Florida High Schools Model United Nations

FHSMUN 45

United Nations Office on Drugs and Crime (UNODC)

Cyber Security and the Right to Privacy in the Digital Age

Contributors: Isaiah Sloan, Brian D. Sutliff & Sasha Ahles

Updated December 2023

"We believe that privacy is a fundamental human right, one that is essential to our vision of a world where technology enriches people's lives. And to help create that world, we are fighting for privacy in multiple areas of our work. We've long said that security is the foundation of privacy—because there is no privacy in a world where your private data can be stolen with impunity. Never before has this threat been more profound, or its consequences more visible…"

Tim Cook, Apple CEO

"But, I think there's something else a little more telling. You know, when you were asked about Chinese censorship, you pivoted immediately to drug use in Singapore. You have absolutely tied yourself in knots to avoid criticizing the CCP's treatment of the Uyghur population, and I think it begs the first question…if the CCP demanded that ByteDance hand over all of the data that they had on U.S users in their possession, and ByteDance refused, I wonder what would happen? Yet, the core concern is that it proposes unparalleled integration with the U.S. government with a private company, which will require significant government resources. All of that allows the continued operation of a social media platform with serious National Security implications. CFIUS's workloads have already dramatically increased in recent years, with a 30 percent increase in declarations and a 45 percent increase in joint voluntary notices. And there's bipartisan consensus that CFIUS needs to be expanded as we speak."

Congressman Kelly Armstrong (R-ND)

"A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves, an unrecorded, unanalyzed thought. And that's a problem because privacy matters. Privacy is what allows us to determine who we are and who we want to be."

–Edward Snowden, Former USNSA Contractor

COMMITTEE BRIEF

Introduction

While cybercrime does not have an established international definition, the UN Office on Drugs and Crime (UNODC) classifies it as "offenses [that] typically cluster around the following categories: offenses that are computer-related and content-related, and offenses related to infringements of copyright."[1] In a day and age where we heavily rely on the Internet and its uses, we have become more susceptible to these emerging transnational crimes, and the complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organized crime groups.[2] An ever-growing problem for everyone, it is critical to identify what constitutes a cybercrime. "Cybercrime exists in many forms, the most common being identity-related offenses. This occurs by 'phishing' (deceiving Internet users into giving their personal information), the dissemination of 'malware' (software that disrupts computer systems and collects personal or sensitive information), and hacking (illegally accessing someone's computer remotely)."[3] These methods are primarily used for stealing credit card information and money. However, more severe and advanced offenses have begun to emerge. According to the recent Study on the effects of new information and technology conducted by the UNODC, "The Internet has become a breeding ground for criminal activity related to copyright and intellectual property rights, as well as offenses such as child pornography and abuse material.[4]

In the wake of the September 11, 2001 attacks on New York City and Washington, DC, the United States (US) Congress passed the USA Patriot Act that dramatically expanded the government's ability to obtain data about individuals' call records, medical histories, financial information, and Internet search queries.[5] Legal challenges to the USA Patriot Act were swift. However, the ultimate resolution of the US government's ability to investigate peoples' digital footprints without obtaining a warrant remains an open question. The US is only one of dozens of countries that are currently grappling with balancing peoples' right to privacy and the emphasis of law enforcement officials on obtaining information related to potential criminal and even terrorist actions. In December 2015, the European Union (EU) approved new legislation aimed at clarifying and strengthening important provisions about an individual's right to privacy, including the so-called "right to be forgotten,"5a relatively recent provision in European law where individuals may request that digital records and references from beyond a certain number of years may be erased. While the right to be forgotten has been accepted by digital privacy advocates, other observers have voiced concerns about individuals potentially expunging relevant, albeit embarrassing, information, particularly when seeking employment, business and personal loans, or even public office.[6]

The Current Scale of the Issue

---

[1] United Nations. (2022, June 23). *A UN treaty on cybercrime en route*.
[2] *Emerging Crimes*, UNODC
[3] *DOHA: UN Conference weighs efforts to combat cybercrime, create safer digital world*
[4] "Study on the Effects of New Information Technologies on Abuse and Exploitation of Children." UNODC, 2015.
[5] *USA PATRIOT Act | FinCEN.gov*. (n.d.).
[6] Padova, Y. (2019). Is the right to be forgotten a universal, regional, or 'glocal' right? *International Data Privacy*

There are more than 5.3 billion active Internet users all around the world. To put this number in perspective, that accounts for about 65.4% of the global population.[7] The Internet has become a crucial aspect of our day-to-day lives. The Internet was created amidst the Cold War to allow government officials and researchers to publish and share information.[8] Nearly 60 years later, one can pick up a phone and access various social media platforms that connect the world to a limitless discussion platform. People can also use that same device to go to Amazon and purchase whatever they think of, whether they need it or not. They can even connect to millions of players worldwide on their favorite multiplayer video game. While these developments in the Internet sector seem like world-changing things, they also come with various drawbacks. While 65.4%[9] of the world has access to the Internet, which can be used to complete various tasks depending on the capability of their network, those same 5.3 billion people are susceptible to cyberattacks that can lead to multiple harmful things down the road. The online world has become an ideal space for criminals due to the enormous victim pool and the ability to maintain anonymity while gaining access to information that is often knowingly, but also quite frequently unwittingly, stored online.[10] In 2022 alone, the Federal Bureau of Investigation (FBI) received over 800,944 registered complaints of cybercrime/attacks[11] With this in mind, recent studies project that nearly 33 billion accounts will be breached in 2023, with the cost of these breaches predicted at 8 trillion dollars.

While these statistics may seem alarming at face value, we must also understand that these statistics only represent one nation, and these statistics are attacks that were officially reported and filed.[12] Many of these cyber crimes go unreported because many people do not know they are victims of these attacks. Many (33%) of those who make up the online space are people under 25, including minors,[13] whose data can easily be breached if proper measures are not taken. As technology and its availability continue to grow, so does the reach of cybercrime. In 2022, there were 87 mobile broadband subscriptions per 100 inhabitants worldwide. Subscriptions continue to grow at a rate of 6%[14] According to a report published by the US National Library of Medicine, titled Increasing Cybercrime Since the Pandemic, it has been reported that since the COVID pandemic, “many cybercrimes increased by at least 10% in all age groups, including phishing by text, online shopping scams, and romance scams”[15]. This growth creates a pressing need to address the issue immediately. Perpetrators of cybercrime and their victims can be located in different regions, and its effect can ripple through societies worldwide, highlighting the need to mount an urgent, dynamic, and international response. While advertising and news stories frequently focus on the problems consumers pose by cybercrime, large-scale public and private institutions are also often targeted, mainly because of the enormous monetary and informational resources at risk.

Cyberterrorism and the Threat to States

Acts of terror have long since been a threat to countries across the globe. However,

---

[7] Shewale, R. (2023, October 21). Internet User Statistics in 2023 — (Global Demographics).
[8] *A brief history of the Internet*. (n.d.).
[9] Shewale, R. (2023, October 21). Internet User Statistics in 2023 — (Global Demographics).
[10] *Anonymity and identity shielding | eSafety Commissioner*. (n.d.). eSafety Commissioner.
[11] *Internet Crime Complaint Center releases 2022 statistics*. (2023, March 23). Federal Bureau of Investigation.
[12] Palatty, N. J. (2023, October 26). 90+ Cyber Crime Statistics 2023
[13] Atske, S. (2023, December 11). *Teens, Social Media and Technology 2022 | Pew Research Center*. Pew Research
[14] Mobile Broadband Subscriptions Continue to Grow Strongly, ITU, February 2023
[15] Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, *23*(4). (2021)

technological advancement has given a whole new aspect to terrorism that was not previously existent or highlighted. The September 11, 2001 attacks "prompted the start of an intensive discussion about the use of information and communication technologies (ICTs) by terrorists,"[16] with reports showing that the offenders used the Internet in preparation for the attacks.[17] The UNODC has observed that "computer systems may be used for a range of acts that promote and support terrorism,"[18]including propaganda (recruitment, radicalization, and incitement to terrorism); financing; training; planning (through secret communication and open source information); execution; and cyberattacks.[19]

Attacks against critical information infrastructures have widely been recognized as a potential target for terrorist attacks. As reliance on information technology grows, so does the vulnerability of these essential structures of information, remarkably interconnected systems linked by computer and communication networks.[20] "Infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defense or economic security of a state,"[21] such as electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, and emergency services. Massive disruptions to systems are not necessary to achieve catastrophic results. Disruptions caused by a network-based attack go further than the failure of a single system, as even short interruptions to services can cause substantial financial damage to e-commerce businesses for civil services and military infrastructure and services. An attack on any of these critical information structures can prove to be a dangerous threat to a state, not only due to the attack's consequences but also because it makes the person(s) or group behind the crime all the more elusive. Cyber attacks allow defenders to be absent from "the scene of the crime" as they use anonymous communication and encryption technology to conceal their identity while carrying out the attack.

We must also identify the significant threat of cyber attacks in war, as most developed nations rely on satellite and radar communication to operate their weapon and defense systems. A recent example of cyber terrorism comes in the wake of the two-year raging war in Ukraine. On December 12th, 2023, Ukraine announced that its largest mobile network was the victim of a large-scale cyber-terrorist attack, which resulted in millions of Ukrainian citizens losing connection to the outside world.[22] The cyberattack on "Kyivstar" –which provides more than half of Ukraine's population with cell service – suffered widespread outages, affecting millions of citizens who could no longer receive alerts of potential Russian airstrikes.[23] The company's Chief Executive Officer Oleksandr Komarov said the attack was "a result of" the war with Russia. "War is also happening in cyberspace. Unfortunately, we have been hit as a result of this war: [The attack] significantly damaged [our] infrastructure and limited access; we could not counter it at the virtual level, so we shut down Kyivstar physically to limit the enemy's access." These cyber-attacks are dangerous to our online presence and data and can harm our physical well-being during war.[24] Without proper action, millions more will be put at risk in the future as

---

[16] (*Information and Communications Technologies | Security Council - Counter-Terrorism Committee (CTC)*, n.d.)
[17]*Cybersecurity | Understanding cybercrime: Phenomena, Challenges and Legal Response*
[18] (*Information and Communications Technologies | Security Council - Counter-Terrorism Committee (CTC)*, n.d.)
[19]Poliveiraa. (n.d.). *Cybercrime Module 14 Key issues: Cyberterrorism*.
[20]*Cyber attacks on critical infrastructure*. (n.d.). Allianz Commercial.
[21] (Under Secretary of Defense for Policy, n.d.)
[22] Hunder, M., Landay, J., & Bern, S. (2023, December 13). Ukraine's top mobile operator hit by cyberattack of war.
[23] Hunder, M., Landay, J., & Bern, S. (2023, December 13). Ukraine's top mobile operator hit by cyberattack of war.
[24] Hunder, M., Landay, J., & Bern, S. (2023, December 13). Ukraine's top mobile operator hit by cyberattack of war.

acts of cyberterrorism will only further evolve into more destructive and nation crippling.

Who Needs Privacy When Everything is Already Compromised?

Cybercrime is a rapidly rising threat to citizens of the global community. With techniques and methods constantly growing and evolving, trudging through the potential threats to one's data becomes riskier. In 2020, the FBI received more than 2,000 Internet crime complaints per day.[25] While the growing number of cyber attacks is occurring globally, certain areas of the world, such as Africa and Brazil,[26] seem to be experiencing growth more than other regions. Internet usage is rising rapidly in Africa, and with it, cybercrime.[27] The growth has given criminals incredible ease when attacking users, "creating a new pool of potential victims." Cybercrime has not only grown in number, but it has expanded in its means of attack.[28] Cybercrime in Africa has moved far beyond the notorious 419 email scam, which promised riches in exchange for cash and bank details, "with gangs embracing more sophisticated ways to use technology, such as malware and bonnets, to get what they want."[29]

As most top security firms worldwide noted, these risks have made logging onto the Internet dangerous for many. The Norton security firm has stated that 70% of South Africans have fallen victim to cybercrime, compared to 50% worldwide.[30] McAfee, a cyber security firm, reported that cybercrime cost South African companies more than $500 million in 2014.

Combating Cybercrime and the Threat to Privacy

Globally, organizations spent around $150 billion in 2021 on cybersecurity.[31]With the rates for cyber attacks rising and the cost to users and companies, the need for a solution has never been greater. Combating crime in all forms comes with challenges, although the concerns facing those looking to combat cybercrime are unique.

Law enforcement's challenges are based on privacy-based protections within international and national law. The International Covenant on Civil and Political Rights (ICCPR) and the European Convention for Protection of Human Rights and Fundamental Freedoms (ECHR), among others, all have "prohibitions on arbitrary interference with privacy, family, home and correspondence."[32] Privacy rights in international law – much like most other rights – are not absolute and, therefore, subject to limitations. For example, in the ECHR, specifically for "the prevention of disorder or crime," the definition of conditions and circumstances under which investigative powers can be used, the identity of authorizing officials, and the length of time investigative measures may be applied are all critical to the human rights assessment of whether or not criminal investigations that infringe privacy are acceptable as lawful and necessary.[33]In all parts of the world, to determine whether the interference with privacy, family, home, or correspondence is justified, "each investigative measure must be assessed in its own legal and practical context."[34] This grey area can become

---

[25] *Internet Crime Report*, FBI, March 2021
[26] Robert Muggah & Nathan Thompson, "Brazil's Cybercrime Problem" *Foreign Affairs.*
[27] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015.
[28] Wolf, A., & Wolf, A. (2023, October 19). *A brief history of cybercrime*. Arctic Wolf.
[29] Alspach, K. (2022, May 17). Why AI-powered ransomware could be "terrifying." *Protocol*.
[30] Tom Jackson, *Can Africa fight cybercrime and preserve human rights?*, BBC News, 10 April 2015.
[31] Andrew Burt, "*The Digital World Is Changing Rapidly.*", Harvard Business Review, 16 May 2023.
[32] *Human Rights and Privacy | American Civil Liberties Union*. (2022, February 15).
[33] *L_2021360EN.01006901.XML*. (n.d.).
[34] Gehl, R. (2017, August 1). *Chapter 1: Introduction*. Pressbooks.

problematic to law enforcement and impede their ability to conduct investigations on cybercrime as they tip-toe around privacy-based protections. “Case law from international human rights courts and tribunal emphasizes that procedural protections are critical to respecting privacy in the context of law enforcement investigations.”[35]These challenges grow exponentially when the crimes cross borders. “Divergent national privacy approaches will become an increasing challenge in the context of transnational law enforcement investigations and developments.”[36]

Tik-Tok…Your Data's Unlocked!

The rapidly growing social media platform “Tiktok” has recently come under fire as word of a large-scale data breach took place within the platform’s user data cloud. TikTok users worldwide grew alarmed as an anonymous hacker group under the name “AgainstTheWest” announced on Twitter (now X) that they had breached and gained access to an insecure cloud server and claimed to have now access to over 2.05 billion records and over 790GB of user data.[37] TikTok immediately released a statement discrediting the claim of the cloud breach, stating, “We have confirmed that the data samples in question are all publicly accessible and are not due to any compromise of TikTok systems, networks, or databases.”[38]While this statement may be somewhat true, Bob Diachenko, a threat intelligence researcher at Security Discovery, said that the breach is “real” and that the data is likely to have originated from “Hangzhou Julun Network Technology Co., Ltd rather than TikTok.”[39] Another widely known reporter on user data breaches, Troy Hunt, the founder and creator of “haveibeenpwned.com” (a website that allows users to screen if their data has been found online), stated that “some data is junk, but it could be non-production or test data. It is a bit of a mixed bag so far.”[40] The unconfirmable nature of this data breach is alarming as users are unaware if their data has been compromised and are not sure which steps should be taken in response. How can we damage control situations such as these when unaware of the validity and severity of said data breaches?

This unconfirmed data breach of the TikTok user data cloud caught the attention of the United States and its Congress. The question of American user data’s security came into question following the supposed data breach just a month before the House Energy and Commerce Committee subpoenaed Tiktok CEO Shou Zi Chew.[41] Members of this committee grew concerned over American user data and their own following this data breach. They were alarmed by the potential risk of TikTok’s parent company, Bytedance, which came under fire as an ex-employee claimed that the Chinese communist party (CCP) had an office within the company and oversaw many operations and may put American data at risk.[42]Cathy McMorris Rodgers (R-Wash), the committee chair of the House Energy and Commerce, opened the hearing with the following statement: “To the American people watching today, hear this: TikTok is a weapon by the Chinese Communist Party to spy on you and manipulate what you see and exploit for future generations,” This statement led to a near five hour back and forth between the

---

[35] *Criminal accountability of United Nations officials, experts on mission Crucial when administering justice, combating impunity, Sixth Committee hears | UN Press*. (2021, October 12).

[36]*Digital Divergence | Constitution Center*. (n.d.). National Constitution Center

[37] The Hacker News. (n.d.). *TikTok denies data breach reportedly exposing over 2 billion users’ information*.

[38] The Cyber Express. (2023, May 26). TikTok denies breach of records. *The Cyber Express*.

[39] Bob Diachenko on X: “OK, #TikTokBreach is real. / X. (n.d.). X (Formerly Twitter).

[40] The Hacker News. (n.d.). *TikTok denies data breach reportedly exposing over 2 billion users’ information*.

[41] Kerr, D. (2023, March 23). Lawmakers grilled TikTok CEO Chew in a high-stakes hearing about the app. *NPR*.

[42] Wang, Y. (2023, March 24). Problem with TikTok’s Claim of Independence from Beijing. *Human Rights Watch*.

committee and Mr.Chew as he deflected and shut down any claims of Chinese interference with any user data especially within the United States. During this same hearing, Mr. Chew emphasized some measures that Tiktok is implementing to reduce further its US users' concerns over the security of their data. In recent months, TikTok announced "Project Texas," an initiative to store American user data on Oracle's cloud servers in the United States to ease concerns over potential Chinese government access to TikTok's data. TikTok CEO Shou Zi Chew says, "We are working with Oracle on new, advanced data security controls that we hope to finalize shortly."[43] He stated that the goal is to ensure that "100% of TikTok's American user data is stored by Oracle Cloud Infrastructure".[44]This move shows TikTok is taking steps to reduce risks around its Chinese ownership at a time when many US lawmakers and officials have raised alarms about the app's data privacy and security practices.

However, while storing US user data in the US through Project Texas is a first step, many experts argue that further actions are still needed before this system can be considered entirely trustworthy. Additional protections would need to be implemented, such as establishing "rules preventing Chinese employees from accessing data" and undergoing "regular third-party audits."[45]TikTok would also need to ensure that no data backups exist that could provide access from China. Some critics believe stricter measures should be explored, like limiting TikTok employees to those without ties to China.[46]Questions additionally persist around what metadata TikTok may still collect and if US user data could be accessed through ByteDance's Chinese products like Douyin.

Project Texas signifies TikTok's efforts to ease rising tensions, but substantial uncertainty remains regarding the enforcement and scope of this initiative. More transparency and accountability will build trust with US regulators and users concerned about Chinese affiliations' influence on TikTok's sensitive data handling. The coming months will be crucial as TikTok aims to implement and strengthen the data protection protocols underpinning Project Texas. The UNODC must utilize its expertise and global platform to promote transparency and accountability in social media data handling to urge companies like TikTok to codify and publish the data protection standards underpinning initiatives such as Project Texas.

Meme Money Mayhem: From DOGE to Disaster

Cryptocurrencies like Bitcoin and Ethereum have exploded in popularity and value in recent years, with the total crypto market cap peaking at over $3 trillion in 2021.[47]However, cryptocurrencies' largely unregulated and decentralized nature has also given rise to new avenues for cyber crimes against unsuspecting investors. A cryptocurrency is a digital currency that uses cryptography to secure and verify transactions.[48] Without a central authority like a bank or government regulating it, cryptocurrency operates on distributed ledger technology called blockchain, which allows digital information to be distributed across a network but not copied. While this innovative system has some merits, the lack of oversight leaves gaps for criminals to carry out schemes and scams.[49]

A prime example is the 2022 collapse of cryptocurrency exchange FTX and its affiliated

---

[43] Shepardson, D., & Wang, E. (2022, July 1). TikTokaims to reassure U.S. lawmakers on data security. *Reuters*.
[44] Shepardson, D., & Wang, E. (2022, July 1). TikTokaims to reassure U.S. lawmakers on data security. *Reuters*.
[45] Treisman, R. (2022, November 17). The FBI alleges TikTok poses national security concerns. *NPR*.
[46] Hadero, H. (2023, March 17). Why TikTok's security risks keep raising fears | AP News. *AP News*.
[47] Ossinger, J. (2021, November 8). Bitcoin ($BTC USD), lead crypto to $3 trillion market cap. *Bloomberg.com*.
[48] Frankenfield, J. (2023, November 4). *Cryptocurrency explained with pros and cons for investment*. Investopedia.
[49] Hayes, A. (2023, December 15). *Blockchain Facts: What is it, how it works, and how it can be used*. Investopedia.

trading firm Alameda Research, headed by Sam Bankman-Fried. FTX raised over $1.8 billion from venture capitalists and was valued at $32 billion at its peak.[50] FTX then abruptly declared bankruptcy on November 11, 2022. An investigation revealed that Bankman-Fried had secretly transferred around $10 billion in FTX customer funds to Alameda Research, which had suffered substantial losses through trading and speculative investments.[51] Bankman-Fried used FTX customer accounts as his piggy bank to plug holes at his trading firm, Alameda. This self-dealing highlights lax oversight around crypto's conflicts of interest. Over 1 million customers and investors have likely lost money due to fraud and theft of deposits through FTX's liquidity issues.

Beyond scams aimed at investors, cryptocurrency is also increasingly used for illicit transactions, including illegal arms sales, drug deals, and human trafficking rings.[52] The blockchain ledger records these transactions, but counterparties remain pseudonymous behind wallet addresses. While law enforcement agencies have tools to "follow the money" with crypto, criminals utilize mixers and decentralized platforms to obscure the money trail across various cryptocurrencies and wallets.[53] This loophole impedes authorities' ability to crack down on underground markets and cybercrime rings exploiting cryptocurrencies to circumvent traditional payment systems. While increased regulation may restore some accountability, cryptocurrencies were intended to avoid centralized control. Nonetheless, additional consumer warnings could help curb deception, and policy discussions around tracing illicit crypto flows are warranted. Most importantly, investors should exercise skepticism when promised improbably high crypto returns to avoid being left holding the bag.[54]

UN System Actions

In the years since the UNODC first began addressing cybercrime capacity issues in developing nations in 2015,[55] the landscape of digital dangers has expanded dramatically in scale and sophistication. While the lack of cybersecurity resources remains an acute vulnerability in the Global South, new technologies like ransomware, data mining, and phishing scams have enabled more complex attacks against government and corporate cyberinfrastructure, even as more sensitive personal data becomes available to malign actors through unsecured online platforms.[56] Recognizing these growing and multifaceted threats, the UN adopted two resolutions in 2021, underscoring member states' commitments to enhancing cybersecurity while protecting privacy and human rights in digital spaces.[57] The General Assembly resolution on the promotion, protection, and enjoyment of human rights on the Internet affirmed the applicability of international human rights law to online activity and the responsibility of tech companies to respect user rights.[58] A separate Russia-sponsored resolution called upon governments to prevent using new technologies for criminal purposes while adhering to international law and avoiding infringing on civil liberties.

---

[50] *SEC.gov | SEC Charges Samuel Bankman-Fried in Crypto Asset Trading Platform FTX*. (2022, December 13).
[51] Berwick, A. (2022, November 13). At least $1 billion of client funds missing at failed crypto firm FTX. *Reuters*.
[52] *Virtual currency in human & drug trafficking increases, so do the challenges for law enforcement*. (2023, July 20).
[53] Financial Crime Academy. (2023, November 8). Understanding crypto money laundering methods:
[54] *SEC.gov | Exercise Caution with Crypto Asset Securities: Investor Alert*. (2023, March 23).
[55] Katharina.kiener-Manu. (n.d.). *Cybercrime Module 10 Key Issues: Cybercrime that Compromises Privacy*.
[56] (2022). *The Geneva Papers on Risk and Insurance - Issues and Practice*,
[57] *Cybersecurity and New Technologies | Office of Counter-Terrorism*. (n.d.).
[58] *UN: Human Rights Council adopts resolution on human rights on the Internet - ARTICLE 19* (2021, August 11).

Additionally, the UN counterterrorism architecture has ramped up efforts to prevent and respond to cyberattacks to disrupt essential infrastructure and institutions in member states.[59] After ransomware attacks orchestrated by organized cybercrime groups disabled Ireland's national healthcare IT systems in 2021, UN counterterrorism chief Vladimir Voronkov warned of the growing nexus between profit-driven hackers and extremist organizations who may exploit similar digital vulnerabilities for ideologically driven chaos.[60] Through multilateral policy initiatives, capacity-building projects, public-private partnerships, and increasingly urgent warnings, the UN system is mobilizing to confront the escalating 21st-century threats to governance, commerce, security, and humanity itself emerging from the ever-expanding ubiquity of the digital world - while also seeking to uphold privacy rights and human rights across online borders.[61] However, significant gaps still need concrete enforcement and accountability mechanisms for cyber harms. The coming years will test both the agility and collective will of the global community to restrain technological monsters of our creation. No digital innovation can be permitted to undermine foundational principles of humanity in the real world.

A Meaningful and Safe Digital Life. The Missing SDG

As the Internet and digital technologies have become deeply integrated into nearly every facet of modern life, some policy experts have argued for establishing a new 18th Sustainable Development Goal (SDG) to promote digital well-being, online privacy, cybersecurity, and responsible tech innovation.[62] With over 4.5 billion people online as of 2021, the UN acknowledges that "access to the Internet is essential for sustainable development" even as risks emerge in digital spaces.[63] However, the 17 Goals do not address technology regulation, digital rights, or Internet governance issues. Andrew Burt and Tabitha Goldstaub contend, "The success of the SDGs depends significantly on whether policymakers and regulators keep up with the fast pace of technological change,"[64] requiring focused global attention on humanity's "virtual development" through a dedicated SDG on Life Online. Such a goal could spur standardized metrics on issues like screen time overuse, implementation of data privacy protections, prevention of cyber harassment and attacks undermining healthcare systems and national security, as well as guidelines ensuring ethical AI practices and accountability across Big Tech companies pervading the online ecosystem - establishing a global consensus that the virtual world merits guardrails and good governance as much as the physical world.[65]

Conclusion

As the Internet and digital technologies continue to advance at breakneck speed, the global community finds itself at a critical juncture. Past UN resolutions to combat cyber threats have fallen short, needing concrete enforcement mechanisms while cybercriminals and extremist groups continue exploiting new technologies faster than governments can respond. Lives and critical infrastructure are threatened by sophisticated attacks enabled by artificial intelligence systems whose biases and impacts evade oversight.

---

[59] *Cybersecurity and New Technologies | Office of Counter-Terrorism*. (n.d.).
[60] *Inside Ireland's public healthcare ransomware scare*. (2021, December 13).
[61] Sodal. (2023, November 29). *The future of multilateral peacebuilding and conflict prevention*. Atlantic Council.
[62] Including Digital Connection in the United Nations Sustainable Development Goals: (2022)
[63] *Global Connectivity | Office of the Secretary-General's Envoy on Technology*. (n.d.).
[64] *Artificial intelligence planning must be inclusive to ensure sustainable development | UN Press*. (2023, May 4).
[65] *Artificial intelligence planning must be inclusive to ensure sustainable development | UN Press*. (2023, May 4).

We have officially entered the digital age with over half the world's population online, but the UN sustainable development agenda needs to include Goals focused directly on humanity's virtual development. If we fail to take swift and decisive action to secure cyberspace and uphold digital rights, we endanger all people - not just today but for future generations. As digital integration accelerates across societies, so must multilateral cooperation to prevent online harms, upholding the UN charter's promise to "reaffirm faith in fundamental human rights" for all those in the real world and the virtual. No single government can address this challenge alone. We must carry the spirit of UN collaborative action into the digital future, applying lessons from past limitations to foster adaptable and enforceable global consensus on the ethics of technology before humanity's innovations irrevocably imperil our collective wellbeing. Technology's promises of convenience and connection cannot eclipse Internet users' rights to security and privacy. Now is the time for urgent unified action to build guardrails for the online world.

Guiding Questions for Debate

1. How can we balance an individual's right to privacy with a government's need for access to data for national security purposes?
2. When private companies collect user data, what regulations are needed to protect privacy while allowing innovative technologies and services?
3. What international laws or norms should guide cyber operations between states to reduce escalation risks?
4. How can multilateral cooperation strengthen cyber security across borders without compromising state sovereignty?

Guiding Questions for Position Paper

1. What has your nation's historical approach been toward balancing security interests with personal privacy protections?
2. How has your nation regulated technology companies' collection and use of citizens' personal data? What further regulations are being considered?
3. What offensive and defensive cyber capabilities has your nation developed? How does your nation view the use of cyber operations by other states?
4. Is your nation a party to any international agreements on cyber norms or law enforcement cooperation? What role should international institutions play in setting cyber security rules?

Resource Review

UNGA Resolution 73/27 (2018) https://bit.ly/RES7327.

UNGA Resolution 73/27 establishes an essential framework for governing cyberspace. Adopted in 2018, the resolution affirms the applicability of international law to cyberspace and the UN's role in developing norms for responsible state cyber behavior. It calls for enhanced cooperation to promote secure, stable, and peaceful uses of ICTs.UNGA Resolution 73/27 provides a starting point for further developing global cybersecurity governance. Future UN resolutions will likely expand rules on protecting critical infrastructure, cybercrime cooperation, and updating norms as technology evolves. The resolution establishes cyberspace as an ongoing challenge requiring continuous multilateral cooperation going forward.

UNGA Resolution 71/28 (2016) https://bit.ly/RES7128.

UNGA Resolution 71/28 affirms the applicability of international law and norms of responsible state behavior in cyberspace. Adopted in 2016, it recognizes the need to continue developing shared understandings of existing and potential threats to ICTs.This resolution provides a framework for ongoing dialogue on applying international law and norms to cyberspace. Future resolutions could further define rules for ICT security, cybercrime cooperation, protecting critical infrastructure, and preventing military cyber conflicts. It frames cyberspace governance as an evolving challenge requiring continuous international cooperation.

UNGA Resolution 68/167 (2014) https://bit.ly/RES68167.

UNGA Resolution 68/167 affirms the right to privacy in the digital age. Adopted in 2014, it expresses concern over surveillance and data collection, violating privacy and undermining trust in ICTs. This resolution provides a framework for further developing global norms and regulations protecting digital privacy. Future resolutions could detail specific oversight mechanisms, safeguards for personal data, remedies for violations, and holding corporations accountable along with states. It establishes privacy as a human right requiring protection as technologies advance.

UNGA Resolution 55/63 (2001) https://bit.ly/RES5563.

UNGA Resolution 55/63 addresses combating criminal misuse of information technologies. Adopted in 2001, it expresses concern over attacks against computer systems and the growing misuse of technologies for criminal activities. This resolution provides a framework for furthering international cooperation on cybercrime laws and enforcement. Future resolutions could detail specific legal mechanisms, agreements on jurisdiction, and law enforcement capacity building. It establishes the need for multilateral collaboration in combating cyber threats globally.