Forum: United Nations Commission On Science and Technology for Development

Issue #11-02 : Measures to address international, technology-aided threats to governments and organizations

Student Officer: Abel Resende and Daniel Igualada

Written by: Juan Estevez, Abel Resende, Daniel Igualada, Onat Ergin

---

Introduction

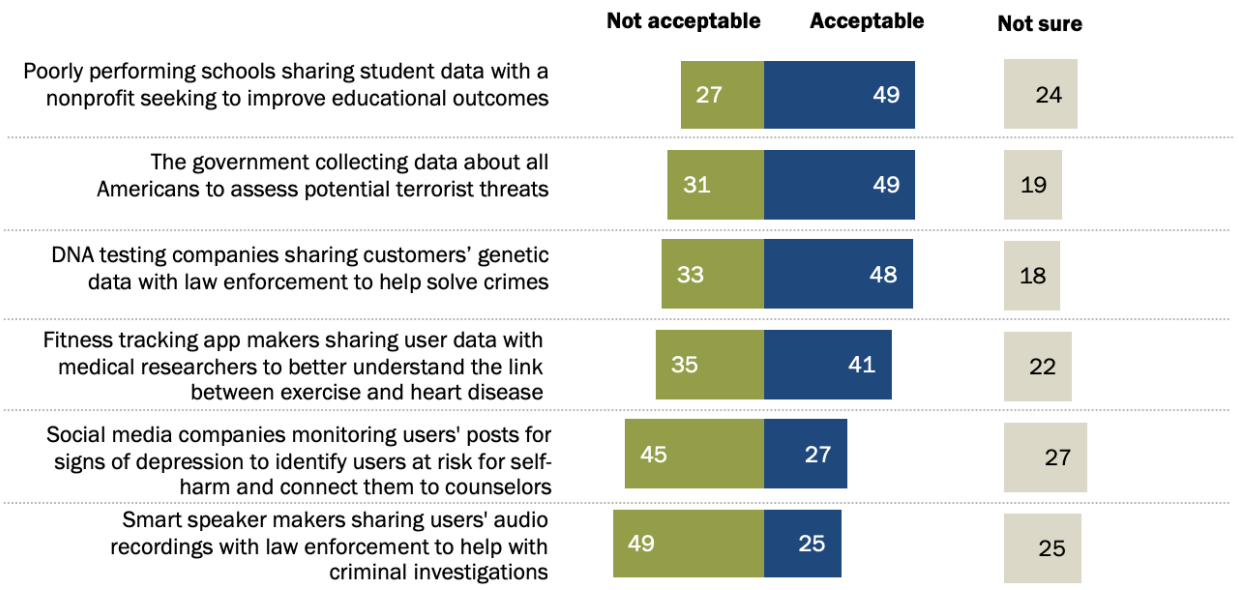
Technology has become the present but most importantly the future of our society and civilization. It is incredible to see and experience the major advances in technology that are being made in ranges of fields such as Information Communications Technology (ICT), Artificial Intelligence (AI), robotics, nanotechnology, space technology, biotechnology and quantum computing to name a few sectors where technology is thriving and growing rapidly. This technological revolution has organizations and governments all around the world on alert because with great power comes great responsibility. These new technologies bring progress and alternative solutions to modern day problems but they also pose threats to society and the world as we know it.

The technological advancements in question are the results of a more than four decade long digital revolution. These breakthroughs are concentrated on the collection, processing and analysis of massive amounts of data generated by the information sciences, having consequences for a wide range of research and development fields. Although these advancements promise considerable social and economic benefits, as well as increased efficiency and productivity in a variety of industries, it is impossible not to be concerned about the possible

threats all this might bring.

There is a growing fear that these technologies, and how they are being employed, could inflict severe issues such as labor force dislocations, market disruptions, important things like exacerbated inequalities and new threats to public safety and national security. These technologies are called dual use as they may be used to help society and can be used to serve malicious purposes along with lethal purposes because they may be used to boost social and economic growth, making management considerably more difficult. Most of them are naturally vulnerable to exploitation and disruption from both near and far since they are very easy to access and utilize.

% of U.S. adults who say the following uses of data or personal information are ...



Note: Those who did not give an answer are not shown.
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

Definition of Key Terms

Media Manipulation

Use of suppressing evidence, cherry picking, logical fallacies, psychological manipulations, outright deception in order to favor specific interests.

Cyber-security

The protection of computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions

Cyber-attack

An attack aimed at interrupting, disabling, damaging, or maliciously managing a computing environment/infrastructure; or destroying the integrity of data or stealing controlled information.

Informational Technology

The use of computers to store or retrieve data and information.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Cyber Intelligence

According to the United States Department of Defense, cyber intelligence is defined as "Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions."

General Overview

As technology and its usage in societies around the world is growing at a faster rate than ever, security concerns regarding this global issue have also severely increased. One of the most recent and perhaps most important concerns surrounds the topic of how technology can be weaponized and cause serious harm and destruction to governments and organizations. Since the majority of governments and organization's vital infrastructure is technologically based, this makes them more susceptible to attacks. Data breaches leaking national and personal information are becoming much more frequent and at larger scales. For example, in January 2021, following the discovery of four 'zero-day' in the Microsoft Exchange Servers, hackers gained full access to user emails and passwords on affected servers, administrator privileges on the server, and access to connected devices on the same network. In total, roughly 250,000 fell victim to the attack, including the European Banking Authority and tens of thousands of more organizations.

These attacks, however, are not just limited to data breaches. The year 2016 saw one of the most prominent string of cyber attacks in history in relation to the 2016 United States Presidential Election. The Mueller report features many instances of russian based hackers attempting to manipulate the election in a variety of ways. According to this report, the Russian hackers managed to access some states' voter registration systems and stole hundreds of thousands of voters' personal information including names, addresses, Social Security numbers, dates of birth and driver's license numbers. Moreover, the hackers infiltrated a voter registration software vendor, and pretended to be the company as they sent out malicious emails to several Florida election administrators. According to the Senate Intelligence Committee's report, in

some states, Russians "were able to gain access to restricted elements of election infrastructure" and "alter or delete voter registration data."

Although technology has revolutionized society in countless ways and plays a major factor in everyday life, the danger posed by people or groups weaponizing these technologies cannot go unnoticed. Whether it be a national government, a giant multinational company, or even a single person; everyone is at risk to these technological attacks.

Major Parties Involved and Their Views

European Union

In 2017, the European Union announced a new strategy to combat misinformation and fake news online. During the first of a two-day conference in Brussels, the E.U. announced the launch of a public consultation service and the creation of a high-level expert group to help the E.U. develop a strategy to stop the spread of fake news. The expert group will include academics, platforms, journalists and civil society organizations that can advise the commission on the scope of misinformation and how to create recommendations based on stakeholders' priorities.

United States

In order to ensure the future of democratic governance worldwide, the U.S. government is aiming to take proactive steps to regulate social media and prevent foreign election interference efforts. The American government suffered domestic and foreign election influence through the use of "fake news," as well as methods of social media manipulation. A report from the Office of the Director of National Intelligence from the U.S. government states that during the

2016 U.S. presidential election, the Russian government ordered the leaking of political material and massive propaganda via social media. Moreover, the reports published by the American government state that Russian actors hacked into U.S. political leaders' email servers and leaked their content via the websites WikiLeaks and DCLeaks. Moreover, the United States Department of Justice published that the Russian government launched a massive propaganda campaign through the Petersburg-based Internet Research Agency (IRA). According to reports from tech conglomerates, the campaign reached at least 126 million U.S. citizens on Facebook, 20 million on Instagram, and 1.4 million on Twitter.

Canada

The government of Canada has recognized the crucial importance of its democracy from cyber threats. In April 2018, the federal administration of Canada launched the Defending Democracy Program as part of the ongoing work to protect customers and promote cyber diplomacy around the world. To address these threats and scale the program globally, officials have been working with many governments, industry, and civil society stakeholders. To help defend against disinformation campaigns, the government has joined with NewsGuard Technologies to enhance digital media literacy and confront misinformation in the online space. Alongside Oxford University's Internet Institute, the government aims to shed light on computational propaganda targeting elections in democratic countries around the world.

France

France has seen first-hand the impact of disinformation campaigns by adversaries, and this type of malicious activity continues. Over the past years, the French government has started to highly regulate fake news and political advertising. For instance, the publication of fabricated information falsely

attributed to a third party is illegal under French defamation laws. Furthermore, paid political advertising in newspapers, radio, television, or online is illegal for at least six months before an election. Additionally, there is a "period of silence" on election day and the day before, during which all campaigning must stop. A new law was adopted in December 2018 that imposes transparency requirements for online advertising and creates a new legal weapon for combating the dissemination of fake news during an election period.

Australia

The national government of Australia has recognized the proliferation of fake news and threats to national security through technology and social media. In June of 2019, the government launched a new research center at Flinders University to combat digital media manipulation in fostering divisions in civil society, maintaining national security, and defending democratic governance. The Jeff Bleich Centre (J.B.C.) for the U.S. Alliance in Digital Technology, Security, and Governance is the first research center in Australia to adopt a multidisciplinary approach by bringing technology, security, governance. The J.B.C. will undertake research in areas of mutual concern to Australia and the United States to improve the capacity of governments and industry to respond to cyber challenges and threats.

Timeline of Events

Date	Description of event
June 2016	In the referendum held for the U.K. Brexit, the majority of the voters chose to leave the European Union.
November 2017	The 2016 United States presidential elections were held.

November 2017	European Commission organized a two-day conference in Brussels to develop a strategy to stop the spread of fake news alongside a high-level expert group.
April 2018	The government of Canada launched the Defending Democracy Program.
November 2018	President of the French Republic, Emmanuel Macron, sent the Paris Call for Trust and Security in Cyberspace, which aimed to face threats endangering citizens and instructure through technology.
December 2018	French government imposes transparency requirements for online advertising and creates a new legal weapon for combating the dissemination of fake news during an election period.

UN involvement, Relevant Resolutions, Treaties and Events

The UNCSTD recognizes the many risks these new technologies posses and have come together with many world leaders and countries to settle regulations and organize dialogues regarding this concern.

- On May 28th of 2018, The United Nations Secretary General's Assembly adopted the "Strategy on new technologies" goals**.** They adopted and created various goals and achievements to follow the Sustainment Development goals and the guidelines of the UN charter.
- On May 9th 2019 the UNCTAD held the 22nd annual session of the United Nations Commission on Science and Technology for Development (CSTD) at the Palais des Nations. They talked about the importance of noticing how

technology can help accomplish the sustainable goals by 2030. In addition to this, they also recognized the possible threats which technology may impose, but emphasized that it is the future and as long as it is regulated by guidelines it must not be stopped.

- In 2021 the UN published a report and a new program called Technology and Innovation drafted by the UNCTAD. This report urges all nations to get ready for the social, economic and revolutionary change technology will bring in this new decade. And to watch out closely any possible threats to privacy and global/national security with new technologies such as AI

Past action

With the development of informational technologies, it's more dangerous for companies and governments as they may be exposed to more cyberthreats. Under the United Nations Office on Drugs and Crime, a programme named "Global Programme on Cybercrime" was established after the General Assembly Resolution 65/230 and resolutions 22/8 and 22/7 passed by
the Commission on Crime Prevention and Criminal Justice. This program assists Member States in combating cybercrime by providing technical assistance and enhancing their cybersecurity infrastructure. MEDC countries, including but not limited to the United States and the United Kingdom, are directly funding this program. LEDCs in Central America, MENA, Eastern Africa, Southeast Asia, and the Pacific were the program's target regions. The program has a number of high minded objectives, including combating cybercrime holistically, strengthening national and international ties between governments, the private sector, and law enforcement, establishing national cybersecurity coordination centers and enacting legislation on the subject, and establishing a strong human rights network to combat cybersex trafficking.

Another step taken by the UN Office on Drugs and Crime was the formation of an Intergovernmental Expert Panel. The purpose of this team, which was formed in response to a request in General Assembly Resolution 65/230, is to do research on cybercrime, how different countries and companies combat cybercrime, how much international cooperation is going on this subject, and relevant laws. Moreover, United Nations also established an ad-hoc committee about cybersecurity by the United Nations General Assembly Resolution 74/247. This committee will be made up of experts from the Intergovernmental Expert Team but also representatives from each region. This group is significant because it will bring scientists and diplomats together.

Possible Solutions

As the issue of cyber attacks has become more prominent in recent years, the measures taken by entities around the world have also become more vigorous and more frequent. Luckily advanced endpoint protection has been developed which enables systems to be shielded from attacks by layers of automated protection. Although this solution has made it more difficult for attackers to infiltrate and disrupt systems, it does not completely prevent it. Furthermore, this type of solution requires constant updating as hackers continue to find new ways to exploit vulnerabilities and bypass these systems.

In regards to other technological solutions, artificial intelligence has become a plausible option. This idea is shrouded by controversy however, since the exploitation and manipulation of A.I. to cause damage and commit crimes has become more frequent. Government bodies and organizations must take into consideration the possible risks that come with relying on A.I. . Even with this, A.I. provides protection through analysis and threat identification that can be acted upon by cybersecurity experts to reduce breach risk and improve overall

security. Moreover, A.I. can instantly identify and prioritize risk and detect intrusions before they start.

It is still vital that whichever route is taken to prevent or be protected from cyber threats remains ethical. Possible solutions could involve governments invoking strict technological regulations upon their nations and increasing the severity of punishment for technologically based attacks. Although this could lessen the frequency of large scale attacks, it might come into question whether the actions by the governments are morally justified.

Sustainable Development Goal (SDG)

As we enter a new decade, defending democracy requires a focus on digital tech. Technology has affected the foundation of democracy negatively, and many citizens have lost faith and trust in national governments. The past decade saw nation-states weaponize technology and launch cyber-attacks against the civilian infrastructure of our societies. This included the foreign interference in the U.S. national elections in 2016, followed by the WannaCry and Not-Petya attacks in 2017, which unleashed damage around the world in ways that were unimaginable when the 2010s decade began. European political processes such as the withdrawal of the United Kingdom from the European Union, and the French presidential election in 2017, were impacted by disinformation campaigns, both internally and externally. With **Sustainable Development Goal 16: Peace, justice and strong institutions**, a global effort is underway to implement new measures to defend democracy and build new hope for the upcoming era. The United Nations aims to "promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels."

Appendix

I. Data Protection and Privacy Legislation Worldwide by the UNCTAD

https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

II. List of cyberwarfare incidents: Significant Cyber Incidents | Center for Strategic and International Studies

III. A report by Stockholm International Peace Research Institute: TECHNOLOGY AND SECURITY IN THE 21st CENTURY

Bibliography

Funke, Daniel. "The EU Is Asking for Help in Its Fight against Fake News." *Poynter*, 13 Nov. 2017, www.poynter.org/fact-checking/2017/the-eu-is-asking-for-help-in-its-fight-against-fake-news

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. OFFICE of the DIRECTOR of NATIONAL INTELLIGENCE, 6 Jan. 2017, www.dni.gov/files/documents/ICA_2017_01.pdf.

Chakrabarti, Samidh. *Hard Questions: What Effect Does Social Media Have on Democracy?* Facebook, 22 Jan. 2018, www.about.fb.com/news/2018/01/effect-social-media-democracy

DiResta, Renee, et al. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge, 17 Dec. 2018, disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf

Update on Twitter's Review of the 2016 US Election. Twitter, 31 Jan. 2018, blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.

Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System. The United States Department of Justice, 16 Feb. 2018, www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

West, Leah. *Defending Democracy from Foreign Cyber Interference: The Role of Canadian Intelligence Agencies in the 2019 Federal Election*. SSRN, 1 Apr. 2021, papers.ssrn.com/sol3/papers.cfm?abstract_id=3815735

University, Flinders. *Defending Democracy From Cyber Warfare*. Newswise, 26 June 2019, www.newswise.com/politics/defending-democracy-from-cyber-warfare.

"Democracy & the SDGs." *Sustainable Development Knowledge Platform*, United Nations, 8 July 2019, sustainabledevelopment.un.org/index.php?page=view&type=20000&nr=5780&menu=2993

Abrams, Abigail. "Here's What We Know so Far About RUSSIA'S 2016 Meddling." *Time*, Time, 18 Apr. 2019, www.time.com/5565991/russia-influence-2016-election/.

Gesley, Jenny, et al. "Regulation of Artificial Intelligence in Selected Jurisdictions." *DigitalCommons@University of Nebraska - Lincoln*, 2019, www.digitalcommons.unl.edu/scholcom/177/.

Hazlegreaves, Steph. "Cyber Security Threats against Global Governments Increase Exponentially." *Open Access Government*, 30 Oct. 2020, www.openaccessgovernment.org/cyber-security-threats-global-governments-increasing/96789/.

Kavanagh, Camino. "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft SMARTER RESPONSES?" *Carnegie Endowment for International Peace*, 28 Aug. 2019, www.carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

Liu, Wei, and at al, "Resource Guide on Artificial Resource Intelligence ." *Sustainable Development Goals*, UNESCO, Apr. 2021, https://sdgs.un.org/sites/default/files/2021-04/Resource%20Guide%20on%20AI%20Strategies_April%202021_rev_0.pdf

Saran, Samir, et al. "In Pursuit of Autonomy: AI and National Strategies." *ORF Special Report*, Observer Research Foundation, Nov. 2018, www.researchgate.net/publication/332752046_In_pursuit_of_autonomy_AI_and_national_strategies.

"UNESCO's 40th General CONFERENCE Confirms the Organization's Historic Turnaround and ITS Repositioning on Contemporary Issues." *UNESCO*, 29 Nov. 2019, https://en.unesco.org/generalconference/40/results

"Using Artificial Intelligence in Cybersecurity." *Balbix*, 18 Aug. 2020, www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.

Vought, Russel T. "Memorandum for the Heads of Executive Departments and Agencies." *Guidance for Regulation of Artificial Intelligence Applications*, 2019, www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

Wolf, Pam Greenberg; Mark. "Legislation Related to Artificial Intelligence." *National Conference of State Legislatures*, 2021, www.ncsl.org/research/telecommunications-and-information-technology/2020-l

egislation-related-to-artificial-intelligence.aspx.