a feature of international relations. Nor is the publication and dissemination of political opinions generally deemed objectionable in liberal democracies. So what is really at issue here?

By way of example, several former U.S. intelligence officials have stated that they considered the theft of Office of Personnel Management records to be a "legitimate" foreign intelligence target.[vi] But even so, U.S. government officials have said that the scale and import of that espionage crossed a line that was unacceptable. So, it would seem that the objection stems from the quantitative scope of the activity in question (i.e. the sheer number of records compromised, the gross imbalance between the cost of conducting the activity versus its harm to the victim, the possible stand-off distance from which such an operation can be conducted without personal risk, etc.), rather than the qualitative nature of the activity itself (i.e. the theft of private information, the type of data targeted, etc.). Chivalric objections to the crossbow and guerilla warfare tactics should immediately come to mind, for new methods of conflict are often too efficacious for the establishment to accept at first outset.

Framing Question 2: When does a quantitative improvement in espionage constitute an unacceptable qualitative change? Do recent offensive cyber advances constitute a qualitative threat to democracy?

<u>Protected Infrastructure</u>

The U.S. Department of Homeland Security did not officially designate election systems as a critical infrastructure until January 2017.[vii] Yet, almost four years earlier in March 2013, the U.S. Director of National Intelligence (DNI) had identified an important incongruity related to how different nation states view online media and their political systems:

> *"Online information control is a key issue among the United States and other actors. However, some countries, including Russia, China, and Iran, focus on 'cyber influence' and the risk that Internet content might contribute to political instability and regime change. The United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems. This is a fundamental difference in how we define cyber threats."*[viii]

That fundamental difference (i.e. the underlying distinction between infrastructure and content) is also germane to the question of which ICT deserve protection as "democratic institutions". Most everyone would likely agree that public authorities must guaranty the security of polling stations, voting machines, and official election returns. In other words, they are expected to prevent direct intervention that is contrary to the rule of law. This is represented by the United States' "infrastructure-centric" view of cyber security that was highlighted by the DNI. Content poses a much more complicated challenge.

Framing Question 3: Is the national government responsible for ensuring the confidentiality, availability, and integrity of all media resources that can influence a democratic electorate? Why not?

The discussion about where to draw the line regarding indirect influence quickly becomes muddied, as we regularly see with proposals for campaign finance reform. Managing the impact of informational content pits two democratic values against one another, namely freedom and equality. How much leverage should freedom of expression permit wealthy individuals and companies to exert on democratic processes? Is every mass media outlet or social media platform to receive a critical infrastructure designation because they can be utilized to influence public opinion? Which entities are "entitled" to special protections and/or restrictions? Each of those questions is a public policy dilemma.

Figure 2: Examples of Civilian Infrastructures that Impact Democratic Elections

	VOTING SYSTEMS	INFORMATION RESOURCES

PUBLIC	Government administered polling stations and officially monitored vote tabulation. Susceptible to corruption by ruling party.	National television, radio, print, and online media outlets. Subject to selective coverage and preferential treatment by ruling party.
PRIVATE	Hardware and software for voting systems and registration databases developed by commercial companies. Susceptible to supply chain and/or remote penetrations.	Independent mass media and online social media platforms. Subject to censorship by government as well as disruption and/or manipulation by third parties.

The status of political parties and their proprietary resources also raises very difficult legal and policy questions. If the compromise of an entity like the Democratic National Committee or the Republican National Committee in the United States is deemed a national security concern, then what level of governmental oversight and regulation of (i.e. access to) that party's ICT networks is appropriate in the national interest? Does that level change depending on whether that party is currently in power? Should smaller political parties be exempt from such regulation if they are not likely targets for foreign intervention? Once again, these cyber challenges are pitting core democratic values against one another (e.g. privacy versus national security) and policy trade-offs are inevitable.

Framing Question 4: Can private data be treated as a national asset against the will of its owner?

Social media represents a uniquely influential and vulnerable feature of modern politics. Its impact during the Arab Spring was noted by governments and demonstrators alike around the world. Since then, the use and manipulation (e.g. "astroturfing" to generate the semblance of broader support) of social media has become an instrumental part of political campaigns, opposition movements, and foreign influence operations. It is possible, at least to a certain degree, to reveal such social media manipulation (e.g. by technically determining the provenance of posted information, detecting automated programs for "re-tweeting" and "liking" posted information, and identifying patterns of coordinated "trolling"), but that requires analysis of large tranches of proprietary data, including both content and technical meta-data. In democratic societies, private ICT companies have no *ex ante* obligation to make their databases available to government authorities for speculative research.

Figure 3: Examples of Information Propagation to Induce Political or Economic Behavior

	INTENTIONAL MESSAGING	UNWITTING EXPLOITATION
INFORM	The 2007 airborne delivery of leaflets over Afghanistan by the U.S. military in order to deter insurgent activity by the Taliban.[ix]	In 2016, Twitter suspended thousands of suspected terrorist accounts that promoted violence and/or spread propaganda.[x]
DECEIVE	Adoption of the title "Bolshevik" (i.e. "one of the majority") by a party faction that was numerically inferior.[xi] The ironic naming of "Greenland" by Erik the Red to encourage emigration to a new colony that was less temperate.[xii]	The Syrian Electronic Army's false "tweet" disseminated from the Associated Press's Twitter account, which led to temporary fluctuations in U.S. stock markets in 2013.[xiii] False news items posted on Facebook during the 2016 U.S. presidential campaign.[xiv]

Data Integrity

As Figure 3 illustrates, many forms of media have been used to spread both information and disinformation for political effect. History is certainly replete with examples of interest groups "marketing" their views to the public – such as the U.S. founding fathers' ascription of the moniker "Anti-Federalists" to their opponents in order to impute a negative connotation – but social media platforms present a new challenge whereby they host content that is neither of their own creation nor necessarily attributable to physically identifiable third-parties. Accordingly, they become enablers for all sorts of online activities that can foster or undermine democratic institutions. That schizophrenia is perhaps best characterized by the hacker consortium Anonymous, which has both thwarted sovereign governments and also publicized child pornographers and corporate fraud.[xv]

Framing Question 5: Is the "common carrier" model the right legal analogy for social media outlets?

All of the themes aforementioned in this paper (e.g. espionage, influence operations, quantitative change, qualitative distinctions, public versus private infrastructure, freedom of expression, national security, etc.) coalesce around the key issue of data integrity. Because democracies rely on the ability of their populaces to make informed decisions, increased dependence on insecure ICT poses considerable threats. How can the public ever differentiate truth from falsehood with certainty?

In fact, international humanitarian law (aka the law or armed conflict) struggles with a similar conundrum when it distinguishes between perfidy (i.e. the illegal intent to betray confidence) and ruses

of war (i.e. permissible deceptions not based on garnering false status).[xvi] Interestingly, though, "misinformation" is listed as a ruse vice perfidy; moreover, the relevant treaty distinctions explicitly do not "affect the existing generally recognized rules of international law applicable to espionage."[xvii] Thus, cyber operations premised on exerting indirect influence are particularly problematic – especially when they only reveal true information.

Framing Question 6: Can two "rights" make a "wrong" … that is, should espionage (which is accepted in international relations) that exposes the truth (a core democratic value) be prohibited?

Ultimately, the most nefarious threat to democratic institutions is the corruption of the integrity of information. The pervasive introduction of false data into mainstream media could erode public confidence and destabilize society. That is, of course, exactly what authoritarian regimes are (i) highly concerned about happening to themselves, and (ii) well-practiced in perpetrating against their adversaries. Yet, democracies pride themselves on permitting their citizens to hold and publicize contrarian (or even counterfactual) opinions, and modern ICT permit foreign voices to participate in domestic dialogues.

It seems then that the most conceptually disturbing challenge for democratic institutions regards digital, highly efficient, indirect, foreign, misinformation campaigns that can neither be prevented nor easily identified. Furthermore, it is unclear what kind of governmental institutions (domestic or international) and/or private sector initiatives could resolve that difficulty, for this seemingly new cyber concern tautologically reduces to the well-known game theory paradox of "who guards the guardians"?

---

i See http://www.atlanticcouncil.org/images/files/publication_pdfs/403/121311_ACUS_FiveCyberFutures.pdf ; See generally, David Kennedy, A WORLD OF STRUGGLE: HOW POWER, LAW, AND EXPERTISE SHAPE GLOBAL POLITICAL ECONOMY, Princeton University Press (2016).

ii See http://news.nationalpost.com/news/canada/canadian-politics/electoral-fraud-did-take-place-in-2011- federal-vote-but-it-didnt-affect-outcome-judge-rules

iii See https://www.theguardian.com/politics/2016/apr/22/barack-obama-brexit-uk-back-of-queue-for-trade-talks

iv See e.g., https://en.wikipedia.org/wiki/French_constitutional_referendum,_1800

v See https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

vi See http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/opm-attack-hack-china- cybersecurity-personal-data-suspect-espionage-verifiable-/29341789/; See https://www.the-american- interest.com/2015/06/16/former-cia-head-opm-hack-was-honorable-espionage-work/

vii See https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure- critical

viii James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, March 12, 2013

ix See http://www.af.mil/News/Article-Display/Article/127729/operation-achilles-leaflet-airdrop-delivers-message- to-taliban/

x See https://www.wired.com/2016/08/twitter-says-suspended-360000-suspected-terrorist-accounts-year/

xi See https://www.britannica.com/topic/Bolshevik; See http://www.historytoday.com/richard-cavendish/bolshevik-menshevik-split

xii See http://news.nationalgeographic.com/2016/06/iceland-greenland-name-swap/; See also, https://www.scientificamerican.com/article/proof-on-ice-southern-greenland-green-earth-warmer/

xiii See https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that- tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.f575e36dfcd2

xiv See http://www.reuters.com/article/us-usa-election-facebook-idUSKBN1380TH

xv See https://sg.finance.yahoo.com/news/Anonymous-exposes-visitors-afpsg-2809071407.html; See http://asia.nikkei.com/Business/Trends/Hackers-turn-stock-advisers-as-Anonymous-targets-China-Inc?page=1

xvi See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (hereinafter Protocol 1), Article 37, June 8, 1977; See also, Protocol 1, Article 39

xvii Protocol 1, Article 39(3); See Protocol 1, Article 37(2)