Renewing our Democratic Alliance

Executive Summary: Panel 4 - Democracy and Cyberspace

Chair: Sue Gardner (formerly of Wikimedia)

Paper Authors: 1) Aaron Shull, JD, & Kailee Hilt, MA (Centre for International Governance Innovation) 2) Dr. Ulrike Klinger, PhD (European New School)

The fourth panel of German and Canadian experts, July 5, on global cyber-security and the impacts on democracy of communications technologies, was chaired by Sue Gardner.

There were two issue papers prepared, reflecting the two basic topics: Aaron Schull and Kailie Hilt of CIGI on "Securing Cyberspace in an Age of Disruption," and Ulrike Klinger of the European New School and Weizenbaum Institute, on "Digital Democracy and Public Discourse: dissonant, disrupted and unedited?"

Co-Chairs of the RODA project, Ben Rowswell President of the Canadian International Council, and Norbert Eschborn, Director in Canada of the Konrad Adenauer Stiftung, welcomed participants. They sketched out the purposes and program of the overall Canada-Germany like-minded project, emphasizing the aim to a) provide the two governments with expert advice on critical issues affecting democracy and human rights support and international cooperation, and b) strengthen research and scholarly networks between Canadian and German civil societies and centres of excellence.

German Ambassador to Canada, Sabine Sparwasser, underlined the immediacy and importance of the issues before the panel, recalling Japanese technology entrepreneur Masayoshi Son's dictum that "those who rule the data will rule the world." Indeed, the world is at an inflection point on issues of cyber security and democratic health, without the infrastructure of socially responsible international governance for cybertechnologies affecting so many lives.

Canadian Ambassador to Germany, Stephane Dion, reminded the panel that freedom of expression is precious, fragile, and needs protection.

Chair and moderator Sue Gardner set the context for the discussion by reflecting on her personal journey from internet optimist to "horrified pessimist" during the 12 years in which she lived and worked in the San Francisco Bay Area at the epicentre of tech. She recalled the internet's origins among "dreamers, visionaries and idealists," in the period in which it was felt the advent of the internet would usher in a new era of knowledge-sharing and communication across borders, and traced tech’s evolution through the entrepreneurial startup era and into the consolidation phase of Big Tech, in which a small number of powerful near-monopolies now dominate the tech landscape.

She summarized for panelists the ways in which tech is now harming democracy: by providing tools used by authoritarian governments to surveil and control their citizens; by accidentally breaking the business model of the journalism industry, leaving people less well-informed and power less accountable; by social media's algorithmic amplification of misinformation and disinformation, which empowers demagogues and extremists, and leaves everybody else confused and distrustful; and by refusing to moderate

discussion spaces and thereby enabling the harassment and abuse of people with marginalized identities, silencing them and pushing them out of public discourse. She described governments' response to these harms as mostly "hanging back, unsure," but praised Germany as a global leader in terms of taking steps to require tech platforms to modify their practices to bring them in line with the values of the people of Germany.

As moderator she set for the panel the central task of proposing structures which could deliver more positive outcomes for society, underlining the real need for countries to work together - which became a leitmotiv of discussion.

An introductory tour de table of panelists to identify forefront preoccupations elicited several points that were subsequently expanded by the panel, among which:

- Infrastructure for governance of communications technologies and cyber is inadequate, barely existent
- There is little connection of privately owned platforms to public values and beneficial norms
- The world is unprepared and under-equipped to cope with the explosion of hugely disruptive cyber-crime
- The trajectory from total optimism to total pessimism has been enabled by too much focus on technology and too little on society and on human agency
- Technology companies' practices are completely opaque, which makes it difficult to study or analyze their societal effects
- Much more research, digital media education, and cross-border work among scholars and governments is essential

Aaron Schull and Kailee Hilt introduced their paper which focused primarily on the cyber-security challenges, and on the need of international governance of cyber and social media platforms.

It is a clearly dangerous time. We are living unprepared and barely protected in a grey zone in which preparation of cyber war goes on at a time of ostensible peace, without universally accepted rules.

Cyber-crime, notably the expanding practice of ransomware, is rampant, without agreed measures for determining responsibility and appropriate responses.

State-to-state preparation for offensive cyber-weapons of disruption and coercion is conducted in great secrecy. The publics of potentially targeted countries are unprepared, their increasing vulnerability enhanced by rapidly expanding inter-connections of the Internet of things.

Middle powers like Germany and Canada should join up to promote the development of governance infrastructure and acceptance of rules of the road.

On governance, policy elaboration must be inclusive of public input. The issues are not just those of national security but bear heavily on normative social values.

Subsequent discussion agreed there is a paucity of laws and constraints on Big Tech; as Sue Gardner had put it, some CEOs operate abroad to conform to contradictory national legal regimes, while others conform to nobody's at all.

Germany's efforts to strengthen cyber-security laws, most recently in 2017, are upgrades to governmental practice, and extend across the board: Germany did not rule out Huawei 5-G networks because they represented a unique geo-strategic threat, but strengthened security requirements for all potential entrants.

Cyber-security legislation succeeds a long history of German preoccupation with disinformation, the other main topic before the panel: German hate laws are severe and have been reinforced by more recent laws against the monetization of harmful information content. The European Union has drawn up a Democracy Action Plan to provide essential context, including for expanded research, consumer protection, and defensive citizen education.

The question was asked whether German legislation, while welcome, can really do much to improve the unacceptable current imbalance in power relationships between the "1% who control platforms and the 99% who are their users" and rectify serious underlying problems, which include:

- Inconsistency between the language of security and technology with norms of democracy
- A lack of corporate and platform transparency, exacerbated by the impenetrability of algorithms, shrouded in secrecy, designed to maximize profits, and not amenable to policing.

Middle countries should indeed consult and act jointly to obtain leverage with Facebook, for example, buoyed by its $1 trillion valuation, to counter its "complete untransparency."

However, several intervenors underlined that international cooperation on all the issues of cybergovernance, transparency, and social responsibility, has a very long way to go. President Macron had urged international coherence of effort but China, Russia, and the US were unsupportive. It has to be realistically acknowledged that these major countries are preparing their capabilities for inserting malware strategically, breaching the national security of potential adversaries. Cyber-espionage is routine.

It was observed that Canada doesn't seem to be sure where its interests lie, in security alliances or in supporting complete transparency and rules-based governance. The apparent fact is that Canada and Germany are like-minded while the US is an outlier, and the proposition of an alliance of democratic countries needs deeper definitional understanding.

Dr. Ulrike Klinger then presented her paper on social media and disinformation.

A baseline fact is that social media are not an exogenous factor to the challenges; they "are" society. But they are built-for-purpose for profit, not to promote rational discourse.

They have become central to political communication but political users target for effect old media as vehicles as well as new, in a hybrid fashion; e.g., Donald Trump's provocative use of Twitter to obtain more mainstream media coverage - a "new door to an old house."

We do focus too much on the technology itself, rather than its effects. But she urged recognition that:

- We can control technologies to attenuate negative collateral effects - i.e., they are not immutable
- But we need to understand the technologies and their effects.

The key question is how we can ensure public values, and rights, are kept in the forefront. We should not "blame" the technology, which is neither "good" nor "bad," but instead shore up human agency as the driving factor - to take control.

It is up to society to force change in platform behaviour. Their lack of transparency is a fundamental obstacle to mediation.

It should not be up to the platforms to self-police. They need incentives to change, that should be shaped for public policy from users whose data constitute the algorithms that represent the platforms' monetized assets.

Discussion concurred that civil society must be central to the writing of the rules. Generally, publics are too passive, aroused more by publicized complaints about specific objectionable commentary on social media than by the need for structural improvement of governance and transparency. It is pointless to leave to politicians the responsibility for rectifying the effect of specific harmful comments.

As we record the harmful incidents and effects of deliberate disinformation, empirical observations have to be aggregated and translated into action recommendations to deter the harm.

Several speakers emphasized again the importance of collaboration in research and determination to prepare an educated public, able to discriminate facts from fiction, which begins with children.

It was pointed out the European Commission and Union is driving relevant rule-making in the world community. But the overall task of providing for governance will consume the next decade, before priorities of public good prevail in practice.

Moderator and Chair Sue Gardner, in closing, polled panelists on their self-identification as optimists or pessimists at this stage of the evolving set of issues: their inclination is pessimistic but with some room for hope.

The Chair saw hope as being justified if serious trans-national cooperation becomes a reality.

It was clear from discussion that the need of governance infrastructure, whether for cyber security, or for social networks, is overriding.

Greater public and user competency in on-line media is essential to progress and redress in governance and to consumer and citizen protection.

But we can't regulate what we don't understand, and the necessity of seeing behind the industrial "curtain" is essential.

Ben Rowswell closed the meeting by urging participants to stay connected, including to further webinars of the RODA Canada-Germany like-minded colloquium on issues of multilateral cooperation and human rights and democracy protection.

Summary prepared by Sue Gardner.