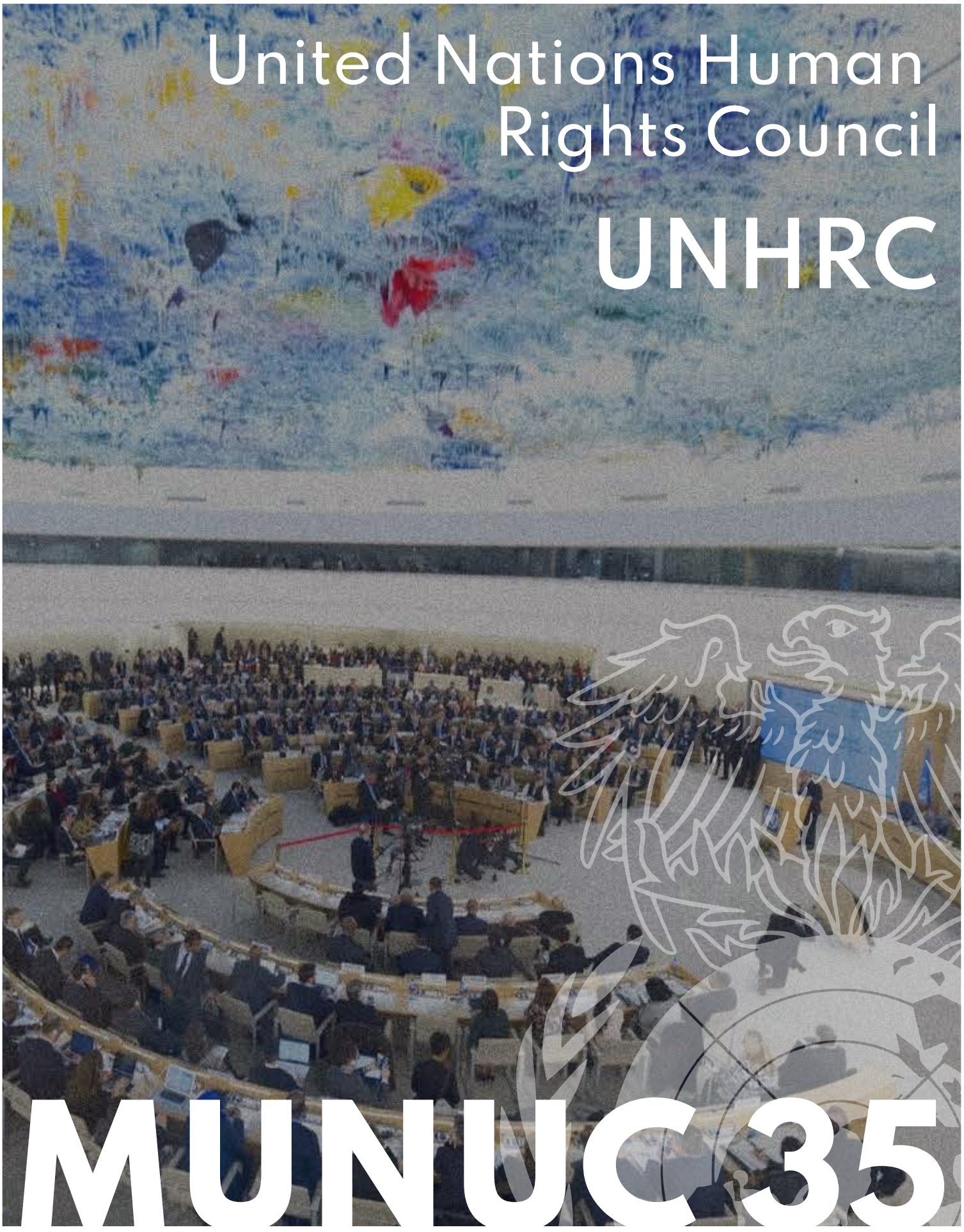
United Nations Human Rights Council

UNHRC



MUNUC 35

Model United Nations of the University of Chicago

TABLE OF CONTENTS

CHAIR LETTERS

Dear delegates,

I'm Irene Qi, and I am so incredibly thrilled to welcome you all to MUNUC 35! Along with Katie, I'll be serving as one of your co-chairs for the United Nations Human Rights Council (UNHRC). During the conference, we'll dive into some of the most pressing human rights issues in our modern, digitizing world. I can't wait to hear your thoughts, ideas, and suggestions as we explore the fundamental freedoms of our global community.

Originally from the Washington D.C. area, I'm currently a second-year in the College majoring in History and Political Science with a potential minor in Art History. I was involved in Model UN all throughout high school, and last year, I was an Assistant Chair for a continuous crisis committee—Senate and Advisors of West Berlin, 1949. Outside of MUNUC, I edit for the opinion section of The Chicago Maroon and work in civic engagement at the Institute of Politics (ask me about the time Obama came to visit!). In my free time, I enjoy art, scuba diving, and exploring the vast Chicago food scene with my best friends.

In this committee, we'll be discussing two interconnected topics that have emerged with developing technologies: Digitizing Human Rights and Dark Web and Cybersecurity. The uncertainty of the digital world's future places us at a precarious and unprecedented position, and I'm excited to see what you all come up with. As you debate solutions and come up with innovative possibilities, it's important for us to remember to treat such issues with empathy, sensitivity, and respect. Through this committee, I hope you'll gain a deeper understanding of pressing human rights issues, collaborate with your peers, and most importantly, have fun! I can't wait to see everyone in February, and in the meantime, please don't hesitate to reach out with any questions regarding MUNUC or UChicago in general.

Sincerely,

Irene Qi

iqi@uchicago.edu

Dear delegates,

Welcome to MUNUC 35! I'm Katie Fraser, and I am so excited to be serving as one of your co-chairs for the United Nations Human Rights Council, also known as UNHRC. This committee is incredibly relevant, allowing us to reflect and create solutions to one of the most pressing and complex issues of this decade – digital rights in the human era.

A little bit about me: I'm a second-year in the College studying Political Science and History! I grew up in Dallas, TX so I'm not great with cold weather, but I've gotten used to wearing a coat over the past chilly year in Chicago. Last year, I was a moderator for the MUNUC 34 UNESCO and a chair for MUNUC Asia's UNESCO, so I am so excited to now have the chance to chair another ECOSOC committee! In addition to MUNUC, I also chair the Chicago Prohibition JCC for ChoMUN (our collegiate level conference), write arts and news articles for The Chicago Maroon, and tutor math for 2nd-grade students. I am so excited to be your chair for this committee and I can't wait to hear all of your great ideas!

Through this committee, I hope you will start creating innovative and unique solutions to such a new, yet important problem: cybersecurity and how digital human rights can be ensured on a global scale. With the novelty of this topic, I believe discussion is incredibly relevant, and will apply broadly to many other current issues the world is facing. More than anything, I hope everyone in the committee is given the opportunity to learn more about the world around us while still having fun! I really look forward to getting to know all of you throughout the conference! Please reach out with any questions.

Sincerely,

Katie Fraser

kjoyfraser@uchicago.edu

HISTORY OF COMMITTEE

The United Nations Human Rights Council, or the UNHRC, was established by the United Nations General Assembly on March 15, 2006, with the passing of resolution 60/251. From June 19-30th, 2006, the council held its first General Conference in Geneva. Preceded by the United Nations Commission on Human Rights, the UNHRC was formed with the intent of strengthening the promotion and protection of human rights around the globe, addressing situations of human rights violations, and making recommendations for best resolving them. Currently, the Council is composed of 47 Member States elected by the General Assembly.

The UN Commission on Human Rights was established even earlier in 1946 and was composed of 53 member states. Similarly, the Commission focused on responding to a range of human rights issues and setting standards to govern the conduct of States.

The UNHRC has pursued these goals through reform-focused initiatives including the Universal Periodic Review (UPR), the Advisory Committee, and a partnership with UN Special Procedures. The UPR allows the UNHRC to review the human rights records of all UN Member States and gives Member States the opportunity to declare what actions they've taken to improve human rights conditions within their countries. The UNHRC's Advisory Committee serves as a "think tank" to offer expertise and research proposals for the advancement of human rights issues across the globe. Lastly, the UNHRC's Special Procedures mandate holders are made up of special rapporteurs, independent experts, and working groups who monitor human rights around the world through country visits, thematic studies, and action on individual cases of human rights violation. The UNHRC aims to promote international human rights standards in every capacity through a variety of methods, all advancing toward the same end goal of the end of human suffering.

TOPIC A: DIGITIZING HUMAN RIGHTS

Statement of the Problem

In our digital world, technology gathers, stores, and accesses vast amounts of information regarding our daily interactions and habits on a second-by-second basis. Whether we're Googling easy recipes, registering for virtual classes, online browsing for a new summer wardrobe, or scrolling through our curated For You pages on TikTok—the collected data feeds our ever-expanding digital footprints. While digital technologies have certainly provided modern convenience and accessible platforms, their impact on and implications for our protected human rights have become a pressing, worldwide concern.

Human rights, the inherent rights of all human beings, regardless of race, sex, nationality, ethnicity, religion, or any other identity, span a wide range of civic, cultural, political, and social rights.[1] The United Nations has upheld international human rights law since its founding, and the 1948 Universal Declaration of Human Rights (UDHR) standardized the fundamental human rights countries should strive to protect. In "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family [as] the foundation of freedom, justice and peace in the world," the UDHR promotes the right to life and liberty, freedom of expression and assembly, the right to movement, work, and education, and more.[2] Since then, human rights law has expanded to include marginalized communities like women, children, persons with disabilities, and other minority groups facing discrimination. The introduction of digital technology, however, has blurred the way we understand our individual freedoms. As countries, corporations, and individual citizens navigate a rapidly evolving digitized world, human rights issues are challenged and called into question.

Digital technologies have undoubtedly incited unprecedented modern progress. Thanks to developments like the Internet or artificial intelligence, the ways we communicate and interact with one another have reached soaring new heights. Tools that promote our individual freedoms are

[1] "Human Rights," United Nations, accessed August 28, 2022, https://www.un.org/en/global-issues/human-rights.
[2] UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III) (10 December 1948), available from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

more easily accessible: online platforms can reach vast, global audiences, providing traditionally marginalized communities or those in more restrictive countries or societies with the means to exercise their freedom of speech and expression.[3] Accessing news, groundbreaking research, and all types of information have become increasingly simple with search engines and social media at our fingertips. This expansion of civic space has allowed almost everyone with Internet access to have the ability to amplify their voice and connect with people holding similar or disagreeing views from all over the world. Nevertheless, such freedoms simultaneously contribute to an exacerbation of human rights issues. The same benefits associated with digital technologies pose malicious risks that undermine our privacy, freedom of expression, and right to participate in civil society. Protecting human rights becomes of the utmost importance—not only in the physical world, but in our digital world as well.

As we browse the Internet, clicking on new webpages and downloading mobile apps, we permit companies to collect and analyze our data. By accepting Terms and Conditions without bothering to read fine details, we enter legal agreements between the provider of a service and ourselves, its users. By accepting cookies, information collectors and trackers stored on our browsers, we grant companies explicit permission to use our information. Most of the time, cookies pose no harm and merely serve to personalize our browsing experience, like through saving the items in our online shopping cart whenever we revisit the site. Nevertheless, the complex of data tracking has introduced challenges to consumer privacy. Coined by Harvard Business School academic Shoshana Zuboff, "surveillance capitalism" refers to the system in which technology giants "unilaterally claim human experience as free raw material for translation in behavioral data."[4] Big Tech companies like Google and Facebook subsequently generate profit by forming "prediction products" from our data in order to push products, influence markets, and even sway elections.[5] Online activity is then used to specifically target consumers under the pressures of capitalism and profit-making. This commodification of personal data can present a threat to our individual liberty and autonomy, as well as to privacy.

[3] Fiona Quimbre and Sam Stockwell, "The Implications for Human Rights in the Digital Age--," RAND Corporation, September 3, 2021, https://www.rand.org/blog/2021/09/the-implications-for-human-rights-in-the-digital-age.html.
[4] William Ham Bevan, "Human Rights in a digital age," University of Cambridge, accessed August 28, 2022, https://www.cam.ac.uk/cammagazine/humanrightsinadigitalage.
[5] Ibid.

Technologies like artificial intelligence and algorithmic decision making widely use tactics like data modeling and predictive analytics. While this practice can serve the public by targeting hate speech or disinformation, 'big data' can also consist of surveillance targeting not only the right to privacy, but also freedoms of expression, movement, and assembly.[6] Freedom of expression, in particular, can be especially impacted by AI systems. The tracking behavior of AI can lead to applications of self-censorship in online spaces and automated content regulation decisions. Furthermore, technologies that threaten freedom of expression and privacy—such as facial recognition, video surveillance, behavior analysis, etc.—have become increasingly popular among public authorities and private organizations.[7] States and businesses can take advantage of the digital realm's accessibility to surveillance that "feeds analysis, prediction, and even manipulation of our behavior" to the risk of undermining democratic processes.[8]

Efforts to regulate digital behavior have also incited concerns regarding the degree of monitoring content. On social media, managing online content can resemble a commitment to uphold and protect digital rights: platforms can create content policies and shut down violating material and actions like cyberbullying and harassment.[9] Furthermore, digital regulations can target hate speech and disinformation—false or misleading information that is intentionally spread to harm or deceive (*mis*information, on the other hand, is false or misleading information that is spread regardless of intent). Disinformation has threatened democratic systems and shaken public trust. Especially during the COVID-19 pandemic, disinformation has been used against vulnerable and at-risk communities, jeopardizing the legitimacy of public health experts as digital tools spread false claims about masking, tests, and vaccines.[10] In particular, underserved communities disproportionately face

[6] "Human rights in the digital age: Making digital technology work for human rights," Universal Rights Group, accessed August 28, 2022, https://www.universal-rights.org/urg-policy-reports/human-rights-in-the-digital-age-making-digital-technology-work-for-human-rights/.
[7] "Privacy and Freedom of Expression In the Age of Artificial Intelligence," ARTICLE 19 and Privacy International, April 25, 2018, https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.
[8] Michelle Bachelet, "Human rights and democracy in the digital age," United Nations Human Rights Office, April 25, 2022, https://www.ohchr.org/en/statements/2022/04/human-rights-and-democracy-digital-age.
[9] William Ham Bevan, "Human Rights in a digital age," University of Cambridge, accessed August 28, 2022, https://www.cam.ac.uk/cammagazine/humanrightsinadigitalage.
[10] Fiona Quimbre and Sam Stockwell, "The Implications for Human Rights in the Digital Age--," RAND Corporation, September 3, 2021, https://www.rand.org/blog/2021/09/the-implications-for-human-rights-in-the-digital-age.html.

the implications of disinformation, as populations lacking access to sources of reliable and trusted information are more susceptible to spreading false claims.

Other digital materials aimed at spreading falsified content, like deepfake technology, have even more dangerous implications for human rights. Deepfakes, AI-generated media in which another person's image replaces someone in an already-existing image or video, are remarkably powerful tools of deception. The spread of such content threatens human rights and dignity. This risk is especially prevalent among marginalized population groups: 96% of all deep fake videos target women.[11]

With the eruption of harmful digital content like disinformation and falsified deep fake videos, regulating content spread online becomes a tricky balance between the preservation of a safe online environment and the protection of one's freedom of expression. Historically, when countries and organizations use content regulation as a means to control the populace, human rights become restricted. Governments have imposed regulations on digital services and used Internet shutdowns to establish control over information and communication. This behavior allows states to target freedom of assembly by disrupting organization efforts and subverting political activism and mobilization.[12] Protecting our right to participate in government through expression and assembly is essential.

Targeting hate speech and fake news must work in tandem with maintaining the free flow of information and opinions on digital platforms. In order to uphold human rights online as well as offline, access to digital environments free of surveillance, harm, and censorship must be protected. States have a duty to recognize digital threats to human rights and act effectively to combat them.

[11] "Human rights in the digital age: Making digital technology work for human rights," Universal Rights Group, accessed August 28, 2022, https://www.universal-rights.org/urg-policy-reports/human-rights-in-the-digital-age-making-digital-technology-work-for-human-rights/.
[12] Fiona Quimbre and Sam Stockwell, "The Implications for Human Rights in the Digital Age--," RAND Corporation, September 3, 2021, https://www.rand.org/blog/2021/09/the-implications-for-human-rights-in-the-digital-age.html.

History of the Problem

With the World Wide Web only coming to life around thirty years ago, the history of the digitization of human rights is fairly new. The time period known as the "digital age," also referred to as the information age, is defined as "the time period starting in the 1970s with the introduction of the personal computer with subsequent technology introduced providing the ability to transfer information freely and quickly."[13] The digital era has emerged through a combination of new technology, particularly computers and the Internet, and changes in surveillance. Instead of being constrained to the movement of information, technology has spread into every area of life, affecting everything from businesses to the basic protection of human rights.

A Need for Digital Human Rights

In the early rise of the internet, digital rights weren't as discussed, due to the Internet only being available to trusted institutions, such as universities. However, with the creation of the World Wide Web in the early 90s, the Internet became available to everyone. The increased accessibility of such a wide database of information introduced a demand for regulation. For example, Internet users had to go through the process of registering domain names, which are critical to navigating websites.[14] With these regulations, it was more difficult to misuse the immense power Internet users were given.

As the Internet became more regulated during its early years, questions arose from users – how could people protect their property online? Piracy was causing CD sales to spiral downward, while online video was becoming more popular. These situations brought digital rights management (DRM), or the management of legal access to digital content,[15] to the center of the digital rights discussion. Businesses had a vital interest in protecting their digital products, or any goods that existed in a digital format.

With the rise in demand for DRM came strong opposition by the public against business-driven digital rights management with its strict approach toward copyright. For example, business-driven

[13] "Digital-Age Definition," YourDictionary, Accessed August 31, 2022, https://www.yourdictionary.com/digital-age.
[14] Christian Kreutz, "Introduction to Digital Human Rights," Crisscrossed, November 8, 2018, https://www.crisscrossed.net/blog/2018-11-08-Introduction-human-digital-rights.
[15] "Digital Rights Management," Wikipedia, August 17, 2022, https://en.wikipedia.org/wiki/Digital_rights_management.

DRM said that it would be illegal to use music videos on YouTube to remix a new song. Users found these policies too harsh, claiming it set a limit on how they could actually use the internet. Therefore, a chosen alternative to digital rights management came to light: the Creative Commons movement. This movement had a "fair use" approach towards digital products in which digital content producers could decide themselves about their license and usage of their content. The expanded use of Creative Commons helped change the way people share content and how the internet operates. While in some places globally, restrictions on using creative works have increased, sharing and remixing are still common. "In domains like textbook publishing, academic research, documentary film, and many more, restrictive copyright rules continue to inhibit creation, access, and remix." [16] However, with the use of Creative Commons licenses, more people can access and reuse digital content, and, as of now, these licenses are used on almost 2 billion works online across 9 million websites.

The History of Digital Surveillance

In the 1970s, the Defense Advanced Research Projects Agency (DARPA), the agency responsible for developing emerging technologies for military, intelligence, and national security purposes, linked four supercomputers to handle massive data transfers. It handed the operations off to the National Science Foundation (NSF) a decade or so later, which proliferated the network across thousands of universities and, eventually, the public, thus creating the architecture and scaffolding of the World Wide Web.

Silicon Valley would later take the same route. By the mid-1990s, the intelligence community was seeding funding to the most promising supercomputing efforts across academia, guiding the creation of efforts to make massive amounts of information useful for both the private sector as well as the intelligence community. They funded these computer scientists through an unclassified, highly compartmentalized program called the Massive Digital Data Systems (MDDS) project that was managed for the CIA and the NSA by large military and intelligence contractors.

[16] "The Story of Creative Commons," Creative Commons Certificate for Educators, Academic Librarians and GLAM, Accessed August 31, 2022, https://certificates.creativecommons.org/cccertedu/chapter/1-1-the-story-of-creative-commons/.

21st Century Examples of Digital Scandals and Corresponding Debates

National Security Agency

On 5 June 2013, a British newspaper, The Guardian, published the first in a series of revelations about indiscriminate mass surveillance by the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ). Edward Snowden, a whistleblower who had worked with the NSA, provided concrete evidence of global communications surveillance programs that monitor the internet and phone activity of hundreds of millions of people across the world. The release of this information had a tremendous effect on the digital world and community, with the three biggest impacts being "increased interest in encryption, business leaving U.S. companies, and a reconsideration of the safety of cloud technology."[17]

The death of Aaron Swartz

Aaron Swartz was involved in almost every corner of digital rights, co-founding activist organizations Demand Progress and the Progressive Change Campaign Committee, becoming an early Reddit co-owner, and earning a spot as a Harvard University Center for Ethics fellow. He was particularly interested in freedom of expression, open government, and open access and freedom of information activism. But his activism also landed him in legal trouble: after downloading 4.8 million documents from the academic database JSTOR, while signed in as a guest to the MIT network, he faced up to 35 years in prison. While some believed that his mass download was unethical, others felt that it was a way of drawing attention to an important problem in the digital world, namely the current model for distributing academic works. In this model, many academics give up their copyrights to commercial publishers who resell them for a much higher price.[18] Later, in 2011, JSTOR settled with Swartz, but prosecutors kept on pushing for prison time. However, before his trial could come to a finish, Swartz tragically ended his own life. Many in the open access movement, which advocates for policies designed to provide unrestricted access to peer-reviewed research online (like journals voluntarily

[17] "Snowden effect," Wikipedia, August 18, 2022, https://en.wikipedia.org/wiki/Snowden_effect#:~:text=According%20to%20TechRepublic%2C%20revelations%20from,the%20safety%20of%20cloud%20technology.
[18] Timothy Lee, "Feds go overboard in prosecuting information activist," arsTechnica, Conde Nast, September 20, 2012, https://arstechnica.com/tech-policy/2012/09/feds-go-overboard-in-prosecuting-information-activist/.

making their content available online or universities mandating research published by members of their community be posted in an online repository) are still invigorated to continue Swartz's mission for a free Internet.

Massive Yahoo data breach

In December 2014, Yahoo's security team discovered that Russian hackers had obtained the usernames, email addresses, phone numbers, birthdates, passwords, and security questions/answers for at least 500 million Yahoo accounts. Within days of the discovery, according to the SEC, "members of Yahoo's senior management and legal teams received various internal reports from Yahoo's Chief Information Security Officer (CISO) stating that the theft of hundreds of millions of Yahoo users' personal data had occurred." Yahoo's internal security team thereafter was aware that the same hackers were continuously targeting Yahoo's user database throughout 2015 and early 2016, and also received reports that Yahoo user credentials were for sale on the Dark Web.

Since September 2016, Yahoo has twice revised its data breach disclosure. In December 2016, Yahoo disclosed that hackers had stolen data from 1 billion Yahoo users in August 2013, and had also forged cookies that would allow an intruder to access user accounts without supplying a valid password in 2015 and 2016. On March 1, 2017, Yahoo filed its 2016 Form 10-K, describing the 2014 hacking incident as having been committed by a "state-sponsored actor," and the August 2013 hacking incident by an "unauthorized third party."

Facebook's Cambridge Analytica scandal

In 2015, a political data-analytics firm named Cambridge Analytica harvested information from over 87 million Facebook users through an external app in 2015. The data came from a personality quiz, which around 270,000 people were paid to take. The quiz—"thisisyourdigitallife"—also pulled data from user's friends' profiles, ending in an enormous data stash. The quiz harvested personal information on where users lived and what pages they liked, which helped build psychological profiles that analyzed characteristics and personality traits. This kind of information was later deployed in political campaigns. In early 2018, Facebook and the firm were implicated.

Facebook dealing with multiple privacy breaches

June 2013: Bug exposes personal data of 6 million users

March 2018: Cambridge Analytica Scandal (refer to above) affects 87 million users

May 2018: Facebook bug makes 14 million users' private posts public

September 2018: Attackers access data of up to 90 million users

December 2018: New York Times discovers Facebook sharing user data without permission

March 2019: Up to 600 million Facebook passwords stored in plaintext files

April 2019: 540 million Facebook user records found on Amazon cloud public server

April 2019: Facebook uploads 1.5 million users' email contacts without permission

September 2019: Data for 419 million Facebook users found on exposed server

December 2019: Hacker group captures data from 300+ million Facebook accounts

June 2020: Facebook accidentally shares user data with third-party developers

April 2021: Personal data for over 530 million Facebook users leaks in online forum

Preserving voter privacy and preventing election interference in the United States

In July 2016, Russian hackers, using an encrypted file with instructions, released 20,000 emails stolen from the servers of the Democratic National Committee to WikiLeaks.

With the continued prominence of data breaches and unexpected surveillance, it is clear that changes in internet security and the digital world are necessary. By first defining how we can understand human rights in the digital world, and then putting those words into action, we can better create guidelines around solutions to keep these digital scandals from occurring.

Past Actions

The Human Rights Council and the broader UN has placed increasing emphasis on protecting human rights amid the advent of new technologies and a complex digital world. In 1966, the UN General Assembly adopted the International Covenant on Civil and Political Rights (ICCPR). A multilateral treaty that establishes rights like freedom of religion, freedom of speech, freedom of assembly, and other electoral and legal rights, the ICCPR also protects individuals from interference with one's privacy. Article 17 declares, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence…"[19] Nearly twenty years later, in 1988, the Human Rights Committee interpreted Article 17 in General Comment 16.[20] The Committee established the right to privacy to include a wide range of interests, including bodily privacy, territorial privacy, privacy regarding personal relationships, reputational protection, and "privacy of one's communications and personal data."[21] Such interpretation, written far before methods of harvesting data and storing personal information became a common tactic among technology companies and state surveillance strategies, does not reflect a changing paradigm of human rights in the digital era.

In recent years, however, the HRC has recognized the urgency required to match pace with a shifting platform. As the UN considers the human rights implications of the Internet and other new technologies, research reports and roadmaps have begun tying human rights and digital rights closer together. In 2018, the HRC adopted Resolution 38/7 on "The promotion, protection and enjoyment of human rights on the Internet." Resolution 38/7 cited the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and it "affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[22] Furthermore, in July of 2019, the HRC adopted Resolution 41/11 on "New and emerging digital technologies and human

[19] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations Treaty Series, vol. 999, p. 171, available from https://www.refworld.org/docid/3ae6b3aao.html.
[20] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988), available from https://www.refworld.org/docid/453883f922.html.
[21] "Informational Privacy in the Digital Age," American Civil Liberties Union, accessed August 28, 2022, https://www.aclu.org/other/human-right-privacy-digital-age.
[22] Human Rights Council resolution 38/7, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/38/7 (17 July 2018), available from https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/7.

rights." This resolution pledged to look into the positive and negative human rights implications of technologies and to promote a multi-stakeholder approach that involved states, private sectors, international organizations, and other civil society, academic, and technical communities. Resolution 41/11 proclaims that "rapid technological change affects States in different ways, and that addressing these impacts…requires international and multi-stakeholder cooperation in order to benefit from opportunities and to address the challenges arising from this change…"[23]

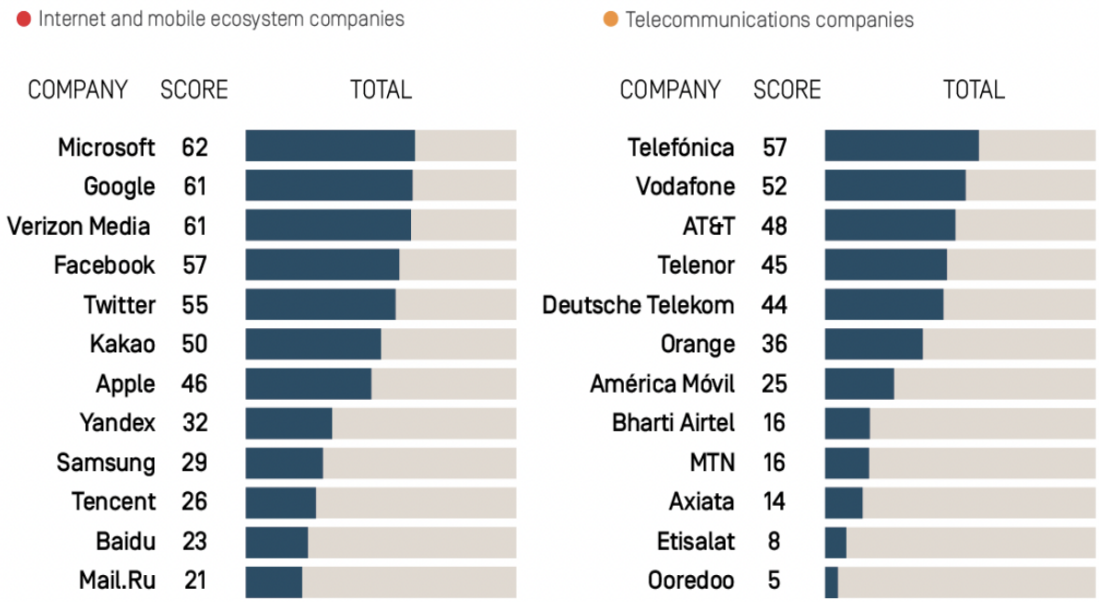
The HRC has also narrowed in on the crucial human right to privacy. In September of 2019, the HRC adopted Resolution 42/15 on "The right to privacy in the digital age." This resolution cited past resolutions on the digital right to privacy, including Resolution 73/179 of December 2018 that promoted further discussion on how artificial intelligence, without safeguards, could impact privacy rights (other resolutions on the right to privacy in the digital age include General Assembly resolutions 68/167 of December 2013, 69/166 of December 2014, and 71/199 of December 2016). The most recent resolution from 2019 reaffirms the right to privacy as stated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In Article 6, it "calls upon all states…To review…their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy…"[24] Similarly, in Article 8, the resolution also "encourages all business enterprises…To meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights…"[25]

While such international agreements have reaffirmed the importance of protecting human rights in the digital era, enacting specific policies has been left to the private sector. Sometimes in cooperation with governments, technology companies and platforms have created their own policies to regulate content in accordance with human rights standards. In 2019, the Ranking Digital Rights Corporate Accountability Index assessed the public commitments and policies regarding freedom of expression and privacy of the leading 24 internet, mobile ecosystem, and

[23] Human Rights Council resolution 41/11, *New and emerging digital technologies and human rights*, A/HRC/RES/41/11 (17 July 2019), available from https://ap.ohchr.org/Documents/dpage_e.aspx?si=A/HRC/RES/41/11.
[24] Human Rights Council resolution 42/15, *The right to privacy in the digital age*, A/HRC/RES/42/15 (7 October 2019), available from https://ap.ohchr.org/Documents/dpage_e.aspx?si=A/HRC/RES/42/15.
[25] Ibid.

telecommunications companies of the world. The majority of Internet users use the products and services offered by these 24 companies, and combined, these companies held a market capitalization of nearly USD 5 trillion.[26] The RDR Index used 35 indicators that evaluated "disclosed commitments, policies, and practices affecting freedom of expression and privacy, including corporate governance and accountability mechanisms," and the final scores represent "the extent to which companies are meeting minimum standards."[27]

Figure 1 | The 2019 RDR Corporate Accountability Index ranking



The 2019 RDR Corporate Accountability Index ranking reveals the extent to which companies meet minimum standards for protecting freedom of expression and privacy.

Evidently, different companies will hold themselves to different standards. Twitter, for example, has taken steps to flag posts that spread disinformation. False claims regarding COVID-19 or election fraud are removed or clarified with a notice warning audiences of the disputed statement. Facebook has also started using algorithms to identify and remove posts that aim to promote violence or hate. In 2020, a new Oversight Board, composed of independent human rights experts, began reviewing

[26] "2019 Ranking Digital Rights Corporate Accountability Index," Ranking Digital Rights, accessed August 28, 2022, https://rankingdigitalrights.org/index2019/
[27] Ibid.

and making decisions on Facebook's content moderation policies. Despite these measures, both Twitter and Facebook barely score above 50 percent on the 2019 RDR Index. Multifaceted, more long term solutions are necessary.

Possible Solutions

The complexity and evolving nature of the digital world requires solutions that will address human rights in a comprehensive and global way. A multi-stakeholder approach should be the goal. Collaboration among states, private technology companies, international bodies and experts, civil society, academic communities, and more is necessary to confront all dimensions of the issue. Nevertheless, finding the balance will be challenging.

Maintaining a public-private partnership will be crucial for protecting digital human rights. Both states and technology companies should find common ground in their mutual interest in regulating the spread of hate speech and disinformation, while also promoting freedom of expression. For companies, more steps should be taken to go beyond legal compliance as "no legal regime enables or requires the full range of actions companies should take to respect and protect users' human rights."[28] Companies can practice transparency, as well, to ensure that users know how their data and personal information can be accessed and used and how their online movement may be regulated. Employing oversight and due diligence measures can also examine how a company's business may impact rights like privacy and freedom of expression, and can ensure a company puts in the maximum effort to protect these rights. Furthermore, as the digital world rapidly shifts and develops, companies should work with investors, civil society, and governments to match developments and produce new strategies.

States, on the other hand, have a primary responsibility to uphold human rights. Instead of allowing technology companies free reign of policies, states can enact clear and firm frameworks for private companies to operate within. Data protection laws can prioritize users' rights by protecting their privacy. States can also implement corporate governance to supervise technology companies, including but not limited to board oversight, reports, and assessments. Government power, too, can be subject to oversight. States' abilities to regulate online speech and use personal data should be kept in check in order to prevent state censorship and abuse of surveillance power.

[28] "Executive summary," Ranking Digital Rights, accessed August 28, 2022. https://rankingdigitalrights.org/index2019/report/executive-summary/

The HRC, UN, and other international organizations can maintain a leading role in establishing international expectations for digital human rights. International organizations should hold states accountable for violations of digital freedoms. For example, oversight of human rights protection can take the form of a single 'social media council' composed of social media companies, public officials, the UN, and civil society. A multi-stakeholder council like such—or perhaps, a number of national councils—could carry the responsibility of monitoring content moderation policies. With the Internet effectively acting as a universal communication tool that can transcend borders and languages, digital human rights thus becomes an international issue requiring universal collaboration and innovation.

Bloc Positions

Asia

Although many countries in Asia are rising to be some of the most technologically advanced in the world, much of the continent is also witnessing an increase in sophisticated technology devoted to digital authoritarianism. In early 2021, Myanmar faced a digital human rights crisis with the coup d'etat staged by the Myanmar military, known as the *Tatmadaw* in the local language. The Tatmadaw used digital surveillance as a tool to seize control of the country, restricting the internet, blocking social media platforms, disseminating disinformation and misinformation, coercing telecom operators to comply with state surveillance, amending laws related to digital rights, and harassing independent online media.

Overall, human rights situations across Asia have long been a concern, and threats against human rights have increasingly crept into the digital space in recent years, with the internet being more and more commonly used. The region is facing more sophisticated tactics that threaten human rights, including the normalization of internet restrictions, a race for control of social media platforms, and the plan to establish national internet gateways.

Africa

A growing number of citizens in Africa are using the internet on a regular basis, making digital technologies pivotal to the enjoyment of their rights and improvement of their livelihoods. However, many governments are taking steps that undermine internet access and affordability, as well as weaken the potential of digital technologies to catalyze free expression and civic participation. With this, there has been an increase in digital rights violations such as arrests and intimidation of online users, internet blockages, and a proliferation of laws and regulations that undermine the potential of technology to drive socio-economic and political development on the continent.

Africa has the lowest internet usage figures compared to other regions and also experiences a deep digital divide. The moves seen in some countries which hamper access and affordability, and which unduly restrict citizens' rights to free speech, privacy and access to information, therefore undermine

efforts to bridge the digital divide. Moreover, they forestall the meaningful uptake of digital access, thus undercutting the potential of technology to improve governance and promote development.

Europe

In 2020, the EU introduced the Digital Services Act (DSA), a project focused on reigning in the power of Big Tech and giving European internet users more control over their digital lives. The wide-ranging plan includes how companies—online platforms, search engines, online marketplaces and every other significant provider of digital services—moderate and manage content; this includes illegal content, hate speech, and disinformation, and it also has a number of implications for children. This legislation was one of the first to broadly set boundaries around Europe's use of the Internet.

More recently, on January 26, 2022, the European Commission issued a Declaration on Digital Rights and Principles. The Declaration outlines the fundamental rights of EU citizens into the digital sphere, building on previous declarations and on the EU Charter of Fundamental Rights. However, even the European Commission, as the author of the declaration, emphasizes its declaratory nature and that it "does not as such affect the content of legal rules or their application."[29] Moving forward, European nations will focus on creating more enforceable regulations, especially concerning protecting people against the exploitation of data by private companies, the development of AI systems while respecting human rights, and freedom of expression on the Internet.

North America

While the United States is a liberal democracy with an emphasis on human rights and a culture of freedom, the government often circumvents that. Laws such as the Patriot Act legalize the use of personal data by the government in order to ensure national security, and that is a condition that can be met easily.[30] There are little to no checks and balances in place to ensure it is used democratically,

[29] Dominik Arncken and Christoph Nüßing, "A Digital Magna Carta? The European Declaration of Digital Rights," JD Supra, February 8, 2022, https://www.jdsupra.com/legalnews/a-digital-magna-carta-the-european-4946481/#:~:text=On%20January%2026%2C%202022%2C%20the,EU%20Charter%20of%20Fundamental%20Rights.
[30] Dara Lind, "Everyone's heard of the Patriot Act. Here's what it actually does." Vox, June 2, 2015, https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

and the same is true with other American surveillance infrastructure, with the Edward Snowden incident showing proof of that.[31] Companies are also given almost complete free reign to use data without consumer consent.[32] Thus, North American nations are interested in treading the fine line between individual rights and the rights and economic gains of companies.

Latin America and the Caribbean

Following World War II, Latin America led the creation of the world's first extensive international Human Rights instrument—the American Declaration of the Rights and Duties of Man, in April 1948—marking the beginning of the Rights Era, months before what would become its greater symbol, the Universal Declaration of Human Rights. However, presently, the absence of a unified political vision for tech policy in Latin America and the Caribbean has put the countries of the region at risk of dependency on a foreign private sector for their digital transformation.

[31] Michael Ray, "Edward Snowden Biography," Encyclopedia Britannica, June 17, 2022, https://www.britannica.com/biography/Edward-Snowden.
[32] Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," New York Times Wirecutter, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

Glossary

Creative Commons (CC): An internationally active non-profit organization that provides free licenses for creators to use when making their work available to the public. These licenses help the creator to give permission for others to use the work in advance under certain conditions. Every time a work is created, such as when a journal article is written or a photograph taken, that work is automatically protected by copyright. Copyright protection prevents others from using the work in certain ways, such as copying the work or putting the work online. CC licenses allow the creator of the work to select how they want others to use the work. When a creator releases their work under a CC license, members of the public know what they can and can't do with the work. This means that they only need to seek the creator's permission when they want to use the work in a way not permitted by the license.

Digital age: The time period starting in the 1970s with the introduction of the personal computer with subsequent technology providing the ability to transfer information freely and quickly.

Digital rights management (DRM): Protection of copyrighted works by various means to control or prevent digital copies from being shared over computer networks or telecommunications networks.

Internet Rights and Principles Dynamic Coalition: The Internet Rights and Principles Dynamic Coalition (IRP Coalition) is an open network of individuals and organizations based at the UN Internet Governance Forum (IGF) committed to making human rights and principles work for the online environment.

Internet Rights Charter: First developed in 2001-2002 by Association for Progressive Communication (APC) members and partner organizations at Internet Rights workshops held in Europe, Asia, Latin America and Africa and updated in 2006, the APC Internet Rights Charter enshrines the rights of people and organizations to use the internet freely, particularly in their work for social, economic and environmental justice. The Charter refers specifically to the internet; however, these principles are relevant to all other information and communication technologies (ICTs), including telephone, radio, and others.

World Wide Web: An information system enabling documents and other web resources to be accessed over the Internet.

Bibliography

Arncken, Dominik and Nüßing, Christoph. "A Digital Magna Carta? The European Declaration of Digital Rights." JD Supra. February 8, 2022. https://www.jdsupra.com/legalnews/a-digital-magna-carta-the-european-4946481/#:~:text=On%20January%2026%2C%202022%2C%20the,EU%20Charter%20of%20Fundamental%20Rights.

Bachelet, Michelle. "Human rights and democracy in the digital age." United Nations Human Rights Office. April 25, 2022. https://www.ohchr.org/en/statements/2022/04/human-rights-and-democracy-digital-age.

Bevan, William Ham. "Human Rights in a digital age." University of Cambridge. Accessed August 28, 2022. https://www.cam.ac.uk/cammagazine/humanrightsinadigitalage.

Human Rights Council resolution 38/7, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/38/7 (17 July 2018), available from https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/7.

Human Rights Council resolution 41/11, *New and emerging digital technologies and human rights*, A/HRC/RES/41/11 (17 July 2019), available from https://ap.ohchr.org/Documents/dpage_e.aspx?si=A/HRC/RES/41/11.

Human Rights Council resolution 42/15, *The right to privacy in the digital age*, A/HRC/RES/42/15 (7 October 2019), available from https://ap.ohchr.org/Documents/dpage_e.aspx?si=A/HRC/RES/42/15.

Klosowski, Thorin. "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." New York Times Wirecutter. September 6, 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

Kreutz, Christian. "Introduction to Digital Human Rights," Crisscrossed. November 8, 2018. https://www.crisscrossed.net/blog/2018-11-08-Introduction-human-digital-rights.

Lee, Timothy. "Feds go overboard in prosecuting information activist." arsTechnica. Conde Nast, September 20, 2012. https://arstechnica.com/tech-policy/2012/09/feds-go-overboard-in-prosecuting-information-activist/.

Lind, Dara. "Everyone's heard of the Patriot Act. Here's what it actually does." Vox. June 2, 2015. https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

Quimbre, Fiona and Stockwell, Sam. "The Implications for Human Rights in the Digital Age--." RAND Corporation. September 3, 2021. https://www.rand.org/blog/2021/09/the-implications-for-human-rights-in-the-digital-age.html.

Ray, Michael. "Edward Snowden Biography." Encyclopedia Britannica. June 17, 2022. https://www.britannica.com/biography/Edward-Snowden.

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966. *United Nations Treaty Series*, vol. 999, p. 171, available from https://www.refworld.org/docid/3ae6b3aao.html.

UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III) (10 December 1948), available from https://www.refworld.org/docid/3ae6b3712c.html.

UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988), available from https://www.refworld.org/docid/453883f922.html.

"2019 Ranking Digital Rights Corporate Accountability Index." Ranking Digital Rights. Accessed August 28, 2022. https://rankingdigitalrights.org/index2019/

"Digital Rights Management." Wikipedia. August 17, 2022. https://en.wikipedia.org/wiki/Digital_rights_management.

"Digital-Age Definition." YourDictionary. Accessed August 31, 2022. https://www.yourdictionary.com/digital-age.

"Executive summary." Ranking Digital Rights. Accessed August 28, 2022. https://rankingdigitalrights.org/index2019/report/executive-summary/

"Human rights in the digital age: Making digital technology work for human rights." Universal Rights Group. Accessed August 28, 2022. https://www.universal-rights.org/urg-policy-reports/human-rights-in-the-digital-age-making-digital-technology-work-for-human-rights/.

"Human Rights." United Nations. Accessed August 28, 2022. https://www.un.org/en/global-issues/human-rights.

"Informational Privacy in the Digital Age." American Civil Liberties Union. Accessed August 28, 2022. https://www.aclu.org/other/human-right-privacy-digital-age.

"Privacy and Freedom of Expression In the Age of Artificial Intelligence." ARTICLE 19 and Privacy International. April 25, 2018. https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

"Snowden effect." Wikipedia, August 18, 2022. https://en.wikipedia.org/wiki/Snowden_effect#:~:text=According%20to%20TechRepublic%2C%20revelations%20from,the%20safety%20of%20cloud%20technology.

"The Story of Creative Commons." Creative Commons Certificate for Educators, Academic Librarians and GLAM. Accessed August 31, 2022. https://certificates.creativecommons.org/cccertedu/chapter/1-1-the-story-of-creative-commons/.

TOPIC B: DARK WEB AND CYBERSECURITY

Statement of the Problem

The international digital community is facing a global safety crisis. With the prominence of the Dark Web and rising cybersecurity threats all around the world, creating measures to protect online users is more important than ever. Digital threats of all kinds present several avenues for harm, both physical and emotional. Additionally, as the world becomes more reliant on and trusting of technology, these threats are easier to encounter, even if readily prepared, which is rarely the case for tech users.

Cybersecurity

With this in mind, two key issues present a cause for concern. The first is cybersecurity threats, specifically cyberattacks, or "malicious and deliberate attempts by an individual or organization to breach the information system of another individual or organization."[33] This type of cyberattack has resulted in hospitals closing,[34] electrical grids going offline,[35] major cities practically shutting down,[36] and even government hacking concerns. A recent report commissioned by IBM calculated the global average cost of a data breach to a company in 2019 to be at $3.92 million USD.[37] As threats to cybersecurity become more common, complex, and severe, measures to strengthen cybersecurity by governments, businesses, and the tech industry are all being increased. However, many of these efforts don't take into account an important factor: the dimension of human rights within cybersecurity.

[33] "What Is a Cyberattack?" Cisco, Cisco Systems, Accessed August 31, 2022, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
[34] Alex Hern, "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017," The Guardian, Guardian News & Media Limited, December 30, 2017, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
[35] Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes, "Ukraine's power outage was a cyber attack: Ukrenergo," Reuters, January 18, 2017, https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.
[36] Swati Khandelwal, "Baltimore City Shuts Down Most of Its Servers After Ransomware Attack," The Hacker News, May 8, 2019, https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html.
[37] *Cost of a Data Breach Report* (IBM Security, 2019), https://www.ibm.com/downloads/cas/ZBZLY7KL.

While there is no universal definition of cybersecurity, the definition developed by the "Internet Free and Secure" working group of the Freedom Online Coalition (FOC), which was made up of technology experts, human rights academics, and government officials, is helpful for reference. The FOC working group defines cybersecurity as "the preservation—through policy, technology, and education—of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline."[38]

The Dark Web

The second issue is the infamous, yet widely-used, Dark Web, one of the most globally-spread cybersecurity threats. The layers of the Internet go far beyond the surface content that many can easily access in their daily searches. These deeper layers are made up of the Deep Web, with content that hasn't been indexed by traditional search engines like Google, and the Dark Web, which contains content that has been hidden on purpose.

In this so-called "Dark Web," the good and the bad coexist. Concerning its good uses, the Dark Web allows for anonymous and highly secure communication channels that prevent government oversight, so reform activists, such as human rights advocates and oppressed journalists, have a way to communicate under the radar. However, on the bad side, the Dark Web serves as a central hub for criminal activity and sales, working as a marketplace where anonymous customers can buy from anonymous sellers with confidence.[39] In order to examine the policing of such a complex interface, we must first separate these sides of the good and the bad.

[38] "Our Mission," Freedom Online Coalition, Accessed August 31, 2022, https://freedomonlinecoalition.com/.
[39] "Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs ," National Institute of Justice, June 15, 2020, https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs.

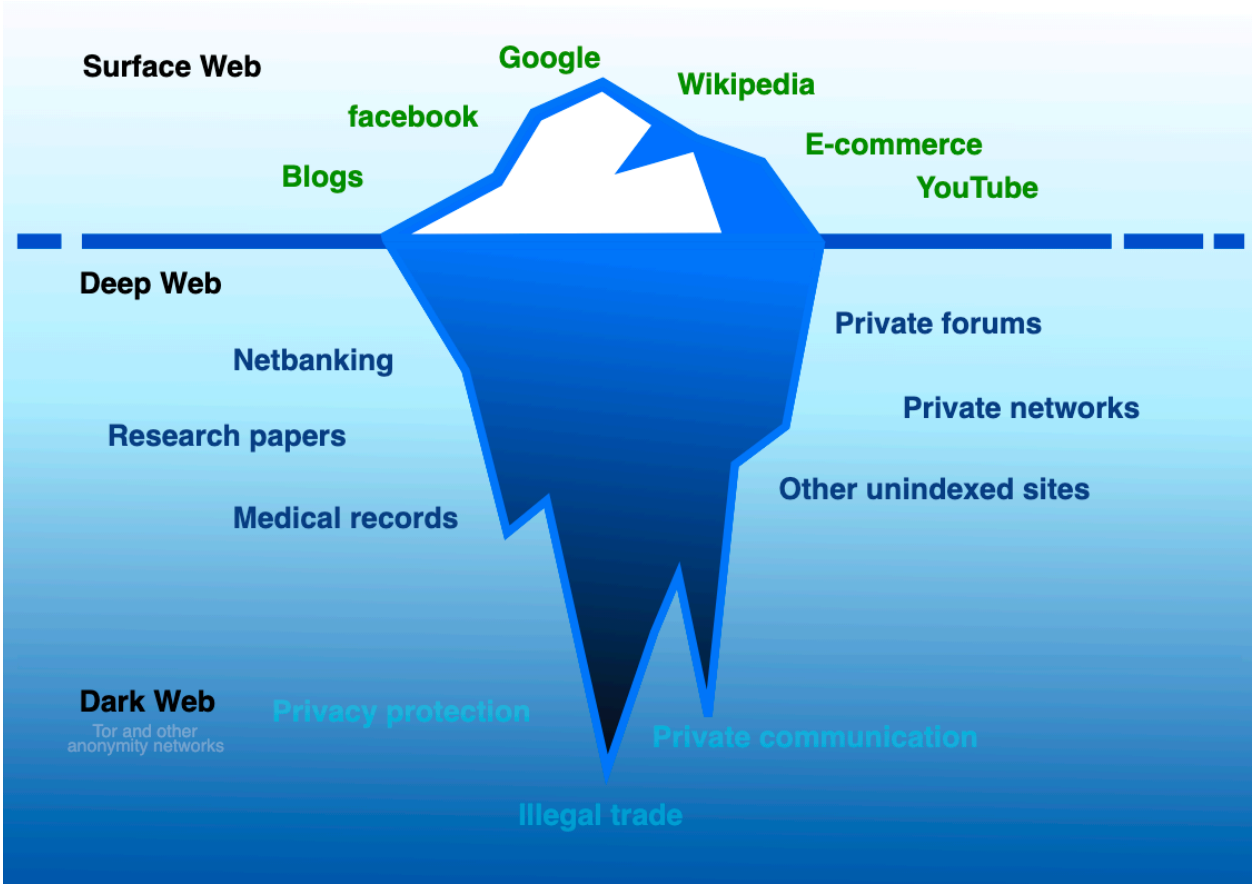


Image 1. Shows the layers of the Internet, from the Surface to the Dark Web.[40]

However, the Dark Web can be used for more than just sales. All kinds of malevolent users leverage this deeper level of the internet, including criminals, terrorists, and government-sponsored spies. Illegal goods such as drugs, weapons, exotic animals, and stolen goods and information are sold for profit. Gambling sites thrive, while thieves and assassins are available for easy hire. The effects permeate across all walks of life. Ransomware, for example, "is a type of malicious software used by hackers that locks particular files or a complete system until a payment is made by the victim."[41] These attacks happen within a certain time period, forcing organizations or people to pay in a hurry. The Dark Web often plays a significant role in the facilitation of ransomware attacks. Additionally, identity theft is a common attack on the everyday person enabled by the Dark Web when private information is posted to the Dark Web without a person's knowledge. Usually taken from high-

[40] Ranjithsiji, "Deepweb graphical representation like iceberg," Wikipedia, April 17, 2018, https://commons.wikimedia.org/wiki/File:Deepweb_graphical_representation.svg.
[41] Mark Lanterman, "Some Thoughts on the Dark Web—and How It Affects You," International Risk Management Institute, March 2018, https://www.irmi.com/articles/expert-commentary/some-thoughts-on-the-dark-web.

profile data breaches, Dark Web users can obtain stolen credit and debit card numbers, compromised medical information, Social Security numbers, and dates of birth, all allowing for a person's identity to be easily put up for sale. Whether being used as a communication, coordination, or action platform, the Dark Web allows these criminals to work with a lesser chance of being caught.

Data on the prevalence of these Dark Web sites, however, is lacking. Tor, an "anonymizing browser"[42] often used to access the Dark Web, estimates that only about 1.5% of Tor users visit hidden services/Dark Web pages.[43] The percentage of these users that actually serve any illegal market is unidentifiable, and there is no information on the Tor traffic accumulated at different sites.

The Dark Web can also take several roles in these crimes. Through forums, chat rooms, and communication services, criminal activity can be planned and coordinated by a number of people. Additionally, the Dark Web provides a platform for criminals to sell illegal or stolen goods. Understanding the methods of facilitating crime that is used on the Dark Web is of great importance, as it allows lawmakers and politicians to target their attention on the bad parts of the Dark Web instead of those that are used for better purposes.

With this rising danger of the Dark Web, politicians, law enforcement, and researchers have taken great interest in finding potential safeguards for Internet users. However, with the anonymity of services such as Tor, obtaining clear data and understanding the scope and nature of these levels of the Internet is very convoluted and difficult. Going forward, research and solutions must focus on how to work with evolving technologies, such as encryption, in an anonymous digital space, so that malicious actors looking to exploit cyberspace, including the Dark Web, can be effectively handled.

[42] Darren Guccione, "What is the dark web? How to access it and what you'll find," CSO Online, IDG Communications, July 1, 2021, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.
[43] nickm, "Tor: 80 percent of ??? percent of 1-2 percent abusive," Tor Blog, Tor Browser, December 30, 2014, https://blog.torproject.org/tor-80-percent-percent-1-2-percent-abusive/.

History of the Problem

The development of the Dark Web and a global culture of cybersecurity closely parallels the development of the Internet and its increasing popularity over the decades. Dark Web platforms have delivered privacy and anonymity, facilitating spaces for those living under oppressive states to access restricted information and communicate sensitive findings. At the same time, the same privacy and anonymity has allowed online crime to flourish. While the Dark Web remains shrouded to the majority of ordinary Internet users today, its origins were tied closely to the origins of the Internet itself.

In the 1960s, the formation of the Advanced Research Projects Agency Network (ARPANET) became the predecessor to the modern Internet.[44] ARPANET started as an experimental computer network and communications system that allowed for users to share information between devices. Despite originating in academia, the United States military quickly took advantage of the invention. Embroiled in the Cold War at the time, the Advanced Research Projects Agency (ARPA)—an arm of the U.S. Department of Defense—looked for a computer-based communications system that did not have a central core. This would increase protection against any opposition trying to disable entire networks by simply destroying a central core. As the U.S. government increasingly privatized use of ARPANET, experiments by academic researchers continued. In the early 1970s, a sale of marijuana between Stanford University's Artificial Intelligence Laboratory and their counterparts at Massachusetts Institute of Technology became the first illegal online transaction using ARPANET (the first *legitimate* online transaction did not occur until the 1990s).[45] In 1983, ARPANET split: MILNET became used by defense agencies, while a civilian version of ARPANET laid the foundations for the modern Internet.

At the same time, as the use of computers rose, developments in cybersecurity and viruses followed. In the early 1960s, BBN Technologies engineer Bob Thomas wrote the code for a program

[44] Erica Kastner, "History of the Dark Web [Timeline]," Standard Office Systems, February 7, 2020, https://www.soscanhelp.com/blog/history-of-the-dark-web.
[45] Mike Power, "Online highs are old as the net: the first e-commerce was a drugs deal," The Guardian, April 19, 2013, https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal.

considered to be the first computer worm in history.[46] The program moved between computers connected by ARPANET, and it showed a simple, innocuous message: "I'M THE CREEPER. CATCH ME IF YOU CAN!" Following the Creeper worm, fellow BBN Technologies colleague Ray Tomlinson—also the famed inventor of email—coded another program known as Reaper. The program not only moved between computers, but could also copy itself and would delete Thomas's 'creeper' worm. Creeper and Reaper laid the groundwork for how worms, viruses, and antivirus software would operate. A couple decades later, in the late 1980s, the Morris Worm became the first widespread incident of a denial-of-service (DoS) attack.[47] The virus infected nearly 10 percent of all computers connected to the Internet at the time (though accurate figures have been debated and difficult to determine), and it could replicate itself and infect a computer multiple times. This caused the computer to slow down with each infection until it ultimately crashed and became unusable. Robert Tappan Morris, the writer of the worm, was convicted in what was the first felony conviction in the U.S. under the Computer Fraud and Abuse Act. Computer Emergency Response Teams (CERTs) were also established as a means to respond to emergencies caused by viruses. While originating at Carnegie Mellon University under U.S. government contract, CERTs eventually expanded across international borders.[48] Furthermore, as the Internet expanded and viruses began saturating users' experiences in the 1990s, antivirus software proliferated and dominated the cybersecurity industry.[49]

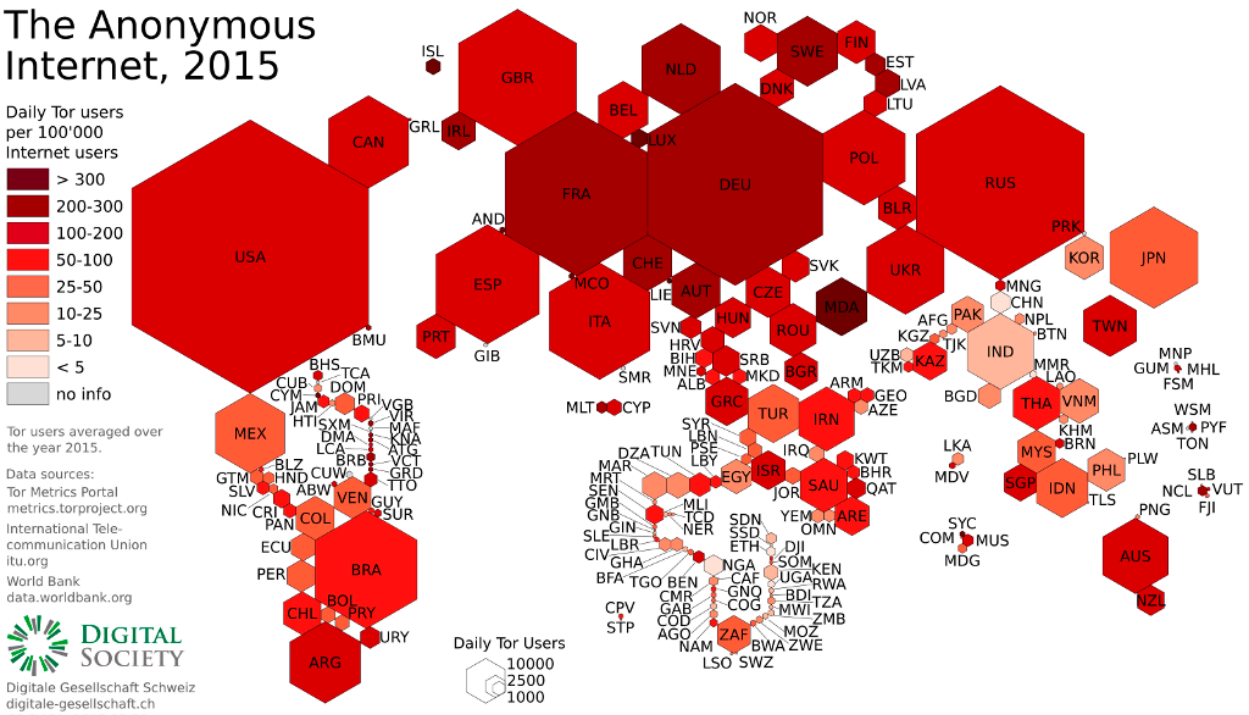
The 1990s became known as the "decade of the Internet boom and the Dot-Com bubble."[50] The Internet was released to the public, illegal music streaming flourished, and increasing concerns over online privacy paralleled the growing demand for online products. U.S. Naval Research Lab (NRL) researchers David Goldschlag, Mike Reed, and Paul Syverson began developing ways of anonymously routing Internet traffic in response to fears regarding surveillance, government tracking, and the lack of security the Internet provided.[51] They created a method called 'onion routing,' which anonymously routed Internet traffic through multiple servers while enclosing

[46] "The fascination evolution of cybersecurity," La Trobe University, accessed August 28, 2022, https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/.
[47] Ibid.
[48] "The CERT Division," Software Engineering Institute, Carnegie Mellon University, accessed August 28, 2022, https://www.sei.cmu.edu/about/divisions/cert/index.cfm.
[49] "The fascination evolution of cybersecurity," La Trobe University, accessed August 28, 2022, https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/.
[50] Erica Kastner, "History of the Dark Web [Timeline]," Standard Office Systems, February 7, 2020, https://www.soscanhelp.com/blog/history-of-the-dark-web.
[51] Ibid.

messages in layers of encryption. Onion routing safeguarded the anonymity of individuals in the intelligence community, protecting whistleblowers and providing a means for citizens and journalists under oppressive regimes to exercise their freedom of expression.[52] In 2002, the Onion Routing Project—commonly known as the Tor Project—was released. Despite originating as a platform intended for free and anonymous communication, Tor became instrumental in "open[ing] the door to the underbelly of the Internet."[53]

Tor gained in popularity over the years, providing a network for anonymous communication. Tor has been financially backed by multiple branches of the U.S. government, as well as international organizations and human rights foundations like Human Rights Watch. In 2008, a Tor browser was developed to increase accessibility. For citizens living under government firewalls and online censorship, the Dark Web provides essential access to information and protection for dissidents. Organizations, including major newspapers, Facebook, and the U.S. Central Intelligence Agency (CIA), also maintain hidden websites on Tor to facilitate communication of sensitive information.[54] In 2013, for example, the famed whistleblower Edward Snowden used Tor to leak classified information from the U.S. National Security Agency regarding mass surveillance to *The Washington Post* and *The Guardian*.[55]

[52] Kristin Austin, "The Origins and History of the Dark Web," IdentityIQ, October 17th, 2019, https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/.
[53] Erica Kastner, "History of the Dark Web [Timeline]," Standard Office Systems, February 7, 2020, https://www.soscanhelp.com/blog/history-of-the-dark-web.
[54] Aditi Kumar and Eric Rosenbach, "The Truth About the Dark Web," International Monetary Fund, accessed August 28, 2022, https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=In%20the%20late%201990s%2C%20two,accessible%20to%20ordinary%20internet%20surfers.
[55] Ewen Macaskill and Gabriel Dance, "NSA Files: Decoded," The Guardian, November 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.



Over 2 million users worldwide use Tor's private network.[56]

Nevertheless, at the same time, the anonymity and privacy protecting whistleblowers also make the Dark Web a breeding ground for online crime. With private browsing networks like Tor, crimes include "arms trafficking, drug dealing, and the sharing of exploitative content."[57] Rhetoric from neo-Nazis, white supremacists, and other extremist organizations run unregulated. Even in areas that lack equitable access to the Internet, Dark Web activity may inadvertently impact populations vulnerable to the drugs market or arms trafficking. Marketplaces have emerged with the invention of cryptocurrency and the release of Bitcoin in 2009. Cryptocurrency, "a form of digital currency that facilitates transactions anonymously," does not leave paper trails and easily facilitates illegal transactions on the Dark Web.[58] Sales of drugs, stolen or counterfeit documents, credit cards, bank credentials, and other services like hacking and technological crime services surged. The famed Silk Road marketplace hosted 1.2 million transactions between around 950,000 users from 2011 to 2013,

[56] "Tor usage worldwide: The Anonymous Internet," Digitale Gesellschaft, June 21, 2017, https://www.digitale-gesellschaft.ch/2017/06/21/tor-usage-worldwide-the-anonymous-internet-new-infographic/.
[57] Aditi Kumar and Eric Rosenbach, "The Truth About the Dark Web," International Monetary Fund, accessed August 28, 2022, https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=In%20the%20late%201990s%2C%20two,accessible%20to%20ordinary%20internet%20surfers.
[58] Erica Kastner, "History of the Dark Web [Timeline]," Standard Office Systems, February 7, 2020, https://www.soscanhelp.com/blog/history-of-the-dark-web.

and was estimated to have nearly $1.2 billion in value. Recreational and pharmaceutical drugs were the primary product of interest. In 2013, the U.S. Federal Bureau of Investigation (FBI) shut down the Silk Road in a successful sting operation and arrested Ross Ulbricht, charging him with money laundering, computer hacking, and conspiracy to traffic narcotics.[59] Nevertheless, similar marketplaces have continued to pop up and linger.

In more recent years, the growing complexity of Dark Web spaces has caused regulation to be challenging. International communities have confronted the global nature of the Dark Web by "improving information sharing, sharpening law enforcement's technical capabilities to take down major illicit marketplaces, and regulating the transfer of cryptocurrency transactions."[60] Cybersecurity attacks have become more sophisticated as well, causing the industry to employ artificial intelligence, machine learning, and behavioral detection.[61] In the rapidly shifting Internet era, international cooperation becomes of paramount importance.

[59] Kristin Austin, "The Origins and History of the Dark Web," IdentityIQ, October 17th, 2019, https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/.
[60] Aditi Kumar and Eric Rosenbach, "The Truth About the Dark Web," International Monetary Fund, accessed August 28, 2022, https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=In%20the%20late%201990s%2C%20two,accessible%20to%20ordinary%20internet%20surfers.
[61] "The fascination evolution of cybersecurity," La Trobe University, accessed August 28, 2022, https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/.

Past Actions

The UN often stresses the importance of cybersecurity and regularly calls on member nations to combat cybercrimes. These committees usually refer responsibilities to the International Telecommunications Union (ITU), a UN agency based in Geneva which is responsible for coordinating efforts on these issues. The ITU focuses resources and programs "on those areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defense, national security, content and cybercrime, which are within their sovereign rights."[62] By setting standards around the use of digital content and technology, the ITU hopes to create better communication and gateways between countries in the digital atmosphere. However, a large difficulty with these standards stem from their only power being a recommendation – the standards are non-binding, and nothing ensures that countries will adhere.

In 2007, the ITU introduced the Global Cybersecurity Agenda (GCA), which serves as a practical framework for all 193 Member States and more than 700 Sector Members to collaborate on cyber security.[63] The GCA consists of five pillars.

1. First, "legal measures" focuses on the persecution of unlawful cyber activities with an internationally consistent legislative approach;

2. "Technical and procedural measures" looks at the security standards of ICT applications and systems and best practices of risk management;

3. "Organizational structures" discusses national policies, and institutional setups allowing for an effective prevention, response to, and crisis management of cyberattacks;

4. "Capacity building" promotes awareness and technology sharing among all stakeholders;

5. And the last pillar, "international cooperation," promotes dialogue and coordinated action of the international community in dealing with cyber threats.

[62] "ITU Explainer: Cybersecurity," GP Digital, Accessed August 31, 2022, https://www.gp-digital.org/wp-content/uploads/2018/08/ITU_Explainers_cybersecurity.pdf.
[63] 02 UN ITU, *Global Cybersecurity Agenda (GCA)* (2007), available from https://www.itu.int/ITU-D/cyb/events/2007/Geneva/docs/kitaw-global-cybersecurity-agenda-geneva-17-sept-07.pdf.

The very first legally binding agreement governing cyberspace was enacted by the Council of Europe (CoE) on a regional level. This agreement, known as the Budapest Convention on Cybercrime, was adopted in 2001 and entered into force in 2004,[64] outlining policies and legislation to protect member states against cybercrime through prosecution of offenses and cooperation between Member States to address common cybersecurity threats.[65] To date, almost all CoE Member States have both signed and ratified the convention with the exception of Ireland, Russia, Sweden, and San Marino.[66] There are also a number of non-members that have become signatories, such as the United States of America. In 2014, the African Union (AU) Convention on Cyber Security and Personal Data Protection established a standard legal framework for aspects such as online business and digital privacy while addressing emerging issues of cyber security and cybercrime.[67] Having solid regulation over cyberspace is critical for safe usage of information and communications technology (ICT), an important part of African economic development and the workforce. [68] However, many African countries haven't taken part in ratifying the constitution, concerned that domestic cyber regulation from the convention won't take into account human rights protections in the UDHR.

In 2004, the General Assembly First Committee installed the Group of Governmental Experts (GGE) to report on Developments in the Field of Information and Telecommunications in the Context of International Security.[69] Since 2004, "six Groups of Governmental Experts (GGE) have studied the threats posed by the use of ICTs in the context of international security and how these threats should be addressed."[70] The GGE has met seven times and published four reports in 2010, 2013, 2015, and 2021. In the 2010 report, concerns around "increased reporting that States are developing ICTs as

[64] Council of Europe, *Convention on Cybercrime* (2001), available from https://rm.coe.int/1680081561.
[65] Council of Europe, *Convention on Cybercrime* (2001), available from https://rm.coe.int/1680081561.
[66] Council of Europe, *Chart of signatures and ratifications of Treaty 185* (2017), available from https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/chart-of-signatures-and-ratifications-of-treaty-185-%E2%80%93convention-on-cybercrime-%28status-as-of-16-06-2016%29.pdf.
[67] African Union, *African Union Convention on Cyber Security and Personal Data Protection* (2014), https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
[68] Mailyn Fidler and Fadzai Madzingira, "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity," Council on Foreign Relations, June 22, 2015, https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity.
[69] Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012," ICT for Peace Foundation, 2012, pp. 5-6, https://citizenlab.ca/cybernorms2012/ungge.pdf.
[70] "Developments in the field of information and telecommunications in the context of international security," United Nations Office for Disarmament Affairs, United Nations, Accessed on August 31, 2022, https://www.un.org/disarmament/ict-security/.

instruments of warfare and intelligence, and for political purposes"[71] were brought up, calling for recommendations around digital accountability and standards. Other important aspects include the coordination of international law with ICTs and cyberspace, state sovereignty, international cooperation, and information sharing to build capacity. By publishing these guidelines, countries have been able to gather information regarding potential solutions moving forward. However, no substantial international consensus has been made for how these solutions should be put into practice.

[71] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2010), available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement.

Possible Solutions

It is important for delegates to keep the following in mind when brainstorming solutions to cybersecurity threats:

1. What can be done in order to better monitor cyberspace on an international and regional scale?

2. How can international criminals be held accountable for cybercrimes?

3. What practices can be put into place to ensure a free, but safe, Internet?

One of the biggest problems with understanding and researching solutions to monitoring cyberspace is the sheer volume of data that comprises the Internet. Therefore, it's impossible to monitor absolutely everything. Historically, the United States has created more concrete systems for monitoring cyberspace, but these have run into some problems within the international community. While some nations view the U.S. as the greatest protector of cyberspace, others view it as its greatest threat. Increasingly, individuals have become more worried about privacy issues and leaks of government information from Edward Snowden, and US spying practices on foreign leaders have only increased this worry.[72] Additionally, some countries are concerned that the U.S. has a large monopoly on cyberspace ownership, as many servers for the Internet originate from the U.S.

Increasingly, it has been argued that the Internet needs to be governed by an international agency which is responsible for answering to the international system as a whole and not individual parties. The Non-Aligned Movement has expressly stated the need for independent control of some parts of their internet to guarantee the protection of defense secrets as well as the ability to guarantee

[72] "NSA boss: We lost trust with allies after Snowden leaks," The Australian, Accessed August 31, 2022, https://www.theaustralian.com.au/subscribe/news/1/?sourceCode=TAWEB_WRE170_a&dest=https%3A%2F%2Fwww.theaustralian.com.au%2Fnational-affairs%2Fforeign-affairs%2Fnsa-boss-we-lost-trust-with-allies-after-snowden-leaks%2Fnews-story%2F8b0e14e1c0e8ee4182727886o3c55a9c&memtype=anonymous&mode=premium&v21=dynamic-groupb-test-noscore&V21spcbehaviour=append.

internet use for the growth of their economy.[73] However, the makeup of such a body is still being debated.

Another major problem with guaranteeing cybersecurity is the issue concerning how to hold nations and international actors accountable for their actions. Nations like Russia[74] and China[75] believe cyberspace should be controlled locally by various national governments and should respect cultural norms and national policy agendas if a state determines the need for this. In much of the West, people believe in a free Internet, but in less democratic countries, leaders may feel threatened by a free internet and wish to control it directly.

Coincidentally, this has sparked debate around the world about how much freedom individuals are willing to give up in order to maintain security online. Originally, the Internet was a completely free, relatively safe place, but as technology has become more widespread and available, dangers have arisen, driving a debate concerning how much freedom should be allowed in cyberspace. If governments took more control over cyberspace, they could be more effective in improving cybersecurity, but there is a risk they would also decrease the level of freedom permissible on the Internet. This debate is especially pertinent in the European Union where individuals are asking where to draw the line between security and freedom of expression. Through increased internationally agreed upon regulation, greater collaboration between nations in terms of catching perpetrators and imposing regulations, and more communication about technological advancements in the realm of cyberspace on an international scale, countries can begin to maintain security, while guaranteeing a safe digital platform.

There are many challenges to creating an international framework for cybersecurity. Though the challenges are great, the potential danger of not doing anything is far greater. The problems posed

---

[73] "Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment," United Nations Meetings Coverage and Press Relations, October 28, 2014, http://www.un.org/press/en/2014/gadis3512.doc.htm.

[74] Tim Maurer, "Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security," Harvard Kennedy School Belfer Center, September 2011, https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

[75] People's Republic of China Mission to the United Nations, *Statement by H.E. Ambassador Wu Haitao, Head of the Chinese Delegation at the General Debate of the First Committee of the 68th Session ofthe United Nations General Assembly* (2013), available from https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/special/meetings/firstcommittee/68/pdfs/GD_8-Oct_China.pdf.

by cybercrime are serious, but they are solvable. It is hoped the international community can put aside their differences and create a free and open Internet that is safe from cybercrime.

Bloc Positions

Asia Pacific

In 2021, Asia was the most targeted region for cybersecurity attacks and accounted for one in four of all cybersecurity attacks across the world. Australia, India, and Japan reported the most incidents in the area, with server access and ransomware as the most popular forms of cyberattacks.[76] Investing in cybersecurity infrastructure in the Asia Pacific region has increased, however, with cybersecurity spending making up 11% of 2022 technology budgets.[77] Although the presence of the Dark Web is relatively small compared to the West, the Asia Pacific's accelerating technology adoption makes the region a more lucrative target for cybercrime. The Asia Pacific should bolster its cybersecurity infrastructure to support the growth of its digital economies.

Africa

States across Africa generally lack sufficient cybersecurity measures. Recent rises in digital attacks have included "sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups."[78] A recent Interpol report revealed that around 90 percent of African businesses operate without adequate cybersecurity protocols, making them vulnerable to cyberattacks.[79] In October 2020, a major hack affected Uganda's mobile money network. Hackers targeted the country's telecoms and banking sectors and reportedly stole at least $3.2 million.[80] Earlier that year, in June, a cyberattack struck South Africa's second-largest hospital operator in the middle of the COVID-19 pandemic.[81] As of June 2020, South Africa reported the third-highest number of cybercrime victims across the

[76] Eileen Yu, "Asia most targeted region in 2021, taking on one in four cybersecurity attacks," ZDNet, February 24, 2022, https://www.zdnet.com/article/asia-most-targeted-region-in-2021-taking-on-one-in-four-cybersecurity-attacks/.
[77] "The Future of Cybersecurity in Asia Pacific and Japan," Sophos, March 31, 2022, https://assets.sophos.com/X24WTUEQ/at/f3vctf7kcmj7rp3xrb3k73/sophos-future-of-cybersecurity-apj-2022-wp.pdf.
[78] "Are African countries doing enough to ensure cybersecurity and Internet safety?" Intentional Telecommunication Union, September 1, 2021, https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/.
[79] Robinson Sibe, "Africa's Chaotic Legal And Regulatory Cybersecurity Landscape Requires Harmonization," Forbes, August 2, 2022, https://www.forbes.com/sites/forbestechcouncil/2022/08/02/africas-chaotic-legal-and-regulatory-cybersecurity-landscape-requires-harmonization/?sh=4e540f51a9ab.
[80] Landry Signé and Kevin Signé, "How African states can improve their cybersecurity," Brookings Institution, March 16, 2021, https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/.
[81] Ibid.

globe.[82] In Africa, cybercrime was reported to have reduced GDP within the continent by over 10 percent, or an estimated $4.12 billion in 2021.[83] Generally, the number of qualified cybersecurity professionals with the resources to respond to online threats is lacking. Nevertheless, there have been efforts to improve cybersecurity structures as countries have passed legislation promoting cybersecurity. Furthermore, of the 131 Computer Emergency Response Teams (CERTs) established internationally, only 19 of them are based in Africa. 6 of those 19 were created between 2018 and 2020, however, showing the recent growth.[84] Efforts to continue strengthening African cybersecurity should be taken.

Europe

Countries in Europe make up 18 of the top 20 places in the global cybersecurity index.[85] The European Union cybersecurity market is expansive and increasing each year, and over 60,000 cybersecurity companies can be found across the area. The EU Agency for Cybersecurity (ENISA), formed in 2004, works closely with member states to advance cybersecurity technologies and develop responses to cybersecurity crises.[86] Furthermore, the EU Cybersecurity Act, established in 2019, introduced a "single EU-wide certification framework" that provided a "comprehensive set of rules, technical requirements, standards, and procedures."[87] This streamlined the fragmented barriers from the status quo of different countries using different security certification schemes. In December 2020, the European Commission and the European External Action Service (EEAS) also developed a new cybersecurity strategy for the EU.[88] The proposal aimed to strengthen Europe's responses to cyberattacks through regulation, investments, and policy. While countries in Europe generally have advanced cybersecurity measures, Dark Web marketplaces continue to flourish with

[82] Adeboye Adegoke, Bridget Boakye, and Melanie Garson, "Cybersecurity in Africa: What Should African Leaders Do to Strengthen the Digital Economy?" Tony Blair Institute, January 24, 2022, https://institute.global/policy/how-rethink-cybersecurity-africa-strengthen-digital-economy.
[83] Ibid.
[84] "Are African countries doing enough to ensure cybersecurity and Internet safety?" Intentional Telecommunication Union, September 1, 2021, https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/.
[85] "Cybersecurity: how the EU tackles cyber threats," European Council and Council of the EU, accessed August 28, 2022, https://www.consilium.europa.eu/en/policies/cybersecurity/.
[86] European Union Agency for Cybersecurity, accessed August 28, 2022, https://www.enisa.europa.eu/.
[87] "Cybersecurity: how the EU tackles cyber threats," European Council and Council of the EU, accessed August 28, 2022, https://www.consilium.europa.eu/en/policies/cybersecurity/.
[88] Ibid.

drugs being bought and sold in high volumes. In 2021, international law enforcement agencies coordinated by Europol shut down DarkMarket, the world's largest Dark Web marketplace. Nevertheless, the takedown also serves as a reminder of the resilience of Dark Web marketplaces, as more platforms continue to rise and take the place of the dismantled ones. European states, besides combating criminal activity on the Dark Web, can also protect private citizens' and companies' data through streamlined cybersecurity strategies.

North America

Growing cyber threats have pushed the United States, Canada, and Mexico to all prioritize cybersecurity and enact measures to identify key cyber assets.[89] The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has specifically zeroed in on international collaboration, and in 2021, CISA released its first international strategy: CISA Global. CISA Global aims to strengthen global policy and engagement to strengthen cybersecurity infrastructure across the world.[90] Mexico also faces significant cybersecurity difficulties, as cyberattacks on Mexican institutions and individuals have undermined financial sectors and their functions.[91]

Latin America and the Caribbean

While Latin America and Caribbean countries have improved their approaches to cybersecurity, the region continues to endure high levels of cybercrime. The COVID-19 pandemic saw a surge in the use of digital services, and in 2020, mobile data traffic grew by 25 percent and over 50 million Latin Americans became online consumers.[92] This increase in digital services also facilitated more opportunities for computer viruses, phishing scams, and other types of cybercrime. Groups with

[89] Luisa Parraguez, Paul Stockton, and Gaéton Houle, "Cybersecurity and Critical Infrastructure Resilience in North America," Wilson Center, accessed August 28, 2022, https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Cyber%20Security%20and%20Critical%20Infrastructure%20in%20North%20America.pdf.
[90] "Fact Sheet: DHS International Cybersecurity Efforts," U.S. Department of Homeland Security, April 21, 2022, https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts.
[91] Luisa Parraguez, Paul Stockton, and Gaéton Houle, "Cybersecurity and Critical Infrastructure Resilience in North America," Wilson Center, accessed August 28, 2022, https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Cyber%20Security%20and%20Critical%20Infrastructure%20in%20North%20America.pdf.
[92] "Going Digital: Privacy & Cybersecurity in Latin America," Wilson Center, August 3, 2021, https://www.wilsoncenter.org/event/going-digital-privacy-cybersecurity-latin-america.

financial motives have targeted organizations across the area, usually with ransomware.[93] Furthermore, criminal networks based on Latin America and the Caribbean have taken full advantage of the anonymity and privacy afforded by Dark Web platforms.[94] Some countries have begun taking steps to address cybersecurity issues, like Brazil's publication of its first national cybersecurity strategy in 2020, but more coordination and initiatives are needed.[95]

[93] Simon Handler, "The 5×5—The state of cybersecurity in Latin America," Atlantic Council, December 9, 2021, https://www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-iån-latin-america/.
[94] Timothy L. Quintero, "The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime," Insight Crime, September 13, 2017, https://insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/.
[95] Simon Handler, "The 5×5—The state of cybersecurity in Latin America," Atlantic Council, December 9, 2021, https://www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-iån-latin-america/.

Glossary

Advanced Research Projects Agency Network (ARPANET): The origins of the modern Internet; started as an experimental computer network and communications system that allowed for users to share information between devices

Cryptocurrency: Digital currency; essential for online transactions made in the Dark Web

Cybersecurity: The practice of protecting information and its systems and infrastructure from digital attacks

Dark Web: A subset of the Internet used especially for anonymous activity and privacy

Global Cybersecurity Agenda (GCA): Serves as a practical framework for international collaboration on cybersecurity; established by the International Telecommunications Union (ITU)

Group of Governmental Experts (GGE): UN-mandated working group of 15 experts appointed by the Secretary-General examining potential and existing cyber threats.

Onion routing: A technique that anonymously routes Internet traffic through multiple servers while enclosing messages in layers of encryption; allows for anonymous communication

Tor: Network that allows for anonymous Internet activity and communication; also known as The Onion Router

Bibliography

02 UN ITU. *Global Cybersecurity Agenda (GCA)*, 2007. available from https://www.itu.int/ITU-D/cyb/events/2007/Geneva/docs/kitaw-global-cybersecurity-agenda-geneva-17-sept-07.pdf.

Adegoke, Adeboye, Bridget Boakye, and Melanie Garson. "Cybersecurity in Africa: What Should African Leaders Do to Strengthen the Digital Economy?" Tony Blair Institute. January 24, 2022. https://institute.global/policy/how-rethink-cybersecurity-africa-strengthen-digital-economy.

African Union, *African Union Convention on Cyber Security and Personal Data Protection*, 2014. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

Austin, Kristin. "The Origins and History of the Dark Web." IdentityIQ. October 17th, 2019. https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/.

Cost of a Data Breach Report. IBM Security, 2019. https://www.ibm.com/downloads/cas/ZBZLY7KL.

Council of Europe. *Chart of signatures and ratifications of Treaty 185*, 2017. available from https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/chart-of-signatures-and-ratifications-of-treaty-185-%E2%80%93convention-on-cybercrime-%28status-as-of-16-06-2016%29.pdf.

Council of Europe. *Convention on Cybercrime*, 2001. available from https://rm.coe.int/1680081561.

European Union Agency for Cybersecurity. Accessed August 28, 2022. https://www.enisa.europa.eu/.

Fidler, Mailyn and Madzingira, Fadzai. "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity." Council on Foreign Relations. June 22, 2015. https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity.

Guccione, Darren. "What is the dark web? How to access it and what you'll find." CSO Online. IDG Communications, July 1, 2021. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

Handler, Simon. "The 5×5—The state of cybersecurity in Latin America." Atlantic Council. December 9, 2021. https://www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-iån-latin-america/.

Hern, Alex. "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017." The Guardian. Guardian News & Media Limited, December 30, 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

Kastner, Erica. "History of the Dark Web [Timeline]." Standard Office Systems. February 7, 2020. https://www.soscanhelp.com/blog/history-of-the-dark-web.

Khandelwal, Swati. "Baltimore City Shuts Down Most of Its Servers After Ransomware Attack." The Hacker News. May 8, 2019. https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html.

Kumar, Aditi and Rosenbach, Eric. "The Truth About the Dark Web." International Monetary Fund. Accessed August 28, 2022. https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar#:~:text=In%20the%20late%201990s%2C%20two,accessible%20to%20ordinary%20internet%20surfers.

Lanterman, Mark."Some Thoughts on the Dark Web—and How It Affects You." International Risk Management Institute. March 2018. https://www.irmi.com/articles/expert-commentary/some-thoughts-on-the-dark-web.

Macaskill, Ewen and Dance, Gabriel. "NSA Files: Decoded." The Guardian. November 1, 2013. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Maurer, Tim. "Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security." Harvard Kennedy School Belfer Center. September 2011. https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

Nickm. "Tor: 80 percent of ??? percent of 1-2 percent abusive." Tor Blog. Tor Browser, December 30, 2014. https://blog.torproject.org/tor-80-percent-percent-1-2-percent-abusive/.

Parraguez, Luisa, Paul Stockton, and Gaéton Houle. "Cybersecurity and Critical Infrastructure Resilience in North America." Wilson Center. Accessed August 28, 2022. https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Cyber%20Security%20and%20Critical%20Infrastructure%20in%20North%20America.pdf.

People's Republic of China Mission to the United Nations, *Statement by H.E. Ambassador Wu Haitao, Head of the Chinese Delegation at the General Debate of the First Committee of the 68th Session of the United Nations General Assembly*, 2013. available from https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/special/meetings/firstcommittee/68/pdfs/GD_8-Oct_China.pdf.

Polityuk, Pavel, Vukmanovic, Oleg and Jewkes, Stephen. "Ukraine's power outage was a cyber attack: Ukrenergo." Reuters. January 18, 2017. https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.

Power, Mike. "Online highs are old as the net: the first e-commerce was a drugs deal." The Guardian. April 19, 2013. https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal.

Quintero, Timothy L. "The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime." Insight Crime. September 13, 2017.

https://insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/.

Ranjithsiji. "Deepweb graphical representation like iceberg." Wikipedia. April 17, 2018. https://commons.wikimedia.org/wiki/File:Deepweb_graphical_representation.svg.

Sibe, Robinson. "Africa's Chaotic Legal And Regulatory Cybersecurity Landscape Requires Harmonization." Forbes. August 2, 2022. https://www.forbes.com/sites/forbestechcouncil/2022/08/02/africas-chaotic-legal-and-regulatory-cybersecurity-landscape-requires-harmonization/?sh=4e540f51a9ab.

Singé, Landry and Signé, Kevin. "How African states can improve their cybersecurity." Brookings Institution. March 16, 2021. https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/.

"Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs." National Institute of Justice. June 15, 2020. https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs.

Tikk-Ringas, Eneken. "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012." ICT for Peace Foundation. 2012. pp. 5-6. https://citizenlab.ca/cybernorms2012/ungge.pdf.

United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2010. available from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement.

Yu, Eileen. "Asia most targeted region in 2021, taking on one in four cybersecurity attacks." ZDNet. February 24, 2022. https://www.zdnet.com/article/asia-most-targeted-region-in-2021-taking-on-one-in-four-cybersecurity-attacks/.

"Are African countries doing enough to ensure cybersecurity and Internet safety?" Intentional Telecommunication Union. September 1, 2021. https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/.

"Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment." United Nations Meetings Coverage and Press Relations. October 28, 2014. http://www.un.org/press/en/2014/gadis3512.doc.htm.

"Cybersecurity: how the EU tackles cyber threats." European Council and Council of the EU. Accessed August 28, 2022. https://www.consilium.europa.eu/en/policies/cybersecurity/.

"Developments in the field of information and telecommunications in the context of international security." United Nations Office for Disarmament Affairs. United Nations, Accessed on August 31, 2022. https://www.un.org/disarmament/ict-security/.

"Fact Sheet: DHS International Cybersecurity Efforts." U.S. Department of Homeland Security. April 21, 2022. https://www.dhs.gov/news/2022/04/21/fact-sheet-dhs-international-cybersecurity-efforts.

"Going Digital: Privacy & Cybersecurity in Latin America." Wilson Center. August 3, 2021. https://www.wilsoncenter.org/event/going-digital-privacy-cybersecurity-latin-america.

"ITU Explainer: Cybersecurity." GP Digital. Accessed August 31, 2022. https://www.gp-digital.org/wp-content/uploads/2018/08/ITU_Explainers_cybersecurity.pdf.

"NSA boss: We lost trust with allies after Snowden leaks." The Australian. Accessed August 31, 2022. https://www.theaustralian.com.au/subscribe/news/1/?sourceCode=TAWEB_WRE170_a&dest=https%3A%2F%2Fwww.theaustralian.com.au%2Fnational-affairs%2Fforeign-affairs%2Fnsa-boss-we-lost-trust-with-allies-after-snowden-leaks%2Fnews-story%2F8b0e14e1c0e8ee4182727886o3c55a9c&memtype=anonymous&mode=premium&v21=dynamic-groupb-test-noscore&V21spcbehaviour=append.

"Our Mission." Freedom Online Coalition. Accessed August 31, 2022. https://freedomonlinecoalition.com/.

"The CERT Division." Software Engineering Institute, Carnegie Mellon University. Accessed August 28, 2022. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

"The fascination evolution of cybersecurity." La Trobe University. Accessed August 28, 2022. https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/.

"The Future of Cybersecurity in Asia Pacific and Japan." Sophos. March 31, 2022. https://assets.sophos.com/X24WTUEQ/at/f3vctf7kcmj7rp3xrb3k73/sophos-future-of-cybersecurity-apj-2022-wp.pdf.

"Tor usage worldwide: The Anonymous Internet." Digitale Gesellschaft. June 21, 2017. https://www.digitale-gesellschaft.ch/2017/06/21/tor-usage-worldwide-the-anonymous-internet-new-infographic/.

"What Is a Cyberattack?" Cisco. Cisco Systems, Accessed August 31, 2022. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.